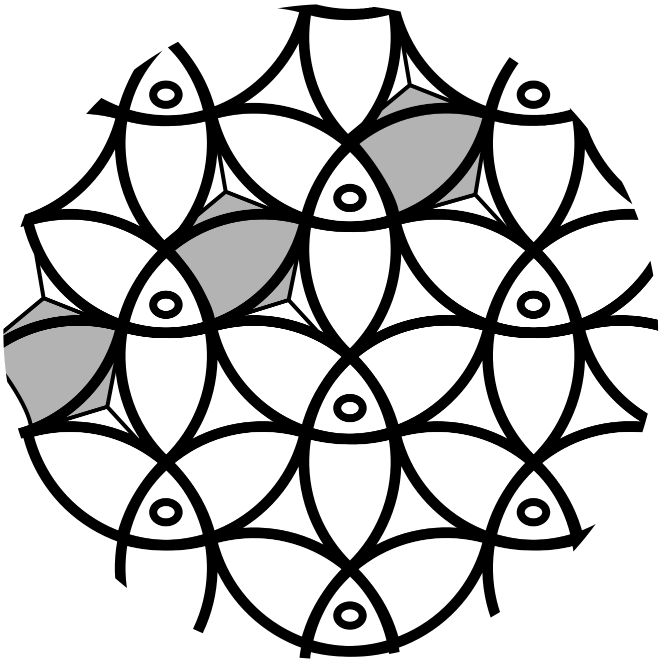
combinatorics 2000



© pistone

gaeta (lt), hotel serapo
28 may - 3 june
2000

scientific committee:
a. bichara, d. ghinelli, g. lunardon, f. mazzocca

supporting institutions:
università degli studi di roma “la sapienza”
cofinanziamento m.u.r.s.t.
“strutture geometriche combinatoria e loro applicazioni”
comune di gaeta

Università “La Sapienza” Roma

Composizione e grafica realizzate dalla
CompoMat Loc. Braccone, 02040 Configni (RI) Telefax 39 746 672240
www.compomat.it
Stpampato a cura del Centro Stampa d’Ateneo

Provisional Program

Sunday May 28

16.00 – 20.00 *Registration*

Monday May 29

08.30 — Departure by bus to Latina ("Università Pontina")

10.00 — Opening session

10.30 — **Bonisoli**

11.30 — **Buratti**

13.00 — Touristic tour (Terracina and Sperlonga) and packet lunch

19.00 — Arrival to Hotel Serapo

20.00 ——— Dinner ———

Tuesday May 30

09.00 – 09.45 — **Piper**

10.00 – 10.45 — **Cameron**

10.45 ——— Coffee break ———

11.15 – 12.00 — **Ball**

13.00 ——— Lunch ———

	A	B	C
15.30 – 15.50 —	**Ebert**	**Ando**	**Alinovi**
15.55 – 16.15 —	**Biliotti**	**Balconi**	**Blunk**
16.20 – 16.40 —	**King**	**Funk**	**Zizioli**
16.45 – 17.05 —	**Thomsen**	**Haemers**	**Zanella**

17.05 ——— Coffe break ———

	A	B	C
17.30 – 17.50 —	**Delera**	**Maenhaut**	**Elia**
17.55 – 18.15 —	**Pasini**	**Marcote**	**Sarmiento**
18.20 – 18.40 —	**Huybrechts**	**Pelayo**	**Schoerner**
18.45 – 19.05 —	**Sebille**	**Okamura**	**Simonis**

20.00 ——— Dinner ———

Wednesday May 31

09.00 – 09.45 — **Lauri**

10.00 – 10.45 — **Colbourn**

10.45 —— Coffee break ——

11.15 – 12.00 — **Havlicek**

13.00 —— Lunch ——

	A	B	C
15.30 – 15.50 —	Cara	Bernasconi	Vaccaro
15.55 – 16.15 —	Gewurz	Chouikha	Milazzo
16.20 – 16.40 —	Merola	Cieslik	Gionfriddo
16.45 – 17.05 —	Musumeci	Hotje	Mammana

17.05 —— Coffe break ——

	A	B	C
17.30 – 17.50 —	Maks	Bernardi	Tsuchiya
17.55 – 18.15 —	Tallini	Bisztriczky	Watanabe
18.20 – 18.40 —	Vincenti	Falcone	Zagaglia
18.45 – 19.05 —	Betten	Khelladi	Pianta
19.10 – 19.30 —			Labbate

20.00 —— Dinner; at the end: ——

—— **Concert** ——

Thursday June 1

09.00 – 09.45 — **Hachenberger**

10.00 – 10.45 — **Pott**

10.45 ———— Coffee break ————

11.15 – 12.00 — **Crapo**

13.00 ———— Lunch ————

	A	B	C
15.30 – 15.50 —	Hering	Pentilla	Batten
15.55 – 16.15 —	Lindner	Delanote	Brown
16.20 – 16.40 —	Rosa	Kuijken	Dover
16.45 – 17.05 —	Schulz	Ferrara Dentice	Iden

17.05 ———— Coffe break ————

	A	B	C
17.30 – 17.50 —	Mavron	De Vito	Donati
17.55 – 18.15 —	Street	Larato	Francot
18.20 – 18.40 —	Tonchev	Siciliano	Aguglia
18.45 – 19.05 —	Webb	Sonnino	Pfeiffer
19.10 – 19.30 —	Zuanni	Polverino	Schmidt

20.00 ———— Dinner ————

Friday June 2

09.00 – 09.45 — **Wefelscheid**

10.00 – 10.45 — **De Clerk**

10.45 ——— Coffee break ———

11.15 – 12.00 — **Buekenhout**

13.00 ——— Lunch ———

	A	B	C
15.30 – 15.50 —	Rinaldi	Giulietti	Kiss
15.55 – 16.15 —	Bean	Hirschfeld	Storme
16.20 – 16.40 —	Bluskov	Korchmaros	Szonyi
16.45 – 17.05 —	Kiechle	Pambianco	Weiner

17.05 ——— Coffe break ———

	A	B	C
17.30 – 17.50 —	Riesinger	Cossidente	Culbert
17.55 – 18.15 —	Pralle	Cherowitzo	Govaerts
18.20 – 18.40 —	Gropp	Bader	Mellinger
18.45 – 19.05 —	Sziklai	De Resmini	Shaw

20.00 ——— Gala Dinner In honour of **Maria Tallini Scafati** ———
(in occasion of her 70th birthday)

List of Participants

1 Abatangelo Luca Maria
Bari - Italy *e-mail:* abatlm@pascal.dm.uniba.it

2 Abatangelo Vito
Bari - Italy *e-mail:* abatvito@pascal.dm.uniba.it

3 Aguglia Angela
Napoli - Italy *e-mail:* aguglia@math.udel.edu
A Combinatorial Characterization of Classical Unitals

4 Alinovi Benedetta
Hamburg - Germany *e-mail:* ms9a009@math.uni-hamburg.de
Halfordered Chain Structures

5 Ando Kiyoshi
Tokyo - Japan *e-mail:* ando@im.uec.ac.jp
A Forbidden Subgraph Condition for a Graph to have a k-contractible Edge

6 Bader Laura
Napoli - Italy *e-mail:* bader@matna2.dma.unina.it
Generalizing Flocks of $Q^+(3,q)$
(with Guglielmo Lunardon & Antonello Cossidente)

7 Balconi Giorgio
Pavia - Italy *e-mail:* marpaolo@dimat.unipv.it
A Class of Dense Self-clique Graphs

8 BALL SIMEON
London - U.K. *e-mail:* `s.ball@qmw.ac.uk`
Arcs, Multi-arcs, Polynomials and Ovoids

9 BARLOTTI ADRIANO
Firenze - Italy *e-mail:* `barlotti@udini.math.unifi.it`

10 BARTOLONE CLAUDIO G.
Palermo - Italy *e-mail:* `cg@dipmat.math.unipa.it`

11 BATTEN LYNN M.
Victoria - Australia *e-mail:* `lmbatten@deakin.edu.au`
Partitions of Finite Projective Planes

12 BEAN RICHARD
Queensland - Australia *e-mail:* `rwb@maths.uq.edu.au`
On the Size of the Largest Critical Set in a Latin Square

13 BENZ WALTER
Hamburg - Germany *e-mail:* `ms3a001@math.uni-hamburg.de`

14 BERARDI LUIGIA
L'Aquila - Italy *e-mail:* `berardi@ing.univaq.it`

15 BERNARDI MARCO PAOLO
Pavia - Italy *e-mail:* `marpaolo@dimat.unipv.it`
On a Problem in the Geometry of Self-affine Fractals

16 BERNASCONI CARLO
Perugia - Italy *e-mail:* `matber@unipg.it`
Neighborhood Spaces: Connectedness and Topological Curves in Finite Spaces

17 BETTEN DIETER
Kiel - Germany *e-mail:* `betten@math.uni-kiel.de`
Unitals and Codes
(with Vladimir D. Tonchev)

18 BICHARA ALESSANDRO
Roma - Italy *e-mail:* `bichara@dmmm.uniroma1.it`

19 BILIOTTI MAURO
Lecce - Italy *e-mail:* biliotti@ilenic.unile.it
The Non-solvable Rank 3 Affine Planes

20 BISZTRICZKY TIBOR
Calgary - Canada *e-mail:* tbisztri@math.ucalgary.ca
Matroidally Rigid Polytopes

21 BLUNCK ANDREA
Vien - Austria *e-mail:* blunck@geometrie.tuwien.ac.at
Generalized Chain Geometries and a non-Classical Chain Space

22 BLUSKOV ILIYA
Prince George - Canada *e-mail:* bluskovi@unbc.ca
Difference Families and Optimization

23 BONISOLI ARRIGO
Potenza - Italy *e-mail:* bonisoli@unibas.it
Collineation Groups of Finite Planes: Any Progress?

24 BONOLI GIOVANNA
Napoli - Italy *e-mail:* bonogiov@matna2.dma.unina.it

25 BROWN JULIA M. N.
Toronto - Canada *e-mail:* juliamnb@YorkU.CA
Embeddings of $PG(3,q)$ in Hughes Planes of Order q^4

26 BRYANT DARRYN
Queensland - Australia *e-mail:* db@maths.uq.edu.au

27 BUEKENHOUT FRANCIS
Bruxelles - Belgium *e-mail:* fbueken@ulb.ac.be
Incidence Geometry and Finite Groups

28 BURATTI MARCO
Perugia - Italy *e-mail:* buratti@mat.uniroma1.it
A description of any Rregular and 1-rotational Design by Difference Methods

29 CAMERON PETER J.
London - U.K. *e-mail:* p.j.cameron@qmw.ac.uk
Codes, Matroids and Trellises

30 Capursi Maria
Newark - USA *e-mail:* `capursi@math.udel.edu`

31 Cara Philippe
Brussel - Belgium *e-mail:* `pcara@vub.ac.be`
Constructing Geometries for $PSL(2, 11)$

32 Cardinali Ilaria
Siena - Italy *e-mail:* `icardinali@unisi.it`

33 Casse Rey
Adelaide - Australia *e-mail:* `rcasse@maths.adelaide.edu.au`

34 Cauchie Sara
Gent - Belgium *e-mail:* `scauchie@cage.rug.ac.be`

35 Ceccherini Pier Vittorio
Roma - Italy *e-mail:* `pvcecch@mercurio.mat.uniroma1.it`

36 Cerroni Cinzia
Palermo - Italy *e-mail:* `cerroni@dipmat.math.unipa.it`

37 Cherowitzo William E.
Denver - USA *e-mail:* `wcherowi@carbon.cudenver.edu`
On Conic Blocking Sets

38 Chouikha A. Raouf
Villetaneuse - France *e-mail:* `chouikha@zeus.math.univ-paris13.fr`
Some Plane Isoperimetric Inequalities and Applications

39 Cieslik Dietmar
Greifswald - Germany *e-mail:* `cieslik@mail.uni-greifswald.de`
The Steiner Ratio of Several Discrete Metric Spaces

40 Colbourn Charles J.
Waterloo - Canada *e-mail:* `cjcolbou@math.uwaterloo.ca`
Group Testing, Combinatorial Designs, and Computational Biology

41 Cossidente Antonio
Potenza - Italy *e-mail:* `cossidente@unibas.it`
Caps on Classical Varieties and their Projections

42 Crapo Henry
Paris - France   *e-mail:* henry.crapo@ehess.fr
Matroids and Tensor Algebra

43 Culbert Craig
Delaware - USA   *e-mail:* culbert@math.udel.edu
Polarity-paired Spreads of $PG(3, q)$, q Odd

44 De Clerk Frank
Gent - Belgium   *e-mail:* fdc@cage.rug.ac.be
Partial and Semipartial Geometries, an Update

45 De Resmini Marialuisa J.
Roma - Italy   *e-mail:* resmini@mat.uniroma1.it
Partitioning Segre Varieties

46 De Salvo Mario
Messina - Italy   *e-mail:* desalvo@www.unime.it

47 De Vito Paola
Napoli - Italy   *e-mail:* devito@matna2.dma.unina.it
Ovoidal Linear Spaces

48 Del Fra Alberto
Roma - Italy   *e-mail:* delfra@dmmm.uniroma1.it
*Dimensional Dual Hyperovals, Steiner Systems and c.L*Geometries*

49 Delanote Mario
Gent - Belgium   *e-mail:* md@cage.rug.ac.be
Affine Semipartial Geometries and Projections of Quadrics

50 Donati Giorgio
Napoli - Italy   *e-mail:* donati@matna2.dma.unina.it
Pappus' Configuration in non Commutative Projective Geometry with Applications to a Theorem of A. Schleiermacher

51 Dover Jeremy
USA   *e-mail:* ajdover@aol.com
Blocking Semiovals in $PG(2, 7)$ and Beyond

52 Doyen Jean
Bruxelles - Belgium e-mail: jdoyen@ulb.ac.be

53 Durante Nicola
Napoli - Italy e-mail: durante@matna2.dma.unina.it

54 Ebert Gary
Newark - USA e-mail: ebert@math.udel.edu
Cyclotomy and Three-Dimensional Flag-Transitive Planes

55 Elia Michele
Torino - Italy e-mail: elia@polito.it
On the Linear Labeling of Lattice Constellations from Algebraic Number Fields
(with Jose Carmelo Interlando)

56 Enomoto Hikoe
Yokohama - Japan e-mail: enomoto@comb.math.keio.ac.jp

57 Faina Giorgio
Perugia - Italy e-mail: faina@dipmat.unipg.it

58 Falcone Giovanni
Palermo - Italy e-mail: falcone@mi.uni-erlangen.de
Dividing Cyclotomic Polynomials

59 Ferrara Dentice Eva
Napoli - Italy e-mail: eva.ferraradentice@unina2.it
An Intrinsic Characterisation of Quadrics

60 Fiori Carla
Modena - Italy e-mail: fiori@unimo.it

61 Fisher J. Chris
Regina - Canada e-mail: fisher@math.uregina.ca

62 Fleming Kirsten
Michigan - USA e-mail: kirsten.fleming@cmich.edu

63 Francot Eliana
Lecce - Italy e-mail: francot@ilenic.unile.it
Unitary Polarities in non Commutative Twisted Field Plane

64 Freni Sveva
Napoli - Italy e-mail: simone@unina2.it

65 Funk Martin
Potenza - Italy e-mail: funk@unibas.it
Canonically Pfaffian cubic bigraphs and blocking-set-free configurations

66 Garner Cyril
Ottawa - Canada e-mail: cgarner@math.carleton.ca

67 Gewurz Daniele
Roma - Italy e-mail: gewurz@mat.uniroma1.it
Actions of Permutation Groups

68 Ghinelli Dina
Roma - Italy e-mail: dina@mat.uniroma1.it

69 Gionfriddo Lucia
Catania - Italy e-mail: gionfriddo@dipmat.unict.it
Upper and Lower Chromatic Numbers for P3-Designs

70 Gionfriddo Mario
Catania - Italy e-mail: gionfriddo@dipmat.unict.it

71 Giulietti Massimo
Perugia - Italy e-mail: giuliet@dipmat.unipg.it
On Complete Arcs Arising from Plane Curves

72 Giuzzi Luca
Brescia - Italy e-mail: giuzzi@dmf.bs.unicatt.it

73 Govaerts Patrick
Gent - belgium e-mail: pg@cage.rug.ac.be
Maximal Partial t-spreads and Minimal t-covers in Finite Projective Spaces

74 Grone Robert
San Diego - USA e-mail: grone@math.sdsu.edu

75 Gropp Harald
Heidelberg - Germany e-mail: d12@ix.uni-heidelberg.de
On some Generalizations of Symmetric Designs

76 Grundhoefer Theo
Wuerzburg - Germany *e-mail:* grundh@mathematik.uni-wuerzburg.de

77 Hachenberger Dirk
Augsburg - Germany *e-mail:* hachenberger@math.uni-augsburg.de
The Combinatorics of Generators for Galois Fields

78 Haemers Willem
Tilburg - The Netherlands *e-mail:* haemers@kub.nl
Characterizations of Some Distance-regular Graphs their Spectra

79 Hagita Mariko
Yokohama - Japan *e-mail:* hagita@comb.math.keio.ac.jp

80 Havlicek Hans
Vienna - Austria *e-mail:* havlicek@geometrie.tuwien.ac.at
Veronese Varieties over Fields with non-zero Characteristic: A Survey

81 Hering Christoph
Tuebingen - Germany *e-mail:* christoph.hering@uni-tuebingen.de
On the Steiner System $S(24, 8, 5)$

82 Hirschfeld James W. P.
Sussex - U.K. *e-mail:* jwph@sussex.ac.uk
Arcs and curves over a Finite Field

83 Hotje Herbert
Hannover - Germany *e-mail:* hotje@math.uni-hannover.de
Skewaffine Spaces in the Language of Distance Spaces

84 Huybrechts Cecile
London - U.K. *e-mail:* c.huybrechts@qmw.ac.uk
Dual Polar Spaces and Fully Gated Graphs

85 Iden Oddvar
Bergen - Norway *e-mail:* iden@mi.uib.no
On Subplanes of Free Planes

86 Jaeger Ragnhild
Bergen - Norway *e-mail:* ragnhily@mi.uib.no

87 Jungnickel Dieter
Augsburg - Germany *e-mail:* jungnickel@math.uni-augsburg.de

88 Karzel Helmut
Muenchen - Germany *e-mail:* karzel@mathematik.tu-muenchen.de

89 Khelladi Abdelkader
Alger - Algeria *e-mail:* kader_khelladi@yahoo.fr
Generalized Tensions and Potentials

90 Kiechle Hubert
Hamburg - Germany *e-mail:* ms8a017@math.uni-hamburg.de
Circularity of certain F-pairs

91 King Oliver
Newcastle - U.K. *e-mail:* o.h.king@newcastle.ac.uk
Group-theoretic Ccharacterizations of Classical Ovoids

92 Kiss Gyorgy
Budapest - Hungary *e-mail:* kissgy@cs.elte.hu
A Construction of Arcs in High-dimensional Projective Spaces

93 Korchmaros Gabor
Potenza - Italy *e-mail:* korchmaros@unibas.it
Caps of the Hermitian Variety Arising from Maximal Curves

94 Kuijken Elisabeth
Gooik - Belgium *e-mail:* ekuijken@cage.rug.ac.be
A geometric description of Hermitian two-graphs and its applications

95 Labbate Domenico
Potenza - Italy *e-mail:* ld487sci@unibas.it
On 2-factor Hamiltonian Bipartite Graphs

96 Larato Bambina
Bari - Italy *e-mail:* larato@pascal.dm.uniba.it
Transitive Parabolic Unitals in Translation Planes

97 Lauri Josef
Malta *e-mail:* jlau@um.edu.mt
Constructing Graphs with Several Pseudosimilar Vertices or Edges

98 Law Maska
Nedlands - Australia e-mail: maska@maths.uwa.edu.au

99 Leonard Philip
Tempe - USA e-mail: pal@math.la.asu.edu

100 Li Marzi Enzo Maria
Messina - Italy e-mail: limarzi@dipmat.unime.it

101 Lindner Curt
Auburn - U.S.A. e-mail: lindncc@mail.auburn.edu

102 Lizzio Angelo
Catania - Italy e-mail: lizzio@dipmat.unict.it

103 Lo Faro Giovanni
Messina - Italy e-mail: lofaro@unime.it

104 Lo Re Pia Maria
Napoli - Italy e-mail: pialore@matna2.dma.unina.it

105 Lorimer J.W. (Michael)
Toronto - Canada e-mail: lorimer@math.toronto.edu

106 Lueneburg Heinz
Kaiserslautern - Germany e-mail: luene@mathematik.uni-kl.de

107 Lunardon Guglielmo
Napoli - Italy e-mail: lunardon@matna2.dma.unina.it

108 Maenhaut Barbara
Milton Keynes - U. K. e-mail: b.m.maenhaut@open.ac.uk
Graphs which are Both H_1 and H_2-decomposable

109 Maks Johannes
Delft - The Netherlands e-mail: j.g.maks@twi.tudelft.nl
Invariants of m-dimensional Linear Subspaces of a Binary $[n, k]$-code

110 Mammana Maria Flavia
Catania - Italy e-mail: flavia@dipmat.unict.it
On the Acrhomatic Number of $P(\alpha, K_n)$ and $P(\alpha, K_{1,n})$

111 Marchi Mario
Brescia - Italy *e-mail:* geomet@dmf.bs.unicatt.it

112 Marcote Ordax Xavier
Barcelona - Spain *e-mail:* francisco.javier.marcote@upc.es
Using a Progressive Withdrawal Algorithm to Study Superconnectivity in ℓ_1-Digraphs

113 Marino Maria Corinna
Messina - Italy *e-mail:* marino@ingegneria.unime.it

114 Maroscia Paolo
Roma - Italy *e-mail:* maroscia@dmmm.uniroma1.it

115 Mavron Vassili
Aberystwyth - U.K. *e-mail:* vcm@aber.ac.uk
Generalized Balanced Weighing and Difference Matrices

116 Mazzocca Francesco
Napoli - Italy *e-mail:* francesco.mazzocca@unina2.it

117 Mellinger Keith
Newark - USA *e-mail:* kmelling@math.udel.edu
Mixed Partitions and 3-Spreads of $PG(7,q)$

118 Melone Nicola
Napoli - Italy *e-mail:* nicola.melone@unina2.it

119 Merola Francesca
Roma - Italy *e-mail:* merola@mat.uniroma1.it
Sequences from Groups

120 Migliorato Renato
Messina - Italy *e-mail:* miglior@dipmat.unime.it

121 Migliori Grazia
Roma - Italy *e-mail:* migliori@mat.uniroma1.it

122 Milazzo Lorenzo
Catania - Italy *e-mail:* milazzo@dipmat.unict.it
Upper and Lower Chromatic Number for Steiner Systems

123 Milici Salvatore
Catania - Italy *e-mail:* milici@dipmat.unict.it

124 Musumeci Silvia
Palermo - Italy *e-mail:* musumeci@dipmat.math.unipa.it
A Class of Imprimitive Permutation Groups

125 Napolitano Vito
Potenza - Italy *e-mail:* nv354sci@pzuniv.unibas.it

126 Okamura Haruko
Kobe - Japan *e-mail:* okamura@center.konan-u.ac.jp
On 2-reducible Paths in k-edge-connected Graphs

127 Olanda Domenico
Napoli - italy *e-mail:* olanda@matna2.dma.unina.it

128 Pambianco Fernanda
Perugia - Italy *e-mail:* fernanda@dipmat.unipg.it
The Smallest Size of A Complete Cap in $PG(3,7)$

129 Pasini Antonio
Siena - Italy *e-mail:* pasini@unisi.it
On Absolutely Universal Embeddings

130 Pelayo Ignacio
Barcelona - Spain *e-mail:* ignacio.m.pelayo@upc.es
Superconnected Digraphs and Graphs with Small Conditional Diameters

131 Pellegrini Silvia
Brescia - Italy *e-mail:* spellegr@bsing.ing.unibs.it

132 Penttila Tim
Australia *e-mail:* penttila@maths.uwa.edu.au
A new Family of Flocks in Characteristic 2

133 Pfeiffer Thorsten
Muenchen - Germany *e-mail:* thorsten.pfeiffer@ercgroup.com
Pappus' Theorem for Ring-Geometries

134 Pianta Silvia
Brescia - Italy *e-mail:* geomet@dmf.bs.unicatt.it
Partial K-loops of Exponent 2 and Factorizations of Graphs with Trapezium Condition

135 Pica Giustina
Napoli - Italy *e-mail:* pica@cds.unina.it

136 Piper Fred
London - U.K. *e-mail:* f.piper@rhbnc.ac.uk
What is a Binary String?

137 Polverino Olga
Napoli - Italy *e-mail:* polverin@matna2.dma.unina.it
On Buekenhout-Metz Unitals

138 Pott Alexander
Magdeburg - Germany *e-mail:* alexander.pott@mathematik.uni-magdeburg.de
On the Geometry of Power Mappings in Finite Fields

139 Pralle Harm
Giessen - Germany *e-mail:* harm.pralle@math.uni-giessen.de
Baer Cone Intersection

140 Priess-Crampe Sibylla
Muenchen - Germany *e-mail:* schoerne@rz.mathematik.uni-muenchen.de

141 Prince Alan R.
Edinburgh - Scotland *e-mail:* a.r.prince@ma.hw.ac.uk

142 Quattrocchi Gaetano
Catania - Italy *e-mail:* quattrocchi@dmi.unict.it

143 Quattrocchi Pasquale
Modena - Italy *e-mail:* quattrocchi@unimo.it

144 Riemenschneider Maren
Darmstadt - Germany *e-mail:* mr@mathematik.tu-darmstadt.de

145 Riesinger Rolf
Wien - Austria *e-mail:* havlicek@geometrie.tuwien.ac.at
Extending the Thas-Walker construction

146 Rinaldi Gloria
Modena - Italy e-mail: rinaldi@unimo.it
Complete Unital-derived Arcs in the Hall Planes

147 Rosa Alexander
Ontario - Canada e-mail: rosa@mcmail.cis.McMaster.CA
Specialized Colourings of Steiner systems $S(2,4,v)$

148 Rutherford Carrie
London - U.K. e-mail: c.g.rutherford@qmw.ac.uk

149 Sarmiento Irasema
Berlin - Germany e-mail: sarmient@math.fu-berlin.de
Hopf Algebras and the Penrose Polynomial

150 Scafati Tallini Maria
Roma - Italy e-mail: tallini@mat.uniroma1.it

151 Schmidt Stefan E.
M.I.T. - (U.S.A.) e-mail: Schmidt@math.mit.edu
Expectation Values for Codes over Rings

152 Schoerner Erwin
Muenchen - Germany e-mail: schoerne@rz.mathematik.uni-muenchen.de
Maximally Valued Division Algebras

153 Schulz Ralph-Hardo
Berlin - Germany e-mail: schulz@math.fu-berlin.de
On Divisible Designs with Dual Translation Group

154 Sebille Michel
Bruxelles - Belgium e-mail: msebille@cso.ulb.ac.be
Line-transitive Point-imprimitive Linear Spaces

155 Shaw Ron
Cottingham - U. K. e-mail: r.shaw@maths.hull.ac.uk
Partial Spreads in $PG(4,2)$*: Sym(6) Aspects*

156 Siciliano Alessandro
Napoli - Italy e-mail: sicilian@mat.uniroma1.it
Linear Sections of Line Grassmannians Over Finite fields

157 Siemon Helmut
Reichenberg - Germany

158 Simonis Juriaan
Eindhoven - The Netherlands *e-mail:* `J.Simonis@twi.tudelft.nl`
Multilinear Representability of Matroids

159 Sonnino Angelo
Potenza - Italy *e-mail:* `sonnino@unibas.it`
Complete Arcs Arising from Conics

160 Spence Edward
Glasgow - Scotland *e-mail:* `ted@maths.gla.ac.uk`

161 Spera Antonino
Palermo -Italy *e-mail:* `spera@dipmat.math.unipa.it`

162 Storme Leo
Gent - Belgium *e-mail:* `ls@cage.rug.ac.be`
Caps in $PG(5,3)$ *and* $PG(6,3)$

163 Street Anne
Queensland - Australia *e-mail:* `aps@maths.uq.edu.au`
Decomposition of Sets of Triples into Small Planes (with Rudi Mathon)

164 Sziklai Peter
Budapest - Hungary *e-mail:* `sziklai@cs.elte.hu`
Covers and Caps of the Klein Quadric $Q^+(5,q)$

165 Szonyi Tamas
Budapest - Hungary *e-mail:* `szonyi@cs.elte.hu`
Small defining Sets for $PG(2,q)$ (with E. Boros)

166 Tallini Luca
Milano- Italy *e-mail:* `luca.tallini@polimi.it`
Onm-ary Balanced Codes

167 Thomsen Momme Johs
Hamburg - Germany *e-mail:* `momme.thomsen@unibw-hamburg.de`
On Groups Whose Inner Automorphism Nearring is a Ring

168 TONCHEV VLADIMIR D.
Houghton - U.S.A. *e-mail:* `tonchev@mtu.edu`
A Mass Formula for Steiner Triple Systems $STS(2^{n-1})$ of 2-rank $2^n - n$

169 TONESI CRISTINA
Gent - Belgium *e-mail:* `tonesi@cage.rug.ac.be`

170 TSUCHIYA MORIMASA
Tokio - Japan *e-mail:* `tsuchiya@ss.u-tokai.ac.jp`
On Construction of Bound Graphs

171 UGHI EMANUELA
Perugia - Italy *e-mail:* `ughi@dipmat.unipg.it`

172 VACCARO MARIA ALESSANDRA
Palermo - Italy *e-mail:* `vaccaro@dipmat.math.unipa.it`
Simultaneous Reduction of a Pair of Symmetric Bilinear Forms to Canonical Form

173 VINCENTI RITA
Perugia - Italy *e-mail:* `alice@unipg.it`
Classical Varieties and Codes

174 WALKER KEITH
Keele - U. K. *e-mail:* `k.walker@keele.ac.uk`

175 WATANABE MAMORU
Kurashiki - Japan *e-mail:* `watanabe@soft.kusa.ac.jp`
On the Orientation Associated with a 3-Face-coloring of a Triangulation

176 WEBB BRIDGET
Milton Keynes - U. K. *e-mail:* `b.s.webb@open.ac.uk`
What is an Infinite Design?

177 WEFELSCHEID HEINRICH
Duisburg - Germany *e-mail:* `wefelscheid@math.uni-duisburg.de`
Infinite Permutation Groups with Nice Transitivity Properties

178 WEINER ZSUZSA
Budapest - Hungary *e-mail:* `weiner@cs.elte.hu`
On Blocking Sets in Higher Dimension

179 Zagaglia Norma
Milano - Italy e-mail: norzag@mate.polimi.it
Scattered Subsets

180 Zanella Corrado
Padova - Italy e-mail: zanella@math.unipd.it
On Embedded Products of Grassmannians

181 Zeitler Herbert
Bayreuth - Germany

182 Zizioli Elena
Brescia - Italy e-mail: geomet@dmf.bs.unicatt.it
Relations between Certain Classes of Incidence Loops, Codes and Chain Structures

183 Zuanni Fulvio
L'Aquila - Italy e-mail: zuanni@ing.univaq.it
On Perfect Cayley Designs

Transitive Parabolic Unitals in Translation Planes

V. Abatangelo, B. Larato*

Politecnico di Bari
e-mail: larato@pascal.dm.uniba.it

We survey some recent results on transitive parabolic unitals in translation planes. Let π be an affine translation plane and $\bar{\pi}$ the projective plane arising from π. A unital $\mathcal{U}$ of $\bar{\pi}$ is *parabolic* if it has only one point at infinity. A parabolic unital $\mathcal{U}$ is *transitive*, if the collineation group G fixing $\mathcal{U}$ fixes the point at infinity of $\mathcal{U}$ and acts transitively on the affine points of $\mathcal{U}$. A general result on transitive parabolic unital was stated in [1].

THEOREM. *Let π be a translation plane of odd order containing a transitive parabolic unital $\mathcal{U}$. Assume that the collineation group G of π fixing $\mathcal{U}$ contains an affine homology. Then π is a semifield plane, and*

(i) *G has a normal subgroup K that acts on the affine points of $\mathcal{U}$ as a sharply transitive permutation group.*
Also, if K is commutative, then

(ii) *π is a commutative semifield plane.*

It has been conjectured that if a transitive parabolic unital $\mathcal{U}$ consists of the absolute points of a unitary polarity in a commutative semifield plane, then the sharply transitive normal subgroup K of G is not commutative. So far, this has been proved for commutative twisted field planes of odd square order, see [2], [3], and very recently for commutative Dickson planes.

References

[1] V. Abatangelo and B. Larato: *Polarity and transitive parabolic unitals in translation planes of odd order*, preprint.

[2] V. Abatangelo, G. Korchmáros and B. Larato: *Transitive parabolic unitals in translation planes of odd order*, Discrete Math. to appear.

[3] V. Abatangelo, M.R. Enea, G. Korchmáros and B. Larato: *Ovals and unitals in commutative twisted field planes*, Discrete Math. **208/209** (1999) 3-8.

A Combinatorial Characterization of Classical Unitals

A. Aguglia*, G. L. Ebert

Università di Napoli "Federico II"
e-mail: aguglia@math.udel.edu

A characterization of classical unitals is given in terms of a configuration pattern assumed by the feet of a unital U embedded in $PG(2, q^2)$, $q > 2$.

It is showed that a necessary and sufficient condition for U to be classical is the existence of two points $p_0, p_1 \in U$ with tangent lines L_0 and L_1 respectively such that for all points $r \in L_0 \setminus \{p_0\}$ and $s \in L_1 \setminus \{p_1\}$ the corresponding feet are collinear.

1991 Mathematics Subject Classification: 51E20.

Key words and phrases: Unital, Hermitian curve, projective plane.

Halfordered Chain Structures

B. Alinovi*, H. Karzel

Technische Universität München - Germany
e-mail: ms9a009@math.uni-hamburg.de

Let E be a set of points, with $|E| \geq 4$, and let $\xi : E^{3'} := \{(a,b,c) \in E^3 \mid a \neq b,c\} \to \{1,-1\}; (a,b,c) \mapsto \xi(a,b,c) =: (a|b,c)$ be a map such that the axiom

(Z) $\forall\ a,b,c,d \in E, a \neq b,c,d :\ (a|b,c) \cdot (a|c,d) = (a|b,d)$

is satisfied. Then the function ξ is called a *halforder* of E and the pair (E,ξ) a *halfordered set.* To each halfordered set (E,ξ) we associate a *separation function* $\tau_\xi : E^{4'} := \{(a,b,c,d) \in E^4 \mid a,b \neq c,d\} \to \{1,-1\}; (a,b,c,d) \mapsto \tau_\xi(a,b,c,d) =: [a,b|c,d] := (a|c,d) \cdot (b|c,d)$ and we say that two halforders ξ_1 and ξ_2 of E are *related*, denoted by ξ_1 *rel* ξ_2, if

(R) $\forall\ (a,b,c,d) \in E^{4'} :\ [a,b|c,d]_1 = [c,d|a,b]_2;$

a halforder ξ of E is called *selfrelated* if ξ *rel* ξ.

Let $K \subset E$; then a function $K_s : (E \setminus K) \times (E \setminus K) \to \{1,-1\}; (a,b) \mapsto K_s(a,b) =: (K_s|a,b)$ is called a *splitting of E by K* if the following condition

(S1) $\forall\ a,b,c \in E \setminus K : (K_s|a,b) \cdot (K_s|b,c) = (K_s|a,c)$

is satisfied.

Also the concept of halfordered chain structure $(\mathcal{P}, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K}; \xi)$ will be introduced (cf. [1] sec. 3) and the connection between all these concepts will be established.

References

[4] Alinovi, B., Karzel, H., Tonesi, C.: *Halfordered chain structures.*, Quaderni del Sem. Mat. di Brescia **18** (1999).

A Forbidden Subgraph Condition for a Graph to have a *k*-contractible Edge

Kiyoshi Ando*

University of Electro-Communications, Chofu - Tokyo, Japan
e-mail: `ando@im.uec.ac.jp`

Ken-ichi Kawarabayashi

KeiO University, Yokohama, Kangawa, Japan

We deal only simple graphs. An edge of a k-connected graph G is said to be k-contractible if the contraction of the edge in G results a k-connected graph. Though many results on contractible edges are known for small k, for large k there are not so many. The following is one of most important results on general k-contractible edges.

THEOREM (Thomassen [1]). *Every triangle free k-connected graph has a k-contractible edge.*

In this note, we give the following result, which is an extension of the Thomassen's theorem.

THEOREM. *Let k,s, and t be positive integers such that $k \geq 5$ and $s(t-1) \leq k$ and let G be a k-connected graph. If G has neither $K_2 + sK_1$ nor $K_1 + tK_2$ as a subgraph, then G has a k-contractible edge.*

References

[5] THOMASSEN, C.: *Non-separating cycles in k-connected graphs*, J. Graph Theory, **5**, (1981), 351-354.

Generalizing Flocks of $Q^+(3,q)$

L. Bader*, G. Lunardon

Dipartimento di Matematica, Università di Napoli "Federico II", Napoli Italia
e-mail: bader@matna2.dma.unina,it

A. Cossidente

Università degli studi della Basilicata

Let $Q^+(3,q)$ denote the hyperbolic quadric of $PG(3,q)$, q any prime power. A $flock$ of $Q^+(3,q)$ is a partition of the quadric in $q+1$ irreducible conics. A flock is *linear* if all the planes of the conics of the flock share a line. Flocks of $Q^+(3,q)$ are equivalent to translation planes (of order q^2 and kernel containing $GF(q)$) associated with (A,B)–regular line spreads of $PG(3,q)$, via a construction involving both the Plücker correspondence and the Klein quadric.

Flocks of $Q^+(3,q)$ have been classified both for q even, in which case they are necessarily linear, and for q odd, in which case they are either linear, or Thas (obtained by taking two halves of suitable linear flocks), or exceptional (which exist for $q = 11, 23, 59$ only).

As $Q^+(3,q)$ is the smallest Segre variety $S_{1,1}$, we extend the notion of flock to the Segre variety $S_{n,n}$ as a partition of $S_{n,n}$ into caps of size $q^n + \cdots + q + 1$. Using the Grassmannian $\mathcal{G}_{1,n}$, we prove that any (A,B)–regular n–spread of $PG(2n+1,q)$ is defined by a partition of $S_{n,n}$ into Veronese varieties canonically embedded in the Segre variety ($flat$ flock) and conversely, so that flat flocks are equivalent to the translation planes of order q^{n+1} and kernel containing $GF(q)$ associated with (A,B)–regular n–spreads of $PG(2n+1,q)$.

We give examples of flat flocks and we also construct partitions of $S_{n,n}$ not defining translation planes but still having interesting geometric properties, paying special attention to the case $n = 2$.

Partitioning Segre Varieties

L. Bader

Università di Napoli "Federico II"

A. Cossidente

Università degli Studi della Basilicata

M.J. de Resmini*

Università di Roma "La Sapienza"
e-mail: resmini@mat.uniroma1.it

Any Segre variety, which is the tensor product of two projective spaces, admits two "natural" partitions, namely those provided by its reguli.

We show that a Segre variety of suitable indices admits a more interesting partition, in the sense that it can be partitioned into Segre varieties of smaller indices. Such a process can be iterated and yields a "nested partition", i.e. a partition of a Segre variety into Segre varieties each of which can turn be partitioned into smaller Segre varieties, and so on.

For some choices of the indices, a partition of a Segre variety into Segre varieties may be constructed in different ways: via projectivities, via coordinates, and via the action of a suitable group, namely a Singer cycle.

The above mentioned results hold for Segre varieties over any field, even if special attention is paid to finite fields in which case other types of partitions are considered too.

Cyclotomy and Three-Dimensional Flag-Transitive Planes

R.D. Baker, G.L. Ebert*, K.H. Leung, Q. Xiang

Dept. of Math. Sci. - University of Delaware - Newark, DE 19716 - USA
e-mail: ebert@math.udel.edu

Using a connection with perfect Baer subplane partitions of $\mathrm{PG}(2, q^2)$, the classification of odd order three-dimensional flag-transitive affine planes admitting a cyclic regular action on the line at infinity was reduced to verifying a certain cyclotomic conjecture. Here we prove this conjecture is true, thereby showing that all such flag-transitive planes are known. If the order is q^3, so that the kernel is $\mathrm{GF}(q)$, the number of isomorphism classes is at least $(q-1)/2e$, where $q = p^e$. If q is prime, the number is exactly $(q-1)/2$. It should be noted that the above mentioned action on the line at infinity is one of only two known possibilitiies for flag-transitive affine planes.

A Class of Dense Self-clique Graphs

G. Balconi

Dipartimento di Matematica "F. Casorati"
Università di Pavia - Pavia - Italy
e-mail: `marpaolo@dimat.unipv.it`

A self-clique graph G is a graph G isomorphic to its clique-graph $C(G)$. Very often a self-clique graph has a cliques-vertices polarity π: let $\pi(G)$ be the polarity graph of π, that is the graph with $V(\pi(G)) = V(G)$, $uv \in E(\pi(G))$ iff $u \in \pi(v)$. We study the graph equation $\pi(G) = \overline{G}$, where $\overline{G}$ is the complementary graph of G and π is a polarity without absolute vertices. We characterize the solutions of this equation: a separated neighborhood indipendence graph (S.N.I. graph) is a graph whose only maximal independent sets are the neighborhoods of vertices and distinct vertices have distinct neighborhoods. S.N.I. graphs are the solutions of the studied graph equation.

We also construct an infinite family of S.N.I. graphs.

Arcs, Multi-arcs, Polynomials and Ovoids

S. Ball

London, UK

e-mail: mbrown@cage.rug.ac.be

1. (k, r)-arcs

A (k, r)-*arc* in a projective plane π_q of order $q = p^h$ is a set $\mathcal{K}$ of k points in π_q with at most r points on a line. A complimentary definition is that of a t-fold blocking set $\mathcal{B}$ that is; $\mathcal{B}$ is a set that meets every line in at least t points. Various bounds have been obtained for size of a (k, r)-arc in $PG(2, q)$. The upper bounds generally coming from the "polynomial method"; associating the points of $AG(2, q)$ with the elements of $GF(q^2)$ and using the collinearity condition that the points x, y and z are collinear if and only if

$$(x-y)^{q-1} = (x-z)^{q-1}.$$

The bounds are dependent on the nature of r and q. For example if $r = p^e$ for some e then the trivial upper bound $k \leq rq - q + r$ is obtainable for $p = 2$ yet not for $p > 2$ and not when $r \neq p^e$. In more recent developments Hill, Landjev and Ward considered (k, r)-multi-arcs $\mathcal{K}$ where they allow the set of points $\mathcal{K}$ to be a multi-set. When $r < q+1$ this is of no benefit and in fact the upper bound reduces drastically in the case when $\mathcal{K}$ does contain multi-points. The complimentary problem for t-fold blocking sets also changes when we allow multi-points however in this case it becomes trivial since we can then obtain the trivial lower bound of $t(q + 1)$. However when $r > q + 1$ not only is it necessary to allow multi-points the problem becomes interesting. The trivial upper bound for a $(k, q + 1 + r)$-arc is

$$k \leq q^2 + 1 + r(q + 1)$$

which is always attainable by taking the set consisting of each point external to a dual $(q+1-r)$-arc twice and each point that is on exactly one line of the dual $(q+1-r)$-arc once. The initial case $r = 1$ turns out to be a special case and this has been studied by Hill, Landjev and Ward who obtain many different constructions of $(q^2+q+2, q+2)$-arcs, some characterisations and the classification in the case when q is a prime and there are more than $q-1$ double points. This classification comes once more from the "polynomial method" which implies that if there are more than $q-1$ double points (it is easy to check that there are no triple points, 4-fold points etc..) then every line meets $\mathcal{K}$ in 2 mod p points. More generally for a $(q^2 + 1 + r(q + 1), q + 1 + r)$-arc $\mathcal{K}$ with $r > 1$ it is easy to see that there are always at least $q - 1$ double points and then it follows that every line meets $\mathcal{K}$ in $r + 1$ mod p points. When q is prime this is enough to classify such arcs and when q is not prime the nature of r is once more important. Note that a maximal $(rq-q+r, r)$-arc in π_q together with all the points of π_q forms a $(q^2+1+r(q+1), q+1)$ arc with no external points.

2. Ovoids

The generalized quadrangle $W(q)$ is constructed from the points and totally isotropic lines of the symplectic polarity in $PG(3,q)$. An *ovoid* in $PG(3,q)$ is a set $\mathcal{O}$ of points with the properties; no 3 points of $\mathcal{O}$ are collinear and the tangents to $\mathcal{O}$ form a plane pencil. An *ovoid* in a generalised quadrangle is a set $\mathcal{O}$ of points with the property that each line contains a unique point of $\mathcal{O}$. An ovoid in $W(q)$ is an ovoid in the ambient $PG(3,q)$ when q is even. The classification of ovoids in $W(q)$ or $PG(3,q)$ has not progressed since Penttila, O'Keefe and Royle's classification of the case $q = 32$ in 1994 and the elliptic quadrics and the Tits ovoids remain the only known ovoids. The classification method used by Penttila, O'Keefe and Royle involved the classification of ovals in planes of the same order and a classification of ovoids by this method would require a classification of ovals which is probably a harder problem. It seems that new methods of considering ovoids are required. One approach is the application of the polynomial method. The points of $PG(3,q)$ can be associated with the (q^3+q^2+q+1)-st roots of unity of $GF(q^4)$ and a symplectic polarity can be chosen in such a way that points x and y are orthogonal if and only if

$$(x,y) := x^{q+1} + y^{q+1} + xy^{q^2+q+1} + yx^{q^2+q+1} = 0.$$

It then follows that the totally isotropic lines are the sets of zeros of polynomials of the form

$$x^{q+1} + (e^{(q^2+q+2)/2} + e^{(q+1)/2})x + e$$

where $e^{q^3+q^2+q+1} = 1$ and we call such a totally isotropic line (line of $W(q)$) the line parameterised by e. If the lines parameterised by e and s meet in the point x then dually the points e and s are joined by the line parameterised by x^{2q}. It is then possible to find equivalent polarities of $W(q)$; for example

$$\pi : x \longrightarrow \text{ line parameterised by } x^{\sqrt{2q}}$$

and find polynomials whose set of zeros form Tits ovoids and dually Lüneburg spreads. This enables us to consider polynomial representations of the Lüneburg planes. An alternative approach using the theory of generalized quadrangles has recently led to the following impressive characterisations by Brown.

Theorem. *Let $\mathcal{O}$ be an ovoid of $PG(3,q)$, q even, and π a plane of $PG(3,q)$ such that $\pi \cap \mathcal{O}$ is a conic. Then $\mathcal{O}$ is an elliptic quadric.*

Theorem. *Let $\mathcal{O}$ be an ovoid of $PG(3,q)$, q even, and π a plane of $PG(3,q)$ such that $\pi \cap \mathcal{O}$ is a pointed conic. Then either $q = 4$ and $\mathcal{O}$ is an elliptic quadric or $q = 8$ and $\mathcal{O}$ is a Tits ovoid.*

Partitions of Finite Projective Planes

L.M. Batten

Deakin University - Victoria 3168, Australia
e-mail: lmbatten@deakin.edu.au

We consider decompositions of finite projective planes into copies of a particular substructure. We show that every projective plane of order $q \equiv 1 (\mathrm{mod}\ 3)$ is decomposable into l linear 3-*sets* and t non-linear 3-*sets* for all non-negative integers l and t such that $3(l+t) = q^2 + q + 1$. We also prove that the presence of a subplane leads to a decomposition of the plane into linear d-*sets* for d a particular function of the order of the subplane.

On the Size of the Largest Critical Set in a Latin Square

R. Bean*

Centre for Discrete Mathematics and Computing
Department of Mathematics
The University of Queensland
Queensland 4072, Australia
email: rwb@maths.uq.edu.au

E.S. Mahmoodian

Department of Mathematical Sciences
Sharif University of Technology
P.O. Box 11365–9415
Tehran, I.R. IRAN

The cardinality of the largest critical set in a Latin square of order n is denoted by $\mathrm{lcs}(n)$. In 1978 Curran and van Rees proved that $\mathrm{lcs}(n) \leq n^2 - n$. Here we show that $\mathrm{lcs}(n) \leq n^2 - 3n + 3$.

On a Problem in the Geometry of Self-affine Fractals

M. P. Bernardi* - C. Bondioli

Dipartimento di Matematica "F. Casorati"
Università di Pavia - Pavia - Italy
e-mail: marpaolo@dimat.unipv.it

Let Γ be a "deterministic" fractal, that is, the compact set which is invariant with respect to a finite system Φ of contraction maps in a complete metric space X.

Suppose that $X = \mathbb{R}^n$, that the contraction maps of Φ are similitudes, and moreover a condition of "minimal overlapping" is satisfied. Then Γ is said to be *self-similar*, and the Hausdorff dimension of Γ coincides with the solution of a simple exponential equation, constructed by means of the similarity ratios of Φ (cf. [2]).

Suppose now that $X = \mathbb{R}^n$ and the contraction maps of Φ are affinities. Then Γ is said to be *self-affine*, and it is still possible to use the affinity ratios of Φ for introducing an "affine" exponential equation, analogous to the preceding one. H. Triebel [4] called its solution d_A the *affine dimension* of Γ and used it extensively in the study of fractal (pseudo)differential operators. However, it is not yet completely clear under what hypotheses d_A describes not only a property of Φ, but an intrinsic property of Γ.

We would like to give some results regarding this problem. We will examine in particular the so-called *general Sierpiński carpets* (cf. [3]), a topic closely related to the combinatorial theory.

References

[6] M.P. Bernardi, C. Bondioli: Z. Analysis Anwend. **18** (1999), 733-751.

[7] J.E. Hutchinson: Indiana Univ. Math. **30** (1981), 713-747.

[8] C. McMullen: Nagoya Math. J. **96** (1984), 1-9.

[9] H. Triebel: *Fractals and Spectra*, Birkhäuser, 1997.

Neighborhood Spaces: Connectdness and Topological Curves in Finite Spaces

C. Bernasconi

Università di Perugia - Italy
e-mail: matber@unipg.it

Starting from the general theory of neighborhood spaces, the guidelines for funding a theory of connectdness and topological curves on finite spaces are outlined.

Application in the field of Image Processing is shown, and the basic role played by graphs is enlightened.

Unitals and Codes

D. Betten*

University of Kiel, Germany
e-mail: betten@math.uni-kiel.de

A. Betten

University of Bayreuth, Germany

V. D. Tonchev

Michigan Technological University, USA

A program is outlined for the enumeration of unital 2-(28,4,1) designs that uses tactical decompositions defined by vectors of certain weight in the dual binary code of a design. A class of designs with a spread that covers a codeword of weight 12 is studied in detail. A total of 702 nonisomorphic designs are constructed that include the classical hermitian and Ree unitals, as well as many other of the 145 previously known 2-(28,4,1) designs.

Caps on Classical Varieties and their Projections

J. Bierbrauer

Michigan Technological University, Houghton

A. Cossidente*

University of Basilicata, Potenza, Italy
e-mail: cossidente@unibas.it

Y. Edel

Mathematisches Institut der Universität, Heidelberg

A family of caps due to Ebert, Metsch and Szönyi arises from projection of a Veronesean or a Grassmannian to a suitable lower-dimensional space. We improve on this construction by projecting to a space of much smaller dimension. More precisely we partition $PG(3r-1,q)$ into a $(2r-1)-$space, an $(r-1)-$space and q^r-1 cyclic caps, each of size $(q^{2r}-1)(q-1)$. We also decide when one of our caps can be extended by a point from the $(2r-1)-$space or the $(r-1)-$space. The proof of the results uses several ingredients, most notably hyperelliptic curves.

The Smallest Size of A Complete Cap in PG(3,7)

J. Bierbrauer

Michigan Technological University, Houghton

S. Marcugini, F. Pambianco*

Università di Perugia, Italy
e-mail: fernanda@dipmat.unipg.it

In this work the minimum order for complete caps in PG(3,7) is determined and almost all the smallest complete caps have been classified. For the solution of this problem we have utilized other than Groups' theory, Graph-theoretical Ramsey theory and projective equivalence properties, the relation between $(n, 3)$-arcs and the eventually existence of opportune codes. Precisely, after having classified all the $(n, 3)$-arcs in PG(2,7), we have proven the existence of $[14, 4, 10]\_7$ codes and the non-existence of $[n, 4, n-4]\_7$ codes, $n = 15$, 16. That led us to put restrictions in the initial hyperplane configurations for the successive search of complete caps.

The Non-solvable Rank 3 Affine Planes

M. Biliotti*

Univ. Lecce
e-mail: biliotti@ilenic.unile.it

N.L. Johnson

Iowa University

A finite affine plane π is said to be a *rank* 3 *affine plane* if and only if there is a collineation group G which acts transitively on the affine points of π and for an affine point 0, the stabilizer subgroup G_0 has exactly three affine point orbits, one of which is $\{0\}$.

The plane is said to be a *solvable* or a *non-solvable* rank 3 affine plane according to whether G is solvable or non-solvable. A well known result of Kallaher and Liebler shows that any rank 3 affine plane is a translation plane. Furthermore,

THEOREM (Kallaher*Let π be a rank* 3 *affine plane with corresponding rank* 3 *group G. Then one of the following holds:*
(a) G is flag-transitive on π and G_l acts as a rank 3 *group on l for all lines l of π,*
(b) G has exactly two orbits on l_∞ and G_l operates doubly transitive on l for all lines l of π.
In case (b) π is called a *weak rank* 3 *affine plane.*

Solvable rank 3 affine planes and the corresponding rank 3 groups have been essentially determined by Foulser and Kallaher in [2] and [3]. Non-solvable flag-transitive planes have been determined in [1], [4]. Here we determine non-solvable weak rank 3 affine planes. Our main result is as follows:

THEOREM*Let π be a non-solvable rank* 3 *affine plane. Then π is one of the following types of planes:*
(1) Desarguesian,
(2) Hall,
(3) Lüneburg-Tits,
(4) irregular nearfield plane of order 11^2, 29^2 *or* 59^2*,*
(5) Korchmáros of order 49*,*
(6) Mason-Ostrom of order 49*,*
(7) one of the three exceptional Walker planes of order 25*.*
The corresponding rank 3 groups are also given.

References

[10] F. Buekenhout, A. Delandtsheer, J. Doyen, P.B. Kleidman, M. Liebeck and J. Saxl: *Linear spaces with flag-transitive automorphism groups*, Geom. Dedicata **36** (1990), 89-94.

[11] D.A. Foulser and M.J. Kallaher: *Solvable, flag-transitive, rank 3 collineation groups*, Geom. Dedicata **7** (1978), 111-130.

[12] M.J. Kallaher: *Translation planes admitting solvable rank 3 collineation groups*, Geom. Dedicata **6** (1977), 305-329.

[13] M.W. Liebeck: *The classification of finite linear spaces with flag-transitive automorphism groups of affine type*, J. Combin. Theory -Ser.A **84** (1998), 196-235.

Matroidally Rigid Polytopes

T. Bisztriczky

Department of Mathematics
University of Calgary, Canada
e-mail: tbisztri@math.ucalgary.ca

Let P denote a (convex)d-polytope with the face lattice $L(P)$ and the oriented matroid $OM(P)$ of affine dependencies. Let Q and R be d-polytopes.The Q and R are combinatorially equivalent if their face lattices are isomorphic(denote by $L(P) = L(Q)$,and geometrically equivalent if there is a bijection between vertex sets that preserves both minimal affine dependecies and the associated bipartition of the coefficients into positive and negative ones(denote by $OM(Q) = OM(R)$. We say that P is matroidally rigid if $L(P') = L(P)$ implies $OM(P') = OM(P)$ for any d-polytope P'. Well known examples of such rigid polytopes are simplices,cyclic polytopes and Lawrence polytopes. We present a new class of examples: d-multiplices with at most $2d$ vertices.

On Absolutely Universal Embeddings

R.J. Blok, A. Pasini*

Università di Siena, Italy
e-mail: pasini@unisi.it

It is well known that, given a point-line geometry Γ and a projective embedding $\varepsilon : \Gamma \to PG(V)$, if $dim(V)$ equals the size of a generating set of Γ, then ε is not derived from any other embedding. Thus, if Γ admits an absolutely universal embedding, then ε is absolutely universal. Tn this paper, without assuming the existence of an absolutely universal embedding, we give sufficient conditions for an embedding ε as above to be absolutely universal.

Generalized Chain Geometries and a non-Classical Chain Space

A. Blunck*, H. Havlicek

Abteilung für Lineare Geometrie -Technische Universität
Wiedner Hauptstraße 8–10, A-1040 Wien, Austria
e-mail: blunck@geometrie.tuwien.ac.at

Let R be a ring with 1 and let K be a subfield of R with $1 \in K$. The *generalized chain geometry* over (K, R) is the incidence structure $\Sigma(K, R)$ whose point set is the projective line over R and whose chains are the K-sublines. If R is a K-algebra, then $\Sigma(K, R)$ is a *chain geometry* and satisfies the axioms of a *chain space*. However, $\Sigma(K, R)$ can also be a chain space if R is not a K-algebra; it suffices that the multiplicative group K^* is normal in R^*. We present an example of a finite generalized chain geometry, with 35 points and 56 chains, that is a chain space but is not isomorphic to any chain geometry.

Results obtained in the course of the FWF-project *Chain Geometries over Skew Fields* (M529-MAT/M574-MAT).

Difference Families and Optimization

I. Bluskov

Department of Mathematics and Computer Science
University of Northern British Columbia
Prince George, B.C., CANADA
e-mail: bluskovi@unbc.ca

Let $B = [b_{ij}]$ be an $n \times k$ matrix with entries in Z_v. If the multiset

$$\{b_{ij} - b_{is} |\ j \neq s,\ 1 \leq j \leq k,\ 1 \leq s \leq k,\ 1 \leq i \leq n\}$$

contains every nonzero element of Z_v exactly λ times, then the existence of B implies the existence of a 2-(v, k, λ) cyclic design (cyclic BIBD). In this case, the group Z_v is a subgroup of the group of automorphisms of the BIBD. We present an optimization algorithm for finding such matrices. Modifications of this algorithm can be applied in the search for 2-(v, k, λ) designs having Z_l, $l < v$, as a subgroup of the group of automorphisms. The algorithms have been successfully applied in recent research on BIBD's.

Collineation Groups of Finite Planes: Any Progress?

A. Bonisoli

Dipartimento di Matematica - Università della Basilicata
via N.Sauro 85, 85100 Potenza (Italy)
e-mail: bonisoli@unibas.it

It has been remarked several times that the role of the classification of finite simple groups in the study of automorphism groups of finite geometric structures is at least two–fold. On the one hand it often gives relevant structural information on the groups as such. On the other hand if the investigation of our favorite geometric or combinatorial object involves some finite simple group, it is often possible to discard many candidates just by scanning the list on the basis of little extra information. The latter approach is mostly regarded as a "final resource" when no better ideas are available, since it requires a lot of work. Furthermore, the results that one gets usually lack the elegance and beauty of most classical theorems of the 50's and 60's, which were generally based on a fine analysis of the geometric situation.
In this talk I want to illustrate some results that have been obtained for finite planes in recent years, under the assumption that the collineation group fixes some "non–linear" object like an oval, a hyperoval or a unital. The crucial role of central collineations is emphasized.

1 Introduction

It has been remarked several times that the role of the classification of finite simple groups in the study of automorphism groups of finite geometric structures is at least two–fold. On the one hand it often gives relevant structural information on the groups as such. On the other hand if the investigation of our favorite geometric or combinatorial object involves some finite simple group, it is often possible to discard many candidates just by scanning the list on the basis of little extra information. The latter approach is mostly regarded as a "final resource" when no better ideas are available, since it requires a lot of work. Furthermore, the results that one gets might lack the elegance and beauty of most classical theorems of the 50's and 60's, which were generally based on a fine analysis of the geometric situation. This analysis often reveals the presence of additional properties that the finite simple group must have. It allows quite often the application of structural results which precede the classification theorem.

In the past few years I have started studying collineation groups of planes fixing an oval or a hyperoval. The survey [22] was devoted to the subject of ovals in finite planes from various points of view. Section 4 of that paper was focusing on collineation groups of arbitrary finite planes fixing an oval. Perhaps the most satisfactory general result that is quoted there is the classification of non–abelian simple collineation groups fixing an oval in planes of odd order, a good example for the situation illustrated above. Theorem A in [6] shows that the only possibility is $PSL(2,q)$ with q odd ≥ 5. The proof of this result does not require the full classification of finite simple groups, but only the classification given in [25] of those finite simple groups in which the largest size of an elementary abelian 2–subgroup is 8.

After the appearance of the survey [22] some further results have been obtained for collineation groups fixing an oval or a hyperoval: in this paper I want to illustrate some of the key ideas and point out in particular that the role of central collineations is as crucial as ever.

Planes of odd order. Let π be a finite projective plane of odd order n with an oval Ω. Let G be a collineation group of π fixing Ω. Using some basic properties of involutory homologies and Baer involutions fixing Ω, it was proved in [4] that an elementary abelian 2–subgroup of G must have order at most 8. I have already remarked in the Introduction the role of this property in proving that the assumption G non–abelian simple with $n \geq 5$ forces G to be isomorphic to $PSL(2,q)$ for some odd $q \geq 5$, see [6]. As a matter of fact this same property was essential in the analysis of the case where G acts primitively on Ω: that was the main concern of the paper [4] and the answer is that π is always desarguesian and G contains $PSL(2,n)$ in its natural 2–transitive permutation representation on the points of the conic Ω, with the unique exception of $n = 9$, in which case G might only contain $PSL(2,5)$ in its primitive permutation representation of degree 10 (which is not 2–transitive).

Little is known in general on how $PSL(2,q)$ can act as a collineation group of a finite plane of order $n \neq q$. Despite the quoted result [6], little is known even if it is assumed that n is odd and $PSL(2,q)$ fixes an oval. We do know that this situation may well occur for $n \neq q$ in a desarguesian plane. We have in fact Alt(5) $\cong PSL(2,5)$ and Alt(5) is a subgroup of $PSL(2,n)$ for infinitely many odd prime power values of n, see [19, II§8.27]. It can also happen that Alt(5) is transitive on the points of the conic ($n = 19$ is one possibility).

Examples in non–desarguesian planes do exist. The paper [7] starts from the observation that a Room oval in the Hughes plane of order q^2 (see [24]) is fixed by a collineation group isomorphic to $PSL(2,q)$, in which all involutions are homologies. This situation is then considered for an arbitrary plane of order q^2. Special attention is devoted to the generalized Hughes planes: those of order 25 and 49 do furnish examples.

A collineation group of a projective plane is said to be irreducible if it fixes no point, line or triangle. The notion of an irreducible collineation group for an arbitrary finite projective plane was highlighted by the work of Hering [18]. The knowledge of the structure of irreducible collineation groups of finite projective planes is sufficiently satisfactory for groups containing non–trivial perspectivities. An important role is played by the so called Hering minimal subplane, that is the subplane generated by the centers and axes of the non–trivial perspecticvities in the group. In particular the induced action on this subplane is strongly irreducible, which means it is irreducible and there is no fixed proper subplane either.

As a matter of fact, much of the work involved in the classification theorems [4] and [6] was to reduce the problem to the case of a group acting irreducibly on a plane. With these techniques the paper [6] yields some progress in the case of an oval Ω in a projective plane π of order $n \equiv 1 \mod 4$ admitting a collineation group G acting transitively on the oval, in particular if G is "minimal" with respect to this property.

The results on irreducible collineation groups are important also for the more recent paper [8], which, as the title reveals, is an attempt to determine the structure of G without any extra assumption on the action of the group on the oval. The description of a 2–group containing non–trivial homologies is rather complete and that knowledge allows the determination of the generalized Fitting subgroup of $G/O(G)$. The general lack of information on collineations of odd prime order fixing Ω is the main reason why at the moment there seems to be no way of controlling the structure of $O(G)$ (the largest normal subgroup of odd order of G).

In the paper [10], on which I reported at the "Combinatorics 98" conference, the point of view is to try to apply the theory of irreducible collineation groups "as is" to irreducible collineation groups fixing an oval in a plane of odd order. As usual the major difficulty is that of finding reasonable sufficient conditions for the existence of non–trivial perspectivities, involutory homologies in this case. Here, the condition $|G| \equiv 0 \mod 4$ does the job. Sufficiently satisfactory is the classification of "minimal" irreducible collineation groups fixing an oval, where minimal means no proper subgroup is irreducible. Here again, if the group order is assumed to be divisible by 4, we have again the groups $PSL(2,q)$, q odd, with the further restriction that q must be a prime, $q^2 \not\equiv 1 \mod 4$.

I have already remarked that if G acts primitively on the points points of Ω, then the situation is completely determined and a lot of information is available even if the action is only assumed to be transitive. What if we allow more than one orbit? Especially interesting seems to be the case of precisely two orbits, one of which shrinks to a single point and the other one is such that the induced action is primitive or even 2–transitive. Examples for this situation occur in desarguesian planes but also in non–desarguesian translation planes coordinatized by commutative twisted fields, see [2] and [16]. It is proved in [16] that if π is a translation plane and Ω touches the line at infinity at one point and G acts 2–transitively on the affine points of Ω then the plane is coordinatized by a commutative semifield and the oval arises from an orthogonal polarity. It may appear almost superfluous to remark that also the proof of this result relies on the existence of involutory homologies at some stage. The question whether the given property characterizes the known examples is quite natural.

The collineation group G acts not only on the points of the oval Ω, but also on the set of all external points and on the set of all internal points. Both actions are faithful and so G has two more permutation representations. In the paper [17], starting from this observation, it is suggested to try to impose some conditions on one or both of these actions and see if some classification result can be obtained. While it is fairly easy to see that transitivity on external points amounts to 2–transitivity on the points of the oval, it is somewhat surprising that a classification is possible under the assumption of a transitive action on internal points. This is the main result of the paper [17] and the outcome is that either the action on Ω is 2–transitive or there is a fixed point and a primitive orbit. The action on the primitive orbit is even 2–transitive as soon as the involutions in the group are homologies. The description of the possibilities for the group G is also fairly detailed.

2 Planes of even order

. A first basic observation is that a collineation group fixing an oval in a finite projective plane of even order must also fix the nucleus of the oval. In particular, the group is certainly not irreducible and so there is no chance of applying Hering's theory here.

On the other hand irreducible collineation groups fixing a hyperoval do exist in desarguesian planes: the full collineation group of the Lunelli–Sce–Hall hyperoval acts irreducibly on the desarguesian plane of order 16. An attempt to draw the consequences of Hering's classification theorem for irreducible collineation groups with an invariant hyperoval has been carried out in [13]. Apart from the usual problem of finding reasonable conditions which guarantee the existence of perspectivities (involutory elations in the case under consideration), extra difficulties arise from the fact that $n + 2$ (the number of points of the hyperoval) may have the prime factor 3 in common with $n^2 + n + 1$ (the total number of points of the plane).

It was proved in [1] that the plane of order 2 and that of order 4 are the only planes admitting a hyperoval which is fixed by a collineation group acting 2–transitively on its points. If the action is only assumed to be transitive but we add the assumption that the group–order be divisible by 4, then the result of [5] tells us that further possibilities may only occur in planes of order 16 (and the Lunelli–

Sce–Hall hyperoval is again an example in $PG(2,16)$). Again Hering's results are relevant in the proof of these properties.

I find it somehow peculiar that in the effort of applying correctly the heavy machinery of group theory to our situation, some elementary but very useful properties of single collineations fixing a hyperoval may go undetected: the paper [23] concentrates on hyperovals in desarguesian projective planes, but contains a proof of the general property that an (involutory) elation fixing a hyperoval in a projective plane of even order $n > 2$ must have a secant line as axis and hence induce an even permutation on the points of the hyperoval.

The previous discussion shows that transitive hyperovals are pretty much under control. What about transitive ovals in even order planes? It may appear strange that the situation here is way out of control even for a 2–transitive action.

Let π be a finite projective plane of even order n with an oval Ω. Let G be a collineation group of π fixing Ω and acting 2–transitively on its points. Denoting by Δ the set of all involutory elations in G, Theorem C in [3] shows that three possibilities arise.

(i) The group G also fixes a line ℓ which is external to Ω, the subgroup $\langle\Delta\rangle$ is the semidirect product of $O(\langle\Delta\rangle)$ by a group of order 2, $|\Delta| = n+1$ and G contains no Baer involutions.

(ii) The plane π is desarguesian, Ω is a conic and $\langle\Delta\rangle = PSL(2,n)$.

(iii) We have $n = 2^{2r}$ for an odd integer $r \geq 3$ and $\langle\Delta\rangle$ is the Suzuki group $\mathrm{Sz}(2^r)$ acting on Ω in its natural 2–transitive permutation representation.

Apart from the trivial case $n = 2$, a unique example is known for case (i), namely for $n = 4$. Using some features of the action of G on the plane π, namely the existence of a G–invariant family of pairwise disjoint ovals (including Ω) with common nucleus, it was proved in [11] that either $n \in \{2,4\}$ or $n \equiv 0 \mod 8$ and the Sylow 2–subgroups of G are generalized quaternion groups. In the paper [9] I was pushing the analysis of G somewhat further by applying a theorem of Hering classifying 2–transitive groups with a regular normal subgroup and such that no involution fixes more than one point: it turns out that G must act as a subgroup of $A\Gamma L(1,q)$ in its natural permutation representation.

It was proved in [20] and [21] that possibility (iii) occurs in the dual Lüneburg plane of order 2^{2r}. The question addressed in [12] is whether occurrence (iii) characterizes the dual Lüneburg plane of order 2^{2r}. The approach developed there is based on the possibility of describing a projective plane π of even order possessing an oval Ω by means of the one–factorizations of the complete graphs arising from the lines of π which are tangent to Ω. This observation was stated in the language of minimal edge colorings in [15]. Within this context the idea essentially coincides with the approach of Buekenhout ovals developed in [14]. We were able to determine all one–factors which may occur in such one–factorizations, obtaining

in particular all one–factorizations of the complete graph on 2^{2r} vertices admitting the one–point–stabilizer of $\mathrm{Sz}(2^r)$ as an automorphism group and having $2^r - 1$ prescribed one–factors, namely those arising from the involutions in the group.
This construction has some interest from the point of view of graph theory: there are not too many infinite families of one–factorizations of complete graphs for which a non–trivial automorphism group is explicitely known.
In general, the problem of determining when two of the above one–factorizations may arise from distinct lines in the same plane remains open. In the language of Buekenhout ovals, that amounts to the problem of reconstructing exterior lines in the so called "ambient" of the B–oval. Nevertheless, the method seems adequate for computer calculations, which we have actually performed in the smallest case $r = 3$: the dual Lüneburg plane is indeed the only plane of order 64 for which possibility (iii) occurs.
It would perhaps be appropriate to conclude with the remark that I am aware of no example of a plane of order $n \neq 2^{2r}$ on which $\mathrm{Sz}(2^r)$ can act as a collineation group, a situation differing somewhat from that of $PSL(2, q)$.

References

[1] V. Abatangelo, Doubly transitive $(n + 2)$–arcs in a projective plane of even order n, J. Combin.Theory Ser. A 42 (1986) 1–8.

[2] V. Abatangelo, M.R. Enea, G. Korchmáros, B. Larato, Ovals and unitals in commutative twisted field planes, Discrete Math. 208/209 (1999) 3–8.

[3] M. Biliotti, G. Korchmáros, Collineation groups strongly irreducible on an oval, Ann. Discrete Math. 30 (1986) 85–98.

[4] M. Biliotti, G. Korchmáros, Collineation groups which are primitive on an oval of a projective plane of odd order, J. London Math. Soc. 33 (1986) 525–534.

[5] M. Biliotti, G. Korchmáros, Hyperovals with a transitive collineation group, Geom. Dedicata 24 (1987) 269–281.

[6] M. Biliotti, G. Korchmáros, Collineation groups preserving an oval in a projective plane of odd order, J. Austral. Math. Soc. Ser. A 48 (1990) 156–170.

[7] M. Biliotti, G. Korchmáros, Projective planes with non–abelian simple collineation group fixing an oval, Arch. Math. (Basel) 60 (1993) 300–304.

[8] M. Biliotti, G. Korchmáros, The Structure of a Collineation Group Preserving an Oval in a Projective Plane of Odd Order, Geom. Dedicata 57 (1995) 73–89.

[9] A. Bonisoli, On a Theorem of Hering and Two–Transitive Ovals with a Fixed External Line, in: "Mostly Finite Geometries", N.L. Johnson ed., Lect. Notes Pure Appl. Math., vol. 190, Dekker, New York 1997, pp. 169–183.

[10] A. Bonisoli, M.R. Enea, G. Korchmáros, Irreducible Collineation Groups Fixing an Oval, Abh. Math. Sem. Univ. Hamburg 69 (1999) 259–264.

[11] A. Bonisoli, G. Korchmáros, On two–transitive ovals in projective planes of even order, Arch. Math. 65 (1995) 89–93.

[12] A. Bonisoli, G. Korchmáros, Suzuki groups, one–factorizations and Lüneburg planes, Discrete Math. 161 (1996), 13–24.

[13] A. Bonisoli, G. Korchmáros, Irreducible collineation groups fixing a hyperoval, preprint.

[14] F. Buekenhout, Etude intrinsèque des ovales, Rend. Mat. (5) 25 (1966) 333–393.

[15] P.J. Cameron Minimal edge–colourings of complete graphs, J. London Math. Soc. 11 (1975), 337–346.

[16] M.R. Enea, G. Korchmáros, Ovals in commutative semifield planes, Arch. Math. 69 (1997) 259–264.

[17] M.R. Enea, G. Korchmáros, $\mathcal{I}$–Transitive Ovals in Projective Planes of Odd Order, J. Algebra 208 (1998) 604–618.

[18] C. Hering, On the structure of finite collineation groups of projective planes, Abh. Math. Sem. Univ. Hamburg 49 (1979) 155–182.

[19] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.

[20] W.M. Kantor, Symplectic Groups, Symmetric Designs and Line Ovals, J. Algebra 33 (1975) 43–58.

[21] G. Korchmáros, Le ovali di linea del piano di Lüneburg d'ordine 2^{2r} che possono venir mutate in sé da un gruppo di collineazioni isomorfo al gruppo semplice Sz(2^r) di Suzuki, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Mem. (8) Mat. Appl. 15 (1979) 295–315.

[22] G. Korchmáros, Old and new results on ovals in finite projective planes, in "Surveys in Combinatorics", A.D. Keedwell ed., LMS Lecture Notes Ser., vol. 166, Cambridge Univ. Press, Cambridge 1991.

[23] T. Penttila, G.F. Royle, On hyperovals in small projective planes, J. of Geometry 54 (1995) 91–104.

[24] T.G. Room, Polarities and ovals in the Hughes plane, J. Austral. Math. Soc. Ser. A 13 (1972) 196–204.

[25] G. Stroth, Über Gruppen mit 2–Sylow Durchschnitten vom Rang ≤ 3, J. Algebra 43 (1976) 398–456.

Small Defining Sets for PG(2,q)

E. Boros, T. Szőnyi*

University of Budapest - Hungary
e-mail: szonyi@cs.elte.hu

A *defining set* of a $2-(v,k,\lambda)$ design $(\mathcal{P},\mathcal{B})$ is a set $\mathcal{B}^*$ of blocks with the following property: if $\mathcal{B}^* \subset \mathcal{B}'$ and $(\mathcal{P},\mathcal{B}')$ is also a $2-(v,k,\lambda)$ design, then $\mathcal{B}=\mathcal{B}'$. Intuitively, this means that the blocks in $\mathcal{B}^*$ determine uniquely the remaining blocks of the design. Gray, Hamilton, and O'Keefe connected the notion of defining sets to nuclei of $(q+1)$-sets in $\mathrm{PG}(2,q)$, and used a result of Blokhuis and Wilbrink to show that the secants and tangents of a q-arc form a defining set. This defining set has $q(q+3)/2$ lines. In this talk we show that there are defining sets with $|\mathcal{B}^*| = o(q^2)$. Both explicit constructions and probabilistic results will be mentioned.

Embeddings of PG (3,q) in Hughes Planes of Order q^4

J.M.N. Brown

York University - Toronto, Ontario M3J 1P3, Canada
e-mail: juliamnb@yorku.ca

We describe a two-to-one incidence preserving map from a pre-incidence system onto $\mathrm{PG}(2, q^2)$ and another two-to-one incidence preserving map from the same pre-incidence system onto the regular Hughes plane of order q^2 (q odd). This furnishes a representation of finite regular Hughes planes. Using this representation, we define a family of embeddings of $\mathrm{PG}(3, q)$ in $\mathrm{Hu}(q^4)$. This family includes at least two nonisomorphic embeddings.

Graphs which are Both H_1 and H_2-decomposable

D. Bryant, B. Maenhaut*

The Open University - Milton Keynes, UK
e-mail: B.M.Maenhaut@open.ac.uk

A graph G is said to be H-decomposable if there exists a collection of subgraphs of G, each isomorphic to H, which partition the edge set of G. If G is H-decomposable, we say that $H|G$. In this talk we consider the question: given two graphs H_1 and H_2, for which values q does there exist a graph G having q edges such that $H_1|G$ and $H_2|G$? The problem will be considered for the cases when H_1 and H_2 are both cycles and when H_1 and H_2 are both complete graphs.

Incidence Geometry and Finite Groups

F. Buekenhout

Bruxelles - Belgium

e-mail: fbueken@ulb.ac.be

The talk is mainly motivated by the theory of buildings and the geometry of exceptional objects, especially sporadic groups and groups with a sporadic behavior. Many of the conceptual developments used here are due to Jacques Tits over the period 1956-1974. Incidence geometry can be briefly defined as the study of multipartite graphs (or numbered simplicial complexes) with inspiration from classical projective and affine geometry, from polytopes and...buildings. Every incidence geometry determines a diagram namely a generalization of a Coxeter diagram and every diagram defines a class of incidence geometries. If an incidence geometry is provided with a group G of automorphisms which is large enough to be transitive on the maximal cliques then the geometric structure can be completely described in terms of G and a collection of subgroups. The process can be reversed. Starting from a group G we can compute all of its geometries satisfying suitable conditions and we may study them. This program has been applied in various ways by various teams in Brussels (including M.Dehon, D.Leemans, Ph.Cara) to reasonably small simple (and other) groups in particular the groups M_{11}, M_{12}, J_1 and J_2 with the help of MAGMA. It has provided roughly speaking about 1000 highly regular new geometries, gems that we believe to be of high potential interest.

References

[14] F. Buekenhout (editor): *Handbook of Incidence Geometry. Buildings and Foundations*, North-Holland. Amsterdam 1995. (1432 pages).

[15] F. Buekenhout: *The rise of Incidence Geometry and Buildings in the 20th Century*, In PL.Butzer, H.Th.Jongen, W.Oberschelp (editors), *Charlemagne and his Heritage, 1200 Years of Civilization and Science in Europe*, vol 2, Brepols, Turnhout, 1998. 235-256.

[16] J. Stillwell: *Exceptional objects*, Amer. Math. Monthly, 105 (1998) 850-858.

A description of any Rregular or 1-rotational Design by Difference Methods

M. Buratti
Dipartimento di Matematica e Informatica - Università di Perugia, Italy.
e-mail: buratti@mat.uniroma1.it

An interesting combinatorial item is the construction of 2-designs (BIBD's) admitting an automorphism group acting sharply transitively on its points (regular BIBD's) and, also, the construction of BIBD's with an automorphism group fixing one point and acting sharply transitively on the others (1-rotational BIBD's).
In the literature there are difference methods providing a description of some, *but not all*, regular or 1-rotational BIBD's.
Since a $2-(v,k,\lambda)$ design may be viewed as a decomposition of λK_v (the λ-multiple of the complete graph on v vertices) into copies of K_k, one may ask, more generally, a possible description, in terms of differences, of any regular or 1-rotational graph decomposition.
Still more generally, one may ask such a description for any regular or 1-rotational *hypergraph decomposition*, thus, in particular, for regular or 1-rotational $t-(v,k,\lambda)$ designs with $t>2$.
Here this aim is successfully achieved by means of a description that allows, concretely, to get many new regular or 1-rotational graph and hypergraph decompositions.

1 Preliminaries

Before recalling the basic definitions concerning designs, it is convenient to speak a little about *multisets*. Given a set X, a multiset on X is a list $L=(x_1,...,x_n)$ of elements from X where repetitions are allowed. Thus, formally, a multiset L on X may be viewed as a map $\mu_L : X \longrightarrow N$ ($N=\{0,1,2,...\}$ being the set of natural numbers) where $\mu_L(x)$ is the *multiplicity of* x in L.

Then, since the set of maps from a set A to a set B is often denoted by B^A, we may denote the set of multisets on X by N^X.

L' is a *submultiset* of a multiset $L \in N^X$ if L' is a sublist of L, namely, if we have $\mu_{L'}(x) \leq \mu_L(x)$ for every element $x \in X$.

If L_1, ..., L_t are multisets on X, then their *strong union* is the multiset $L_1 \underline{\cup} ... \underline{\cup} L_t$ obtained by linking together the L_i's. In particular, by $\underline{t}L$ I denote the strong union of t copies of the multiset L.

Now, let G be a group acting on a set X and let $L = (x_1, ..., x_n)$ be a multiset on X. We say that L is *G-invariant* if we have $(x_1^g, ..., x_n^g) = L$ for any $g \in G$. The *development of L under G* is the multiset $dev_G L = dev_G(x_1) \uplus ... \uplus dev_G(x_n)$ where, for $i = 1, ..., n$, $dev_G(x_i)$ is the G-orbit of x_i.

If L is G-invariant, it is obvious that we have $L = dev_G L'$ for a suitable submultiset L' of L.

I will often speak of $devL$ understanding which is the group G with respect to the development is done.

Throughout the paper G will denote an additive group while G^+ will denote the semigroup associated with G with elements in $G \cup \{\infty\}$, ∞ being a symbol not in G, and composition law obtained by extending that of G by the rule $\infty + g = g + \infty = \infty \; \forall g \in G$.

Speaking of the action of G on G^+, I always mean the natural action defined by $g(x) = x + g$ $(g \in G, x \in G^+)$. Also, speaking of the action of G on 2^{G^+} or N^{G^+}, I always mean the action of G on these sets induced by the action of G on G^+ defined above.

A $t-(v, k, \lambda)$ *design* is a pair $(V, \mathcal{B})$ where V is a set of v *points* and $\mathcal{B}$ is a multiset of k-subsets (*blocks*) of V with the property that any t-subset of V is contained in exactly λ blocks.

Such a design is said to be *complete* when $\mathcal{B} = \binom{V}{k}$.

An incomplete 2-design is said to be a *balanced incomplete block design* (BIBD).

A *t-wise balanced design* is defined as a t design where, however, one also allows that the blocks may have non-constant size. In this case one speaks of a $t-(v, K, \lambda)$ design where K is the set of block-sizes in the design. In particular, a *pairwise balanced design* (PBD) with $\lambda = 1$ is a *linear space.*

A *groop divisible design* (GDD) of *index* λ is a point-block structure $(V, \mathcal{B})$ together with a partition of V into *groops* with the properties that each block meets each group in at most one point and that any two points belonging to distinct groops lie, together, in exactly λ blocks.

In particular, by (v, n, K, λ)-GDD I mean a GDD of index λ with v points, block-sizes belonging to K, and where each group has size n.

It is clear that a (v, K, λ)-PBD may be viewed as a $(v, 1, K, \lambda)$-GDD.

A (v, n, k, λ)-GDD where $nk = v$ is a *transversal design* and is denoted by $\text{TD}_\lambda(k, v)$. In this case each block meets each group in exactly one point.

An automorphism group of a design $(V, \mathcal{B})$ is a group of bijections on V that fixes $\mathcal{B}$.

One says that a design is *regular* or *1-rotational* when it possesses an automorphism group acting sharply transitively on its points or, respectively, fixing one point and acting sharply transitively on the others.

When one speaks of a cyclic, (resp. abelian, non-abelian, ...) design one means a regular design under a group having the respective property. Analogously, we may speak of a cyclic, abelian, non-abelian, ... 1-rotational design with the obvious meaning.

There is an extensive literature concerning the construction of regular BIBD's by *difference methods*.

Undoubtely, the most known method is that concerning the construction of regular *symmetric* BIBD's (BIBD's with as many points as blocks). The existence of a regular symmetric (v, k, λ)-BIBD is equivalent to that of a (v, k, λ) *difference set*. This is a k-subset B of a group G with the property that its *list of differences* $\Delta B = (b - c \,|\, b, c \in B, b \neq c)$ covers $G - \{0\}$ exactly λ times. The resultant symmetric design is the pair $(G, devB)$. For a good survey on difference sets see [11].

It is an easy matter to check that no non-trivial 1-rotational symmetric design exists.

This paper does not allow to get new informations about symmetric designs.

There are many approaches to get regular or 1-rotational BIBDs, PBDs and GDDs by difference methods. The *difference families* introduced by Bose [3] allow to describe, in terms of differences, any BIBD which is regular under a group G acting semiregularly on its blocks. Analogously, *relative difference families* [4] - that naturally generalize *relative difference sets* [16] - describe GDD's that are regular under a group G acting semiregularly on its blocks. The approaches of [5] and [7] allow to describe, respectively, any abelian linear space and any abelian 1-rotational linear space. Some explicit constructions for non-abelian BIBD's may be found in [15].

Concerning the construction by difference methods of regular t-designs with $t > 2$ there is very few material in the literature. I am only aware of some papers by Beth and Kolher (see [2]). These papers essentially give a description in terms of differences of some cyclic t-designs with $t > 2$.

No description by difference methods of 1-rotational t-designs with $t > 2$ is known to myself.

Before speaking of *graph and hypergraph decompositions* I recall some terminology about graphs and hypergraphs.

A hypergraph is a pair $X = (V, \mathcal{E})$ where V is a set of *vertices* and $\mathcal{E}$ is a multiset of subsets (*edges*) of V. It is *simple* when it does not have multiple edges and each edge has size at least two. It is is a *graph* when all its edges have size 2.

A *hypergraph* B is a *subhypergraph* of a hypergraph X if we have $V(B) \subset V(X)$ and $\mathcal{E}(B) \subset \mathcal{E}(X)$.

Let B be a subhypergraph of X and let $v \in V(B)$. The multiset of *neighbours* of v in B is the multiset $N_B(v) \in N^{V(B)}$ in which the multiplicity of each $w \in V(B)$ is the multiplicity of $\{v, w\}$ in $\mathcal{E}(B)$. Its size is the *degree* of v in B and is denoted by $deg_B(v)$.

An automorphism group of a hypergraph X is a group of bijections on $V(X)$ preserving $\mathcal{E}(X)$.

Two hypergraphs X and X' are *isomorphic* when there exists a bijection (*isomorphism*) between $V(X)$ and $V(X')$ mapping $\mathcal{E}(X)$ into $\mathcal{E}(X')$.

A hypergraph X is *sharply-vertex-transitive* (*1-rotational*) under a group G if it admits G as an automorphism group acting regularly on $V(X)$ (fixing one vertex and acting regularly on the others).

I denote by t-$K(V)$ the complete t-*uniform* hypergraph with vertex-set V, i.e., the hypergraph $(V, \binom{V}{t})$. By t-K_v I mean a hypergraph $(V, \binom{V}{t})$ where V is a non-specified v-set. When $t = 2$ I will simply write $K(V)$, K_v instead of 2-$K(V)$ and 2-K_v.

The *m-multiple* of a hypergraph X is the hypergraph $\underline{m}X = (V(X), \underline{m}\mathcal{E}(X))$.

A *decomposition of a graph* X into copies of graphs belonging to an assigned set $\mathcal{Y}$ is a multiset $\mathcal{D} = (B_1, ..., B_b)$ of subgraphs of X each isomorphic to some graph of $\mathcal{Y}$ and such that $\mathcal{E}(B_1) \underline{\cup} \mathcal{E}(B_2) \underline{\cup} ... \underline{\cup} \mathcal{E}(B_b) = \mathcal{E}(X)$. One also says that $\mathcal{D}$ is a $(X, \mathcal{Y})$-design.

Of course this concept may be extended to hypergraphs in the obvious way. Thus we may speak of a $(X, \mathcal{Y})$-design as a decomposition of a hypergraph X into copies of hypergraphs belonging to an assigned family $\mathcal{Y}$.

In the case where $\mathcal{Y} = \{Y\}$ consists of a single hypergraph one simply speaks of a (X, Y)-design.

An automorphism group of a $(X, \mathcal{Y})$-design $\mathcal{D}$ is a group of bijections on $V(X)$ fixing $\mathcal{D}$.

A (X, Y)-design is *regular* (*1-rotational*) if it admits an automorphism group acting sharply transitively on $V(X)$ (fixing one vertex and acting sharply transitively on the others).

Observe that a (v, k, λ)-BIBD is equivalent to a $(\underline{\lambda}K_v, K_k)$-design.

Much more generally, a $t - (v, k, \lambda)$ design is equivalent to a (X, Y)-design where $X = \underline{\lambda}(t\text{-}K_v)$ and $Y = t\text{-}K_k$.

Thus, a regular (1-rotational) $t - (v, k, \lambda)$ design may be viewed as a regular (1-rotational) t-$(\underline{\lambda}K_v), K_k)$-design.

In the literature one can find many regular or 1-rotational $(\lambda K_v, Y)$-designs obtainable by difference methods (see, e.g. [17], [18]). Anyway, curiously, an explicit systematic description of these methods seems to be lacking. The situation is still worst for arbitrary $(X, \mathcal{Y})$-designs.

The purpose of this paper is to give a general method able to describe, in terms of differences, any regular or 1-rotational $(X, \mathcal{Y})$-design.

In my opinion the method is promising since, in many cases, it allows to construct nice designs by hand. So, I believe that a "clever" use of this method, possibly together with the help of a computer, may lead to lots of designs previously unknown.

Here, I report the descriptions starting from that of a regular or 1-rotational BIBD to arrive to that, very general, of a regular or 1-rotational $(X, \mathcal{Y})$-design where X and $\mathcal{Y}$ are arbitrary.

The last description includes all the previous ones. The reason for which I preferred to proceed by dealing, in this order, with BIBD's, PBD's, GDD's, t-designs with $t > 2$, graph decompositions and, finally, hypergraph decompositions, is that I thought that an immediate presentation of the last description could appear extremely heavy.

I will give detailed proofs in a future paper [6]. No proof will be reported here. I only give the descriptions and, case by case, easy examples to clarify them.

2 Regular or 1-rotational BIBD's, PBD's and GDD's

Given a group G, the *list of differences* of a k-subset B of G^+ is the multiset ΔB on $G^+ - \{0\}$ defined as follows:

$$\Delta B = (b - c \,|\, b, c \in B, b \neq c \neq \infty)$$

Note that we have:

$$|\Delta B| = \begin{cases} k(k-1) & \text{if } \infty \notin B \\ (k-1)^2 & \text{if } \infty \in B \end{cases}$$

In order to achieve a description of any regular or 1-rotational BIBD by difference methods, it is convenient to consider a sublist of ΔB.

Let G_B be the G-stabilizer of B, i.e., $G_B = \{g \in G \, : \, B + g = B\}$. One may easily see that the multiplicity of each non-zero element of G^+ in ΔB is divisible by $|G_B|$ so that it makes sense to speak of the list

$$\partial B = \frac{1}{|G_B|} \Delta B$$

that I call the *list of partial differences* of B. Equivalently, one may see that

$$\partial B = (b - \ell \,|\, \ell \in L_B, b \in B - \{\ell\})$$

where L_B is a system of representatives for the G_B-orbits that are contained in B, i.e., L_B is a system of representatives for the left cosets of G_B in G that are contained in B.

Note that we have $\partial B = \Delta B$ if and only if B has trivial stabilizer. Also, note that:

$$|\partial B| = \begin{cases} \dfrac{k(k-1)}{d} & \text{if } \infty \notin B \\ \dfrac{(k-1)^2}{e} & \text{if } \infty \in B \end{cases}$$

where d is a divisor of $gcd(k, |G|)$ while e is a divisor of $gcd(k-1, |G|)$.

Concerning the multiplicity of ∞ in ∂B, we have:

$$\mu_{\partial B}(\infty) = \begin{cases} 0 & \text{if } \infty \notin B \\ \frac{k-1}{|G_B|} & \text{if } \infty \in B \end{cases}$$

In view of the forthcoming theorems, these simple informations about $|\partial B|$ and $\mu_{\partial B}(\infty)$ may be very useful whenever we want to construct a regular or 1-rotational design.

More generally, given a multiset $\mathcal{F} = (B_1, ..., B_n)$ of subsets of G^+, I define the *list of partial differences of* $\mathcal{F}$ by

$$\partial\mathcal{F} = \partial B_1 \underline{\cup} ... \underline{\cup} \partial B_n$$

Definition 2.1 *Let G be a group, let $\Gamma = G$ or G^+, and let K be a set of positive integers. A (Γ, K, λ) partial difference family (PDF) is a multiset $\mathcal{F}$ of subsets of Γ with sizes from K such that $\partial\mathcal{F} = \underline{\lambda}(\Gamma - \{0\})$. If $|\Gamma| = v$ we also say that $\mathcal{F}$ is a (v, K, λ)-PDF in Γ.*

A (Γ, k, λ)-PDF is a (Γ, K, λ)-PDF where $K = \{k\}$.

Theorem 2.2 *Let G be a group and let $\Gamma = G$ $(\Gamma = G^+)$ with $|\Gamma| = v$. Let $\mathcal{F}$ be a multiset of subsets of Γ. Then $(\Gamma, dev\mathcal{F})$ is a regular (1-rotational) (v, K, λ)-PBD under G if and only if $\mathcal{F}$ is a (v, K, λ)-PDF in Γ.*

Now note that the block-multiset of any design admitting an automorphism group G is obtainable as development under G of a suitable submultiset $\mathcal{F}$ of $\mathcal{B}$. Thus we may state:

Theorem 2.3 *The existence of a regular (1-rotational) (v, K, λ)-PBD under G is completely equivalent to the existence of a (v, K, λ)-PDF in G (G^+).*

In particular, we have:

Theorem 2.4 *The existence of a regular (1-rotational) (v, k, λ)-BIBD under G is completely equivalent to the existence of a (v, k, λ)-PDF in G (G^+).*

The term *partial difference family* has been also used by Abel [1]. He defines a PDF in G as a multiset of subsets of a group whose development under G itself is the block-multiset of a BIBD. The *uniform* PDF's as defined in this section are, a posteriori, the same PDF's of Abel in view of Theorem 2.2. Anyway, in the definition of Abel it does not appear clear how this term is so appropriate. Also he does say how to check whether a given multiset of subsets of a group is a PDF.

Concerning GDD's, we observe that no 1-rotational GDD (that is not a BIBD) may exist. Instead regular GDD's exist but, as observed in [4], their groop size is constant. In fact, identifying the point-set of a regular GDD under G with G itself and the action of G on its points as the regular right representation of G, we have that its groops are the right cosets of a suitable subgroup of G. The crucial theorem concerning GDD's may be stated as follows.

Theorem 2.5 *The existence of a regular (v, n, K, λ)-GDD under G is completely equivalent to the existence of a $(v, K \cup \{n\}, \lambda)$-PDF in G of type $\mathcal{F} = \underline{\lambda}\{N\} \underline{\cup} \mathcal{F}'$ with N a subgroup of G of order n and all the components of $\mathcal{F}'$ with size $k \in K$. The block-multiset of the GDD generated by such a PDF is $dev\mathcal{F}'$.*

Let us give some explicit constructions in order to clarify the above theorems.

Example 2.6 Consider the set $\mathcal{F} = \{B_1, B_2, B_3, B_4\}$ of 4-subsets of the group $G = Z_{12}$ defined as follows:

$$B_1 = \{0, 3, 6, 9\}, \quad B_2 = \{0, 4, 6, 10\}, \quad B_3 = \{0, 1, 3, 8\}, \quad B_4 = \{0, 3, 4, 5\}$$

The first component B_1 is a subgroup of G so that $G_{B_1} = B_1$ and hence $\partial B_1 = (\pm 3, 6)$.

Then we have $G_{B_2} = \{0, 6\}$; in fact $B_2 = L + \{0, 6\}$ where $L = \{0, 4\}$. Thus we have $\partial B_2 = (b - \ell \mid \ell \in L, b \in B_2 - \{\ell\}) = \pm(4, 2, 6)$.

Finally, both B_3 and B_4 have trivial stabilizer so that

$$\partial B_3 = \Delta B_3 = \pm(1, 3, 4, 2, 5, 5) \qquad \partial B_4 = \Delta B_4 = \pm(3, 4, 5, 1, 2, 1)$$

Linking together the above lists of partial differences, we see that $\partial\mathcal{F} = \underline{3}(G - \{0\})$, i.e., $\mathcal{F}$ is a $(12, 4, 3)$-PDF in Z_{12}. Thus $(Z_{12}, dev\mathcal{F})$ is a cyclic $(12, 4, 3)$-BIBD.

Example 2.7 Let G be the group with elements in the Cartesian product set $Z_2 \times Z_{12}$ and operation law defined by the rule

$$(x, y) + (x', y') = \begin{cases} (x + x', y + y') & \text{if } x' = 0 \\ (x + x', 7y + y') & \text{if } x' = 1 \end{cases}$$

Hence G is a semidirect product of Z_2 and Z_{12}.

Consider the multiset $\mathcal{F} = (B_1, B_2, B_3, B_4)$ of 4-subsets of G^+ defined as follows:

$$B_1 = \{(0,0), (0,4), (0,8), \infty\}, \qquad B_2 = \{(0,0), (0,6), (1,0), (1,6)\}$$

$$B_3 = \{(0,0), (1,3), (0,1), (1,10)\}, \quad B_4 = \{(0,0), (0,2), (0,5), (1,1)\}$$

Note that $B_1 - \{\infty\}$ is the subgroup of order 3 of G so that $G_{B_1} = B_1 - \{\infty\}$ and hence $\partial B_1 = ((0,4),(0,8),\infty)$.

Also, note that B_2 is a subgroup of order 4 of G so that $G_{B_2} = B_2$ and hence $\partial B_2 = ((0,6),(1,0),(1,6))$

Then we have $G_{B_3} = \{(0,0),(1,3)\}$; in fact $B_3 = L + \{(0,0),(1,3)\}$ where $L = \{(0,0),(0,1)\}$. Thus we have

$\partial B_3 = (b - \ell \mid \ell \in L, b \in B_3 - \{\ell\}) = ((0,1),(1,3),(1,10),(0,11),(1,2),(1,9))$.

Finally, B_4 has trivial stabilizer so that

$\partial B_4 = \Delta B_4 = ((0,2),(0,5),(1,1),(0,3),(1,11),(1,8),(0,10),(0,7),(1,5),(0,9),(1,7),(1,4))$

Linking together the above lists of partial differences, we see that $\partial\mathcal{F} = G^+ - \{0\}$, i.e., $\mathcal{F}$ is a $(25,4,1)$-PDF in G^+. Thus $(G^+, dev\mathcal{F})$ is a 1-rotational $(25,4,1)$-BIBD.

When I constructed, by hand, the above design, I was not aware of a paper by Kramer, Magliveras and Mathon [13] where, up to isomorphisms, all $(25,4,1)$-BIBD's with a non-trivial automorphism group are classified. There are exactly 16 such BIBD's and only one of them has full automorphism group of order divisible by 24 (its order is 504). Hence my example provides another presentation (maybe more easy) of that design.

Recall that a *partition* (see [22]) of a group G is a set of subgroups of G intersecting each other in the zero element of G and whose union is G.

Note that such a partition is a $(G,K,1)$-PDF where K is the set of orders of its components. Thus, as a particular consequence of Theorem 2.2 we refind the following very well known result.

Theorem 2.8 *Let G be a group admitting a partition $\mathcal{F}$. Then $(G, dev\mathcal{F})$ is a linear space.*

Now, let G be a Frobenius group with kernel N and complement A. Then the set of conjugates of A together with N form a partition of G. Thus, as a consequence of Theorem 2.5, we refind the following result (see [10]).

Theorem 2.9 *Let G be a Frobenius group of order v with kernel N and complement A of order k. Let $\mathcal{A}$ be the set of conjugates of A. Then $(G, dev\mathcal{A})$ is a $TD_1(k,v)$.*

3 Regular or 1-rotational t-design ($t > 2$)

In order to get a description in terms of differences of regular and 1-rotational t-designs with $t > 2$, I firstly introduce the concept of *list of differences of order n*.

Given a group G, the *list of differences of order* n of a subset B of G^+ is the multiset $\Delta^n B$ on $\binom{G^+-\{0\}}{n}$ defined as follows:

$$\Delta^n B = (X - y \,|\, X \in \binom{B}{n}, y \in B - (X \cup \{\infty\}))$$

Also here one may see that the multiplicity of each n-subset of $G^+ - \{0\}$ in $\Delta^n B$ is divisible by $|G_B|$ so that it makes sense to speak of the list

$$\partial^n B = \frac{1}{|G_B|}\Delta^n B$$

that I call the *list of partial differences of order* n of B and that we can also express in the form

$$\partial^n B = (X - \ell \,|\, X \in \binom{B}{n}, \ell \in L_B - (X \cup \{\infty\}))$$

where L_B is a system of representatives for the left cosets of G_B in G that are contained in B.

More generally, given a multiset $\mathcal{F}$ of subsets of G^+, I call *list of partial differences of order* n of $\mathcal{F}$ the list $\partial^n\mathcal{F}$ defined by $\partial^n\mathcal{F} = \underline{\bigcup}_{B\in\mathcal{F}} \partial^n B$.

It is obvious that $\Delta^1 B$ may be identified with the list ΔB defined in the previous section.

Definition 3.1 *Let G be a group, let $\Gamma = G$ or G^+, and let K be a set of positive integers. A $t-(\Gamma, K, \lambda)$ partial difference family (PDF) is a multiset $\mathcal{F}$ of subsets of Γ with sizes from K such that $\partial^{t-1}\mathcal{F} = \underline{\lambda}\binom{\Gamma-\{0\}}{t-1}$.*

If $|\Gamma| = v$ we also say that $\mathcal{F}$ is a $t-(v, K, \lambda)$-PDF in Γ.

A $t-(\Gamma, k, \lambda)$-PDF is a $t-(\Gamma, K, \lambda)$-PDF where $K = \{k\}$. We have the following crucial theorem.

Theorem 3.2 *Let G be a group and let $\Gamma = G$ $(\Gamma = G^+)$ with $|\Gamma| = v$. Let $\mathcal{F}$ be a multiset of subsets of Γ. Then $(\Gamma, dev\mathcal{F})$ is a regular (1-rotational) $t-(v, K, \lambda)$ design under G if and only if $\mathcal{F}$ is a $t-(v, K, \lambda)$-PDF in Γ.*

From the above theorem we get:

Theorem 3.3 *The existence of a regular (1-rotational) $t-(v, K, \lambda)$ design under G is completely equivalent to the existence of a $t-(v, K, \lambda)$-PDF in G (G^+).*

It is obvious that the above theorems includes, as particular cases, Theorems 2.2 and 2.3

As an easy example let us construct the unique $3-(8, 4, 1)$-design (the point-plane design of $AG(3, 2)$) by difference methods.

Example 3.4 Let $G = Z_7$ and let $\mathcal{F} = (B_1, B_2)$ where B_1 and B_2 are the following 4-subsets of Z_7^+:

$$B_1 = \{0, 1, 3, \infty\} \qquad B_2 = \{0, 1, 4, 6\}$$

Both B_1 and B_2 have trivial G-stabilizer so that $\partial^2 B_1 = \Delta^2 B_1$ and $\partial^2 B_2 = \Delta^2 B_2$. We have:

$$\Delta^2 B_1 = (\{1,3\}, \{1,\infty\}, \{3,\infty\}, \{2,6\}, \{6,\infty\}, \{2,\infty\}, \{4,5\}, \{4,\infty\}, \{5,\infty\})$$

$$\Delta^2 B_2 = (\{1,4\}, \{1,6\}, \{4,6\}, \{3,6\}, \{5,6\}, \{3,5\}, \{3,4\}, \{2,3\}, \{2,4\}, \{1,2\}, \{1,5\}, \{2,5\})$$

Linking together the above lists of differences we get $\partial^2 \mathcal{F} = \Delta^2 \mathcal{F} = \binom{G^+ - \{0\}}{2}$. It follows, by Theorem 3.2, that $(G, dev\mathcal{F})$ is a cyclic 1-rotational $3-(8,4,1)$ design.

Needless to say that, in practice, Theorem 3.2 is not so effective as Theorem 2.2. Its application appears in fact quite lengthy in general. However, if we look for regular or 1-rotational t-designs ($t > 2$) with the help of a computer, it is maybe more convenient to apply Theorem 3.2 rather than the *Kramer- Mesner method* (see [14]).

4 Regular or 1-rotational graph decompositions

We firstly propose a generalization of the concept of a *Cayley graph.*

Recall that given a group G and a subset Ω of $G - \{0\}$ for which $-\Omega = \Omega$ holds, the *Cayley graph* of G on Ω, denoted by $Cay[G : \Omega]$, is the simple graph with vertex-set G and edges of the form $\{g, g + \omega\}$ with $\omega \in \Omega$.

It is well-known (see [19]) that, up to isomorphisms, the Cayley graphs are precisely the simple sharply-vertex-transitive graphs.

Now, given a multiset Ω on $G - \{0\}$ with the property that each $g \in G$ has the same multiplicity of $-g$ in Ω, I define, more generally, the *Cayley graph of G on Ω* as the *graph $Cay[G : \Omega]$* with vertex-set G and edge-multiset $\mathcal{E}$ in which the multiplicity of each $\{x, y\} \in \binom{G - \{0\}}{2}$ is exactly equal to the multiplicity of $x - y$ in Ω.

Reasoning as in [19] one may see that, up to isomorphisms, the class of all (also non-simple) sharply-vertex-transitive graphs coincides with the class of Cayley graphs defined as above.

Still more generally, given a multiset Ω on $G^+ - \{0\}$ containing each $g \in G$ as many times as $-g$, we may consider the graph $Cay[G^+ : \Omega]$ obtainable from $Cay[G : \Omega]$ by adding to it $\mu_\Omega(\infty)$ times the edge $\{\infty, g\}$ for any $g \in G$.

It is easy to see that a graph is *1-rotational* under a group G if and only if it is isomorphic to $Cay[G^+ : \Omega]$ for a suitable Ω.

Observe that if $\Omega = \underline{\lambda}(\Gamma - \{0\})$ where $\Gamma = G$ or G^+, then $Cay[G : \Omega] = \underline{\lambda} K(\Gamma)$.

As already pointed out, any (v,k,λ)-BIBD may be viewed as a decomposition of the graph $\underline{\lambda} K_v$ into copies of K_k. A question naturally arises:

What about regular and 1-rotational $(X,\mathcal{Y})$-designs in general?

First of all, it is easy to see that a regular $(X,\mathcal{Y})$-design under G must have X sharply-vertex-transitive with respect to G and hence, for what said above, X must be of the form $Cay[G:\Omega]$ for a suitable Ω.

Also, a 1-rotational $(X,\mathcal{Y})$-design under G has X of the form $Cay[G^+:\Omega]$ for a suitable multiset Ω on $G^+ - \{0\}$.

Let B be a subgraph of $X = Cay[G^+:\Omega]$. We call *list of differences of B in X* the multisubset of $G - \{0\}$ defined as follows:

$$\Delta B = (v - w \,|\, v \in V(B), w \in N_B(v) - \{\infty\})$$

As in Section 2, one may see that if G_B is the G-stabilizer of B, then each non-zero element of G appears in ΔB a multiple of $|G_B|$ times. I call *list of partial differences of B* the list $\partial B = \frac{1}{|G_B|}\Delta B$ which is also equal to

$$\partial B = (v - \ell \,|\, \ell \in L_B, v \in N_B(\ell) - \{\infty\})$$

where L_B is a system of representatives for the left cosets of G_B in G that are contained in $V(B)$.

Note that

$$\partial B = \frac{1}{d} \sum_{v \in V(B)-\{\infty\}} deg_B(v)$$

and that

$$\mu_{\partial B}(\infty) = \frac{deg_B(\infty)}{d}$$

where, in each case, d is a divisor of $|V(B) - \{\infty\}|$.

More generally, given a multiset $\mathcal{F}$ of subgraphs of G^+, I define the list of partial differences of $\mathcal{F}$ by $\partial\mathcal{F} = \underline{\bigcup}_{B\in\mathcal{F}} \partial B$.

Definition 4.1 *Let $X = Cay[\Gamma:\Omega]$ with $\Gamma = G$ or G^+, and let $\mathcal{Y}$ be a set of graphs. A $(X,\mathcal{Y})$ partial difference family (PDF) is a multiset $\mathcal{F}$ of subgraphs of X each isomorphic to some graph of $\mathcal{Y}$ with the property that $\partial\mathcal{F} = \Omega$.*

A (X,Y)-PDF is a $(X,\mathcal{Y})$-PDF where $\mathcal{Y} = \{Y\}$ consists of a single graph. We have the following theorem.

Theorem 4.2 *Let $X = Cay[\Gamma:\Omega]$ with $\Gamma = G$ $(\Gamma = G^+)$ and let $\mathcal{F}$ be a multiset of subgraphs of X each isomorphic to some graph of an assigned set $\mathcal{Y}$. Then $dev\mathcal{F}$ is a regular (1-rotational) $(X,\mathcal{Y})$-design under G if and only if $\mathcal{F}$ is a $(X,\mathcal{Y})$-PDF.*

From the above theorem we immediately get:

Theorem 4.3 *The existence of a regular* (1*-rotational*) $(X, \mathcal{Y})$*-design under* G *is completely equivalent to the existence of a* $(X, \mathcal{Y})$*-PDF in* G (G^+).

Applying Theorem 3.2 with $\Omega = \underline{\lambda}(\Gamma - \{0\})$ we get regular and 1-rotational $(\underline{\lambda}K_v, Y)$-designs ($v$ being the size of Γ). Thus, in particular, applying it with Ω as above and $\mathcal{Y} = \{K_k\}$ we refind Theorem 2.2.

As a first new application of Theorems 4.2, 4.3, we show that an example of *cube-decomposition* of the complete graph K_{16} given by Kotzig [12] falls in a new infinite family of *hypercube decompositions* of the complete graph that I am going to describe below.

Recall that the *hypercube of dimension* t (or t*-dimensional cube*), denoted by Q_t, is the Cayley graph $Cay[Z_2^t : \Omega]$ where Ω is any set of t independent vectors of Z_2^t.

Let us view the complete graph K_{2^n} as the Cayley graph $Cay[Z_2^n : \Omega]$ where $\Omega = Z_2^n - \{0\}$. Now note that, in the case where $2^n - 1 = tu$ with $n \geq t$, it is possible to partition Ω into t-ples Ω_1, Ω_2, ..., Ω_u of independent vectors of Z_2^n. Each $B_i = Cay[< \Omega_i >: \Omega_i]$ is a subgraph of K_{2^n} which is isomorphic to Q_t. Also, its list of partial differences coincides with Ω_i. It follows that $\mathcal{F} = (B_1, B_2, ..., B_u)$ is a (K_{2^n}, Q_t)-PDF. Thus we have:

Theorem 4.4 *Let* t *be a divisor of* 2^{n-1} *with* $t \leq n$*. Then there exists a regular* (K_{2^n}, Q_t)*-design.*

Now, I want to consider two problems concerning the decomposition of a complete graph into "small graphs" that Heinrich [9] leaves open. We show how Theorem 4.2 allows to solve them.

The first of these problems is the construction of a $(K_v, K_5 - e)$-design for $v \in \{37, 55, 73, 109, 397, 415, 469, 487, 505, 541, 613, 685\}$.

This problem may be solved for v a prime, namely for $v \in W$ where $W = \{37, 73, 109, 397, 487, 541, 613\}$ by using the following general technique:

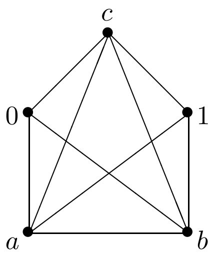
Construction Let v be a prime $\equiv 1 \pmod{2|E(Y)|}$. Given a subgraph B of $K(Z_v)$, let $\Delta^+ B = (x \in \Delta B : 1 \leq x \leq \frac{v-1}{2})$ so that $\Delta B = \{1, -1\}\Delta B$. Also, given $h \in Z_v - \{0\}$, let hB be the subgraph of $K(Z_v)$ with vertex-set $\{hv \,|\, v \in V(B)\}$ and edge-set $\{he \,|\, e \in E(B)\}$. If B is a subgraph of $K(Z_v)$ isomorphic to Y and such that $\Delta^+ B$ is a complete system of representatives for the cyclotomic classes of index $|E(Y)|$ in Z_v, then $\mathcal{F} = (hB \,|\, h \in H)$ is a $(K(Z_v), Y)$-PDF.

Using this technique Wilson [21] proved the existence of a (K_v, Y)-design for any (v, Y) with $v \equiv 1 \pmod{2|E(Y)|}$ sufficiently large.

This result was previously established by Wilson himself [20] in the particular but very important case where $Y = K_k$, case in which the construction essentially gives a $(v, k, 1)$-BIBD.

We can use the above technique for solving the mentioned problem concerning the construction of $(K_v, K_5 - e)$-designs with $v \in W$. We have to find a subgraph B of $K(Z_v)$ isomorphic to $K_5 - e$ such that Δ^+B be a system of representatives for the cyclotomic classes of index 9 in Z_v. It suffices to take B as follows:

$B =$



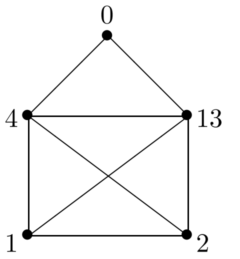
where $\{a, b, c\}$ has to be taken as indicated in the following table.

v	37	73	109	397	487	541	613
$\{a,b,c\}$	{4,6,15}	{2,6,49}	{2,5,89}	{9,14,43}	{6,14,29}	{2,27,41}	{3,13,41}

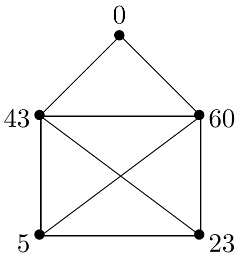
The second problem is the construction of a $(K_{65}, K_5 - P_3)$-design, P_3 being the *path* with three vertices. This problem has been independently solved by Colbourn [8] and myself.

My solution to the problem works as follows. I considered the subgroup $U = \{\pm 1, \pm 8\}$ of the units of Z_{65} acting semiregularly on $Z_{65} - \{0\}$. Then I looked for two subgraphs B_1 and B_2 of $K(Z_{65})$ isomorphic to $K_5 - e$ and such that $\Delta^+B_1 \uplus \Delta^+B_2$ is a complete system of representatives for the U-orbits on $Z_{65} - \{0\}$. I found that the following subgraphs satisfy this requirement.

$B_1 =$



$B_2 =$



Then $\mathcal{F} = (B_1, B_2, 8B_1, 8B_4)$ is a $(K(Z_{65}), K_5 - e)$-PDF. In fact we have $\Delta\mathcal{F} = \{1, 8\}(\Delta B_1 \uplus \Delta B_2) = \{\pm 1, \pm 8\}(\Delta^+B_1 \uplus \Delta^+B_2) = Z_{65} - \{0\}$.

Now, I also give an example of application of Theorem 4.2 to get a 1-rotational (K_v, C_v)-design for any odd v, C_v being the v-*cycle*.

Example 4.5 Let v be an odd integer, let $G = Z_{v-1}$, and let B the following v-cycle in $K(G^+)$:

$$B = (\infty, 0, 1, -1, 2, -2, ..., i, -i, ..., \frac{v-3}{2}, -\frac{v-3}{2}, \frac{v-1}{2}, \infty)$$

It is almost immediate to see that $\Delta B = \underline{2}(G^+ - \{0\})$ and that $G_B = \{0, \frac{v-1}{2}\}$. Thus we have $\partial B = G^+ - \{0\}$. It follows, by Theorem 4.2, that $devB$ is a 1-rotational (K_v, C_v)-design under G.

The above examples are of regular or 1-rotational (X, Y)-designs where X is a complete graph.

Concerning (X, Y)-designs where X is not complete, observe that if N is a subgroup of order n of a group G of order v, then a regular (X, K_k)-design with $X = Cay[G : \underline{\lambda}(G - N)]$ is equivalent to a regular (v, n, k, λ)-GDD under G (see Theorem 2.5).

Another very easy example of a regular decomposition of a non-complete graph is the following.

Example 4.6 Let Q_n be the n-dimensional hypercube and let d be a divisor of n. Take any partition of a base Ω of Z_2^n into n/d subsets Ω_1, ..., $\Omega_{n/d}$ of size d. Then $(Cay[<\Omega_1>: \Omega_1], ..., Cay[<\Omega_{n/d}>: \Omega_{n/d}])$ obviously is a $(K(Z_2^n), Q_d)$-PDF and hence we get the existence of a regular decomposition of the n-dimensional cube into d-dimensional cubes.

5 Regular or 1-rotational hypergraph decompositions

In order to get a description of regular or 1-rotational hypergraph decompositions in terms of differences, it is convenient to furtherly generalize the concept of a Cayley graph that I gave in the previous section.

Let G be a group and let Ω be a multiset of subsets of $\Gamma - \{0\}$ ($\Gamma = G$ or $\Gamma = G^+$) with the property that

$$\mu_\Omega(S) = \mu_\Omega[((S - g) \cup \{-g\}) - \{0\}] \qquad \forall\, S \in 2^{\Gamma - \{0\}}, \forall\, g \in S \tag{1}$$

I call *Cayley hypergraph of* Γ *on* Ω the hypergraph $Cay[\Gamma : \Omega]$ with vertex-set Γ and edge-multiset $\mathcal{E}$ defined by the following rule:

$$\mu_\mathcal{E}(S) = \mu_\Omega[(S - s) - \{0\}] \qquad \forall\, S \in 2^\Gamma$$

where s is an arbitrary element of $S - \{\infty\}$. Note that this definition does not depend on the choice of such an element s in view of (1). It is possible to prove that:

Theorem 5.1 *A hypergraph is sharply-vertex-transitive or* 1*-rotational under a group* G *if and only if, up to isomorphisms, it is of the form* $Cay[\Gamma : \Omega]$ *for a suitable multiset* Ω *on* $2^{\Gamma-\{0\}}$ *satisfying condition* (1) *where* $\Gamma = G$ *or* G^+ *respectively.*

Note, in particular, that $\underline{\lambda}(t\text{-}K(\Gamma)) = Cay[\Gamma : \Omega]$ where $\Omega = \underline{\lambda}\binom{\Gamma-\{0\}}{t-1}$.

Now, let us try to describe regular or 1-rotational $(X, \mathcal{Y})$-designs where X is an arbitrary hypergraph.

First of all, it is easy to see that a regular or 1-rotational $(X, \mathcal{Y})$-design under G must have, up to isomorphisms, X of the form $Cay[\Gamma : \Omega]$ for a suitable multiset Ω of subsets of $\Gamma - \{0\}$ where $\Gamma = G$ or G^+ respectively.

Let B be a subhypergraph of $X = Cay[G^+ : \Omega]$. I call *list of differences of* B *in* X the multiset of non-empty subsets of G defined as follows:

$$\Delta B = ((E - v) - \{0\} \,|\, v \in V(B) - \{\infty\},\, E \in \mathcal{E}(B),\, E \ni v)$$

Once again we may see that if G_B is the G-stabilizer of B, then each non-empty subset of G appears in ΔB a multiple of $|G_B|$ times, G_B being the stabilizer of B under G. Then I define *list of partial differences of* B by $\partial B = \frac{1}{|G_B|}\Delta B$ which we can also express in the form:

$$\partial B = ((E - v) - \{0\} \,|\, v \in L_B - \{\infty\},\, E \in \mathcal{E}(B),\, E \ni v)$$

where L_B is a system of representatives for the left cosets of G_B in G that are contained in $V(B)$.

More generally, given a multiset $\mathcal{F}$ of subgraphs of G^+, the list of partial differences of $\mathcal{F}$ is the list $\partial\mathcal{F} = \underline{\bigcup}_{B\in\mathcal{F}}\partial B$.

The definition and theorems that follow may be obtained from Definition 4.1 and Theorems 4.2, 4.3 by simply replacing the word "graph" with the word "hypergraph". I write them explicitely for convenience of the reader.

Definition 5.2 *Let* $X = Cay[\Gamma : \Omega]$ *with* $\Gamma = G$ *or* G^+*, and let* $\mathcal{Y}$ *be a set of hypergraphs. A* $(X, \mathcal{Y})$ *partial difference family* (PDF) *is a multiset* $\mathcal{F}$ *of subhypergraphs of* X *each isomorphic to some hypergraph of* $\mathcal{Y}$ *with the property that* $\partial\mathcal{F} = \Omega$.

A (X, Y)-PDF is $(X, \mathcal{Y})$-PDF where $\mathcal{Y} = \{Y\}$ consists of a single hypergraph. We have the following theorem.

Theorem 5.3 *Let $X = Cay[\Gamma : \Omega]$ with $\Gamma = G$ ($\Gamma = G^+$) and let $\mathcal{F}$ be a multiset of subhypergraphs of X each isomorphic to some graph of an assigned set $\mathcal{Y}$. Then dev$\mathcal{F}$ is a regular (1-rotational) $(X, \mathcal{Y})$-design under G if and only if $\mathcal{F}$ is a $(X, \mathcal{Y})$-PDF.*

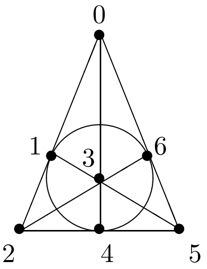
From the above theorem we immediately get:

Theorem 5.4 *The existence of a regular (1-rotational) $(X, \mathcal{Y})$-design under G is completely equivalent to the existence of a $(X, \mathcal{Y})$-PDF in G (G^+).*

Applying the above theorems with $\Omega = \underline{\lambda}\binom{\Gamma-\{0\}}{t-1}$ and $Y = t$-K_k we essentially refind Theorems 3.2 and 3.3.

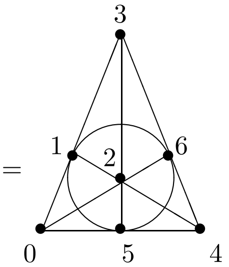
Now, as truly new examples of application of Theorem 5.3, we construct some regular or 1-rotational decompositions of 3-K_v into copies of the *Fano plane*. In the following, Y will always denote the Fano plane.

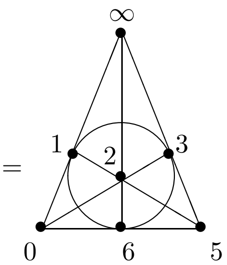
Example 5.5 Consider the following subhypergraph B of 3-$K(Z_8)$:

$B =$ 

One may easily check that $\partial B = \Delta B = \binom{Z_8-\{0\}}{2}$ so that $devB$ is a cyclic decomposition of 3-K_8 into Fano planes.

Example 5.6 Consider the following subhypergraphs B_1 and B_2 of 3-$K(Z_7^+)$:

$B_1 =$ 

$B_2 =$ 

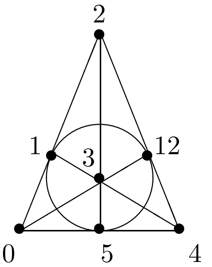
Note that B_1 is fixed by Z_7 so that $\partial B_1 = (E - \{0\} \,|E \in \mathcal{E}(B), E \ni 0)$. Thus $\partial B_1 = (\{1,3\},\{2,6\},\{4,5\})$.

Then check that B_2 has trivial stabilizer and that ΔB_2 covers exactly once all the 2-subsets of $Z_7^+ - \{0\}$ not appearing in ∂B_1. It follows that $\mathcal{F} = (B_1, B_2)$ is a $(3\text{-}K(Z_7^+), Y)$-PDF and hence that $dev\mathcal{F}$ is a 1-rotational decomposition of 3-K_8 into Fano planes.

The above two examples suggest to study the following problem.

Problem 5.7 *Given a $2-(v,3,1)$ design Y, find a cyclic decomposition and a 1-rotational decomposition of 3-K_{v+1} into copies of Y.*

Example 5.8 Consider the following subhypergraph B of $K(Z_{23})$:

$B =$ 

Let $Z_{23}^{\square}$ be the group of squares in Z_{23}. Check that this group acts semiregularly on the set $\Omega = \binom{Z_{23}-\{0\}}{2}$. Then check that B has trivial Z_{23}-stabilizer and that ΔB is a complete system of representatives for the $Z_{23}^{\square}$-orbits on Ω. It easily follows that $\mathcal{F} = (mB \,|\, m \in Z_{23}^{\square})$ is a 3-$(K(Z_{23}), Y)$-PDF so that $dev\mathcal{F}$ is a cyclic decomposition of 3-$K(Z_{23})$ into Fano planes.

References

[1] R.J.R. Abel, *Difference families*, in CRC Handbook of Combinatorial Designs (C.J. Colbourn and J.H. Dinitz, eds.), CRC Press, Boca Raton, FL, 1996, pp. .

[2] T. Beth, D. Jungnickel and H. Lenz, *Design Theory.* Cambridge University Press, Cambridge, 1999.

[3] R.C. Bose, *On the construction of balanced incomplete block designs*, Ann. Eugenics 9 (1939), 353-399.

[4] M. Buratti, *Recursive constructions for difference matrices and relative difference families*, J. Combin. Designs 6 (1998), 165-182.

[5] M. Buratti, *Constructions for point-regular linear spaces*, J. Stat. Plann. Infer., to appear.

[6] M. Buratti, *On regular or 1-rotational graph and hypergraph decompositions*, in preparation.

[7] M. Buratti and F. Zuanni, *On singular 1-rotational Steiner 2-designs*, J. Combin. Theory Ser. A **86** (1999), 232-244.

[8] C.J. Colbourn and P-J. Wan, *Minimizing drop cost for SONET/WDM networks with $\frac{1}{8}$ wavelength requirements*, preprint.

[9] K. Heinrich, *Graph Decompositions and Designs*, in CRC Handbook of Combinatorial Designs (C.J. Colbourn and J.H. Dinitz, eds.), CRC Press, Boca Raton, FL, 1996, pp. 361-366.

[10] D. Jungnickel, *Transversal designs associated with Frobenius groups*, J. Geom. 17 (1981), 140-154.

[11] D. Jungnickel, *Difference sets*, in Contemporary design theory: A collection of surveys, (J.H. Dinitz and D.R. Stinson eds.), Wiley, New York, 1992, pp. 241-324.

[12] A. Kotzig, *Decomposition of complete graphs into isomorphic cubes*, J. Combin. Theory B 31 (1981), 292-296.

[13] E.S. Kramer, S.S. Magliveras and R. Mathon, *The Steiner systems $S(2,4,25)$ with nontrivial automorphism group*, Discrete Math. 77 (1989), 137-157.

[14] E.S. Kramer and D.M. Mesner, *t-designs on hypergraphs*, Discrete Mth. 15 (1976), 263-236.

[15] W.H. Mills, *The constructions of BIBDs using nonabelian groups*, Congr. Numer. 21 (1979), 73-86.

[16] A. Pott, A survey on relative difference sets, Groups, difference sets, and the monster, de Gruyter Berline-New York, 1996, pp. 195-232.

[17] A. Rosa, *O cyklickych rozkladoch kompletneho grafu na neparnouholniky*, Casop. pestov. mat. 91 (1966), 56-63.

[18] A. Rosa, *On cyclic decompositions of the complete graph into $(4m+2)$-gons*, Mat.-Fyz. Cas. 16 (1966), 349-352.

[19] G. Sabidussi, *On a class of fixed-point free graphs*, Proc. Amer. Math. Soc. 9 (1958), 800-804.

[20] R.M. Wilson, *Decompositions of complete graphs into subgraphs isomorphic to a given graph*, Congr. Numer. 15 (1976), 647-659.

[21] R.M. Wilson, *Cyclotomy and difference families in elementary abelian groups*, J. Number Theory 4 (172), 17-47.

[22] G. Zappa, *Partizioni ed S-partizioni dei gruppi finiti*, Symposia Mathematica, Ist. Naz. di Alta Matem. 1 (1968), 85-94.

Dimensional Dual Hyperovals, Steiner Systems and $c.L^*$ Geometries

M. Buratti, A. Del Fra*

Università "La Sapienza"
e-mail: delfra@axrma.uniroma1.it

A d-dimensional dual hyperoval in $\Pi = PG(n,q)$ is a family F of d-spaces spanning Π, pairwise meeting in exactly one point and such that every point of Π is incident with either 0 or 2 members of F [3]. d-dimensional dual hyperovals generalize the usual dual hyperovals in a projective plane (correspondent to $d=1$) and allow to construct geometries belonging to the diagram $c.L^*$ [3]. Some preliminary results concerning dimensional dual hyperovals were given in [1], [2], [3] and [4]. F is said to satisfy property (T) if, for any triple S_1, S_2, S_3 of distinct members of F, the d space S_1 meets the $2d$-space spanned by S_2 and S_3 in a line (the minimum possible intersection). Property (T) implies that the d-spaces of F can be collected in blocks of size $q+2$, giving rise to a Steiner system $S(3, q+2, \frac{q^{d+1}-1}{q-1}+1)$, satisfying the following property:

(P) its derived Steiner systems $S(2, q+1, \frac{q^{d+1}-1}{q-1})$ are all isomorphic to the point-line system of $PG(d,q)$.

When $q=2$, such a system will be called a *quasi-Boolean quadruple system*. We use this terminology since the so called *Boolean quadruple system*, i. e., the point-plane design of $AG(d+1,2)$, obviously satisfies property (P). For any d, set $n(d) = \binom{d+2}{2} - 1$. In this paper we prove that if a d-dimensional dual hyperoval is built in $PG(n,2)$, starting from the Boolean $S(3,4,2^{d+1})$, then $n \leq n(d)$. For every d, we construct two d-dimensional dual hyperovals in $PG(n(d),2)$ and in $PG(n(d)-1,2)$ respectively, starting from the Boolean $S(3,4,2^{d+1})$. The first one is possibly isomorphic to a known d-dimensional dual hyperoval obtained by the Grassmann variety of lines of $AG(n(d)+1,2)$ [2]. We also give an algebraic method to get "many" non-isomorphic quasi-Boolean quadruple systems $S(3,4,2^{d+1})$ for any d. They should give rise to other d-dimensional dual hyperovals, for every d. We prove this for the lowest values of d.

References

[17] A. Del Fra: *On d-dimensional dual hyperovals*, Geom. Dedicata, to appear.

[18] C. Huybrechts: *c.AG***-geometries and dimensional dual hyperovals in projective spaces*, preprint.

[19] C. Huybrechts and A. Pasini: *Flag-transitive extensions of dual affine spaces*, Contrib. Algebra Geom., 40 (1999), 503-532.

[20] S. Yoshiara: *A new family of d-dimensional dual hyperovals in* $PG(2d+1,2)$, European J. Combin, 20 (1999), 489-503.

On Perfect Cayley Designs

M. Buratti, Fulvio Zuanni*

Università de L'Aquila - L'Aquila, Italy
e-mail: zuanni@ing.univaq.it

We introduce the concept of a *Perfect Cayley Design* (PCD) that generalizes that of a *Perfect Mendelsohn Design* (PMD) as follows. Given an additive group H, a $(v, H, 1)$-PCD is a pair $(X, \mathcal{B})$ where X is a v-set and $\mathcal{B}$ is a set of injective maps from H to X with the property that for any pair (x, y) of distinct elements of X and any $h \in H - \{0\}$ there is exactly one $B \in \mathcal{B}$ such that $B(h') = x, B(h'') = y$ and $h' - h'' = h$ for suitable $h', h'' \in H$. It is clear that a $(v, Z_k, 1)$-PCD simply is a $(v, k, 1)$-PMD. This generalization has concrete motivations in at least one case. In fact we observe that *triplewhist tournaments* may be viewed as *resolved* $(v, Z_2^2, 1)$-PCD's. We present four composition constructions for *regular* and *1-rotational* resolved PCD's. As a consequence, we get new infinite families of resolved PMD's and of *Z-cyclic whist tournaments*.

Codes, Matroids and Trellises

P.J. Cameron

School of Mathematical Sciences - Queen Mary and Westfield College - London E1 4NS U.K.
e-mail: p.j.cameron@qmw.ac.uk

There is a natural bijection between representable matroids and linear codes over a given field, which is not as well known as it ought to be. An early result on this is Greene's theorem asserting that the weight enumerator of the code is a specialisation of the Tutte polynomial of the matroid. This connection also throws light on the minimal trellis for decoding a given code, and gives new results (and easier proofs of old results) on trellis complexity.

1 Introduction

This is a survey paper on the connection between matroids and linear codes, on trellis decoding, and of applications of the code–matroid connection to the problem of determining the smallest trellis for a code equivalent to a given code. Proofs of the assertions appear elsewhere. The paper is based to a large extent on the Ph.D. thesis [8] of Constantinos Papadopoulos, to whom I express my gratitude. Others who have contributed are R. A. Bailey, Carrie Rutherford and Fuad Shareef.

2 Codes

In this section we give brief summaries of the theories of codes and matroids. For more details we refer to standard textbooks such as [6] for codes and [9] for matroids. Let F be a set called the *alphabet* and n a positive integer. A *word* of length n over F is simply an n-tuple of elements of F; typically we write $a_1a_2\cdots a_n$ instead of $(a_1, a_2, \ldots, a_n)$. In the most important case here, F is a field; from now on, this is always assumed to be the case. The code C is *linear* if it is a subspace of F^n. A linear code of length n and dimension k is referred to as an $[n, k]$ code. Let C be a $[n, k]$ code. A *generator matrix* for C is a $k \times n$ matrix whose rows form a basis for C. The *dual code* $C^\perp$ of C is the set

$$C^\perp = \{x \in F^n : x \cdot c = 0 \text{ for all } c \in C\},$$

where $\cdot$ denotes the standard inner product on F^n. The *Hamming distance* $d(a,b)$ between words a and b is the number of coordinates where they differ:

$$d(a,b) = |\{i : 1 \leq i \leq n, a_i \neq b_i\}|.$$

The *weight* $\mathrm{wt}(a)$ is the number of non-zero coordinates of a, that is, $\mathrm{wt}(a) = d(a,0)$, where 0 is the all-zero word. If F is finite, the *weight enumerator* $W_C(x,y)$ of the code C is the homogeneous polynomial

$$W_C(x,y) = \sum_{c \in C} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)} = \sum_{i=0}^{n} A_i x^{n-i} y^i,$$

where A_i is the number of words of weight i in C. Two codes C, C' of length n over F are *monomial equivalent* if C' can be obtained from C by permuting the coordinates and multiplying coordinates by non-zero scalars. This is the natural equivalence relation on linear codes, and preserves dimension, weight enumerator, and most significant properties. The ith *generalised Hamming weight* $d_i(C)$ of a code C, for $1 \leq i \leq k = \dim(C)$, is defined to be the smallest support size of an i-dimensional subcode of C. So $d_1(C)$ is the *minimum weight* of C. The sequence $(d_1(C), \ldots, d_k(C))$ is called the *Hamming weight hierarchy* of C. These numbers are strictly increasing; in fact, the following is true:

Theorem 2.1 *The generalized Hamming weights of a linear code over* $\mathrm{GF}(q)$ *satisfy*

$$d_{i+1} \geq d_i + \left\lceil \frac{d_i(q-1)}{q(q^i-1)} \right\rceil .$$

This result in the case of binary codes is due to Helleseth *et al.* [4].

3 Matroids

Let E be a set. A *matroid* M on E is a pair $(E, \mathcal{I})$, where $\mathcal{I}$ is a non-empty family of subsets of E (called *independent sets*) with the properties

(a) if $I \in \mathcal{I}$ and $J \subseteq I$, then $J \in \mathcal{I}$;

(b) (the *exchange property*) if $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then there exists $e \in I_2 \setminus I_1$ such that $I_1 \cup \{e\} \in \mathcal{I}$.

Matroids were introduced by Whitney to axiomatise the notion of linear independence in a vector space. Indeed, if E is a family of vectors in a vector space V, and $\mathcal{I}$ is the set of linearly independent subsets of E, then $(E, \mathcal{I})$ is a matroid. More formally, a *representation* of a matroid $(E, \mathcal{I})$ over a field F is a map χ from E to an F-vector space with the property that a subset I of E belongs to $\mathcal{I}$ if and only if $\chi(I)$ is linearly independent. Two representations χ, χ' of M are *equivalent* if there is an invertible linear transformation of V whose composition with χ is χ'. It follows from the second axiom that all maximal independent sets in a matroid M have the same cardinality k, called the *rank* of M. These maximal independent sets are called the *bases* of M. It can be shown that the set of all complements of bases of M is the set of bases of another matroid M^* on E, called the *dual* of M. Matroids can be defined in many equivalent ways. One which will be important to us is by means of the *rank function* ρ, the function from the power set of E to the non-negative integers given by the rule that $\rho(A)$ is the cardinality of any maximal independent subset of A. (Again, the exchange property shows that any two maximal independent subsets of A have the same cardinality.) It is possible to axiomatise the rank functions of matroids, but that will not be necessary here. One feature of matroids is that they are precisely those structures where the greedy algorithm always succeeds in choosing a base of minimum weight. More formally:

Proposition 3.1 *Suppose that $M = (E, \mathcal{I})$ is a matroid, and that the elements of E are totally ordered. Then*

(a) there is a base $A = \{a_1, \ldots, a_k\}$ with $a_1 < \cdots < a_k$, called the first base*, such that if $X = \{x_1, \ldots, x_k\}$ is any other base with $x_1 < \cdots < x_k$, then $a_i \leq x_i$ for $i = 1, \ldots, k$;*

(b) there is a base $B = \{b_1, \ldots, b_k\}$ with $b_1 < \cdots < b_k$, called the last base*, such that if $X = \{x_1, \ldots, x_k\}$ is any other base with $x_1 < \cdots < x_k$, then $x_i \leq b_i$ for $i = 1, \ldots, k$.*

The first base A is found by the greedy algorithm: $\{a_1\}$ is the smallest independent set of size 1; then a_2 is the smallest element such that $\{a_1, a_2\}$ is independent; and so on. A dual remark applies to the last base. The first and last bases of the dual matroid M^* are the complements of the last and first bases of M respectively.

4 The code–matroid connection

Let A be a $k \times n$ matrix over a field F, satisfying the condition that the rows of A are linearly independent, so that the row space of A has dimension k. There are two different structures that can be built from A. First, the row space of A is an $[n, k]$ code over F, that is, a k-dimensional subspace of F^n. Now row operations on A simply change the basis for the code, leaving the actual code completely unaltered. Column permutations, and multiplications of columns by non-zero scalars, replace the code by a monomial equivalent code. Second, there is a matroid M on the set $E = \{1, 2, \ldots, n\}$, in which a set I is independent if and only if the family of columns of A whose indices belong to I is linearly independent. (We cannot quite say that the elements of E are the columns and independence is linear independence, since E might have repeated columns.) Moreover, the function χ mapping i to the ith column is a representation of M over F. Now row operations on A don't change M but replace the representation χ by an equivalent representation, while column permutations and scalar multiplications replace M by an isomorphic matroid. So, if we call two matrices A and A' *CM-equivalent* if A' is obtained from A by a row operation and a monomial transformation of the columns, we see that CM-equivalence classes of matroids correspond bijectively to both monomial equivalence classes of linear codes, and equivalence classes of representations of matroids, under the natural notions of equivalence in each case. Thus we expect information to transfer back and forth between code and matroid. In later sections, we will implicitly do so, by talking about (for example) the first and last base of a code (meaning the first and last base of the corresponding matroid). A code C is called *projective* if any two columns of a generator matrix for C are linearly independent (equivalently, if the dual code $C^\perp$ has minimum weight at least 3). The corresponding condition for matroids is that of being a *simple matroid*, that is, all subsets of size at most 2 are independent (so that there are no loops or parallel elements in the matroid). If this holds, then the representation of the matroid can be regarded as being in the projective space $\mathrm{PG}(k-1, F)$ rather than in the vector space F^k. Thus, representations of simple matroids provide another framework for studying point sets in projective spaces. For example, the zeros of a word in the dual code $C^\perp$ are the points of a hyperplane section of the point set, and so the weight enumerator of $C^\perp$ gives the cardinalities of the hyperplane sections. It is a simple exercise to show the following:

Proposition 4.1 *If the matroid M corresponds to the code C, then the dual matroid M^* corresponds to the dual code $C^\perp$.*

5 Tutte polynomial and weight enumerator

Let M be a matroid on the set E, having rank function ρ. The *Tutte polynomial* of M is most easily defined as follows:

$$T(M; x, y) = \sum_{A \subseteq E} (x-1)^{\rho E - \rho A} (y-1)^{|A| - \rho A}.$$

For example, the Tutte polynomial of the uniform matroid $U_{n,k}$ is

$$T(U_{n,k}; x, y) = \sum_{i=0}^{k} \binom{n}{i} (x-1)^i + \sum_{i=k+1}^{n} \binom{n}{i} (y-1)^i.$$

Moreover we have:

Proposition 5.1 *(a) The number of bases of M is equal to $T(M;1,1)$.*

(b) The number of independent sets of M is equal to $T(M;2,1)$.

(c) The number of spanning sets of M is equal to $T(M;1,2)$.

(d) $T(M;2,2) = 2^n$.

The Tutte polynomials of a matroid and its dual are very simply related:

Proposition 5.2

$$T(M^*;x,y) = T(M;y,x).$$

In the remainder of this section we briefly discuss a particular instance where the connection between codes and matroids is useful. The following theorem was proved by Greene [3].

Theorem 5.3 *Let C be a code over a field with q elements, and M the corresponding vector matroid. Then*

$$W_C(x,y) = y^{n-\dim(C)}(x-y)^{\dim(C)}T\left(M;\frac{x+(q-1)y}{x-y},\frac{x}{y}\right).$$

Note that, if $X = (x+(q-1)y)/(x-y)$ and $Y = x/y$, then

$$(X-1)(Y-1) = q.$$

So the weight enumerator is an evaluation of the Tutte polynomial along a particular hyperbola in the 'Tutte plane'. The proof will not be given here, but merely indicated. There is a recursive formula for the Tutte polynomial of a matroid in terms of Tutte polynomials of matroids with one fewer element (the so-called "deletion–contraction rule"). Similarly, the weight enumerator of a code can be expressed in terms of the weight enumerators of the codes obtained by shortening and puncturing the code at some position. Then the equality of the two expressions in the theorem follows by induction. (The punctured code corresponds to the deleted matroid, and the shortened code to the contracted matroid.) From Theorem 5.3 and Proposition 5.2, we can deduce the *MacWilliams relation*, which shows that the weight enumerator of the dual code $C^\perp$ can be calculated from that of C.

Theorem 5.4

$$W_{C^\perp}(x,y) = \frac{1}{|C|}W_C(x+(q-1)y, x-y).$$

Proof Since $C^\perp$ has dimension $n-\dim(C)$ and corresponds to the dual matroid M^*, we have

$$W_{C^\perp}(x,y) = y^{\dim(C)}(x-y)^{n-\dim(C)}T\left(M; \frac{x}{y}, \frac{x+(q-1)y}{x-y}\right).$$

On the other hand, we have

$$\frac{1}{|C|}W_C(x+(q-1)y, x-y) =$$
$$q^{-\dim(C)}(x-y)^{n-\dim(C)}(qy)^{\dim(C)}T\left(M; \frac{qx}{qy}, \frac{x+(q-1)y}{x-y}\right).$$

The two expressions are equal.

Note that this proof is entirely combinatorial, in contrast to the usual proof which involves characters of the additive group of F^n.

6 Trellis decoding

For a small but not quite trivial example, suppose that we are using the binary dual Hamming code of length 7 to send information. The codewords are:

0000000
0011011
0101101
0110110
1001110
1010101
1100011
1111000

The minimum weight is 4, so we can correct one error and detect two errors. However, in a practical communication channel, the received word is likely to be an analog signal, sampled at seven time points, so we obtain seven real numbers. Suppose that we receive

$$w = (-0.1, 0.0, 0.2, 0.9, 1.8, 0.9, 1.4) \in \mathbb{R}^7.$$

If we round each value to the nearest of zero and one, we obtain 0001111, which is at distance 2 from the second, third and fifth codewords in the list, so we have a decoding failure. If we make the (physically realistic) assumptions that the errors at the sampling points are independent identically distributed Gaussian variables, then it can be shown that the most likely codeword to have been transmitted is the one at smallest Euclidean distance from w in $\mathbb{R}^7$, which turns out to be 0101101. The method of *trellis decoding* provides a way to decode to the nearest Euclidean codeword without first rounding the individual entries of w, and without calculating the Euclidean distance of w to every codeword. Let F be an alphabet. A *trellis* over F is a directed graph whose vertices come in *layers* $V_0, V_1, \ldots, V_n$, where V_0 contains a single vertex s called the *source*, and V_n contains a single vertex t called the *target*, and whose edges also come in *layers* $E_{i-1,i}$ for $i = 1, \ldots, n$, where an edge in $E_{i-1,i}$ has initial vertex in V_{i-1} and terminal vertex in E_i. Moreover, each edge has a label, which is an element of the alphabet F. Now any path from s to t in F has length n, and the labels of the edges on the path (taken in order) form a word of length n. We say that the trellis is *one-to-one* if different paths realise different words. The set C of all words represented by paths in the trellis is the *code represented by* the trellis. Figure 1 shows a trellis for the dual Hamming code. Now the trellis is used as follows. Each symbol in the alphabet F is represented by a real number (the signal level corresponding to accurate transmission of that symbol). If $F = \mathrm{GF}(2)$, we may assume without loss of generality that the signal levels for the elements $0, 1 \in F$ are the real numbers $0, 1$. In general, we identify the set F with the corresponding set of real numbers.

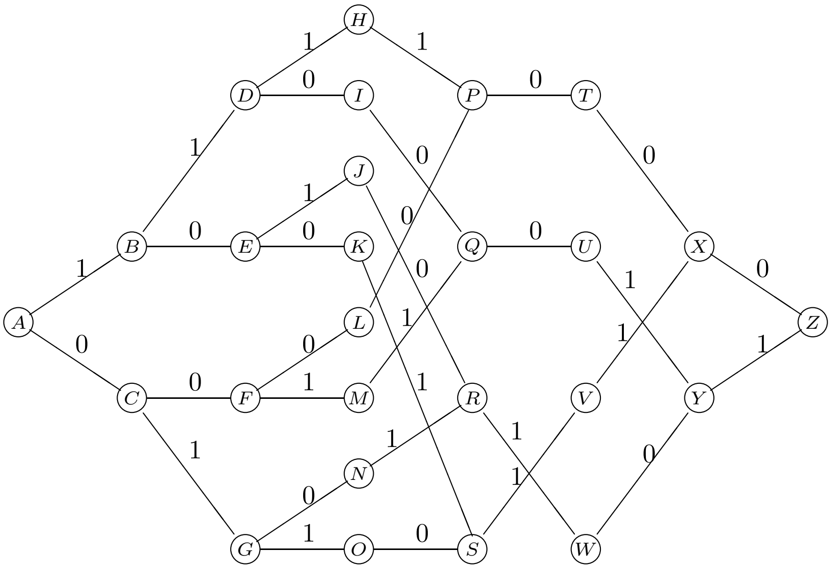


Figure 1: A trellis for the dual Hamming code

Now, when the ith component w_i of the received word w is known, we assign the *length* $l(e) = (w_i - a)^2$ to an edge e with label a in the layer $E_{i-1,i}$. When all components of w have been received, then the sum of the edge lengths in any path from s to t is equal to the squared Euclidean distance from w to the corresponding codeword. So finding the nearest codeword to w is transformed into the problem of finding the shortest path in a directed graph with edge lengths. Most of the work can be done in real time. Once edge lengths $l(e)$ are assigned to edges $e \in E_{i-1,i}$, we assign to each vertex $v \in E_i$ the number

$$f(v) = \min\{f(v') + l(v', v) : (v', v) \in E_{i-1,i}\}$$

(where the induction begins with $f(s) = 0$). Then $f(v)$ is the length of the shortest path from s to v. Once all components of x are known, then the length of the shortest path from s to t is determined, and the actual path can be found by working backwards. (This is essentially Dijkstra's shortest path algorithm.) In our example, the numbers work out as shown in Figure 2. We see that the shortest path is

$$A \to C \to G \to N \to R \to W \to Y \to Z,$$

and give the correct message corresponding to this path, which is 0101101.

7 The minimal trellis for a code

Every code is represented by at least one trellis. We can simply take $|C|$ paths from s to t which are edge-disjoint and have only the end vertices in common, and label each path to represent one codeword. However, the discussion of decoding above shows that a smaller trellis will give more efficient decoding. The algorithm given involves one multiplication for each edge, and k additions and $k-1$ comparisons at each vertex with in-degree k. So the number of arithmetic operations is twice the edge count of the trellis, and the number of comparisons is equal to the *cycle rank* (number of vertices minus number of edges plus one). A third obvious measure of trellis size is the vertex count of the trellis. *Muder's theorem* [7] shows that, for a linear code, there is a trellis which is uniformly best in terms of vertex count.

Theorem 7.1 *Let C be a linear code of length n. Then there is a trellis T representing C, with layers $V_0, \ldots, V_n$, such that, if another proper trellis T' for C has layers $V'_0, \ldots, V'_n$, then $|V'_i| \geq |V_i|$ for $i = 0, \ldots, n$. Moreover, if $|V'_i| = |V_i|$ for $i = 0, \ldots, n$, then T' is isomorphic to T. Furthermore, T also minimises the sizes of all the edge layers and the cycle rank.*

I will not prove this theorem here, but instead describe the simple construction of the Muder trellis given in [1]. This also shows how to calculate the size of the trellis from knowledge of the first and last bases for the matroid associated with the code

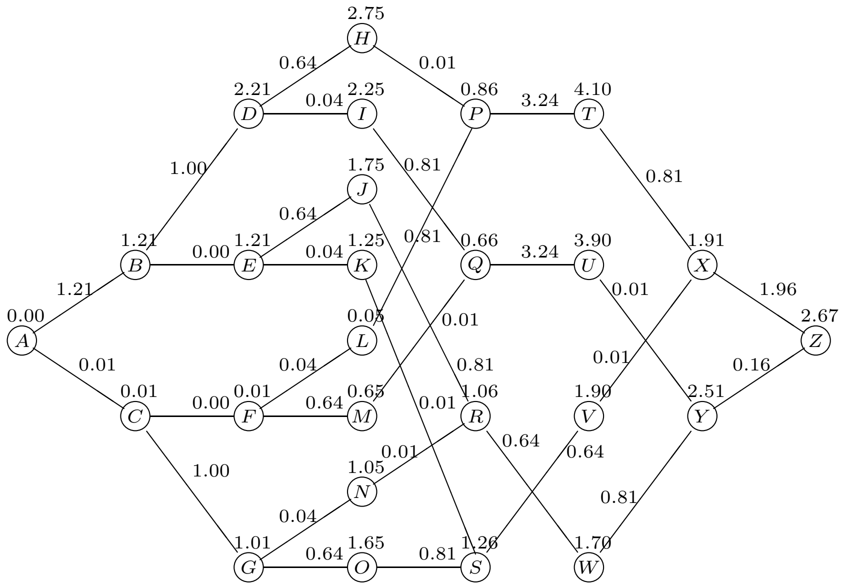


Figure 2: A trellis with edge-lengths and distances

(see Proposition 3.1). Let C be a linear code over F, and let $A = \{a_1, \ldots, a_k\}$ be the first base and $B = \{b_1, \ldots, b_k\}$ be the last base, where $a_1 < \cdots < a_k$ and $b_1 < \cdots < b_k$. For $0 \leq i \leq n$, we define the ith *past subcode* of C to be

$$P_i = \{c \in C : c_j = 0 \text{ for all } j > i\},$$

and the ith *future subcode* to be

$$F_i = \{c \in C : c_j = 0 \text{ for all } j \leq i\}.$$

By convention, $P_n = F_0 = C$. If we take a generator matrix G for C in echelon form, we see that F_i is spanned by the rows of G whose leading 1 occurs to the right of i. Hence

$$\dim(F_i) = |A \cap \{i+1, \ldots, n\}| = k - |A \cap \{1, \ldots, i\}|.$$

Dually,

$$\dim(P_i) = |B \cap \{1, \ldots, i\}|.$$

Also, of course, we have

$$P_i \cap F_i = \{0\},$$

so P_i and F_i generate their direct sum. Now the following construction produces the minimal trellis for C. The vertices in the ith layer are the elements of the quotient space $V_i = C/(P_i \oplus F_i)$, that is, cosets of $P_i \oplus F_i$ in C. For each codeword c, we put an edge with label c_i from the coset $(P_{i-1} \oplus F_{i-1}) + c \in V_{i-1}$ to the coset $(P_i \oplus F_i) + c \in V_i$. We identify edges with the same label between the same vertices. Note that, for example, two edges with the same initial vertex and the same label also have the same terminal vertex. For suppose that $c - d \in P_{i-1} \oplus F_{i-1}$, say $c - d = p + f$ with $p \in P_{i-1}$ and $f \in F_{i-1}$. Suppose also that $c_i = d_i$. By definition, $p_i = 0$, hence $f_i = (c - d - p)_i = 0$, and $f_i \in F_i$. Thus, $c - d = p + f \in P_i \oplus F_i$, and so the terminal vertices of the corresponding edges are the same. Similar arguments show:

Proposition 7.2 *The trellis just constructed is isomorphic to the Muder minimal trellis.*

This shows that the first and last bases determine the sizes of the layers in the Muder trellis:

Proposition 7.3 *Let C be a linear code over $\mathrm{GF}(q)$. Then the sizes of the vertex and edge layers in the Muder trellis for C are given by*

$$\begin{aligned} |V_i| &= q^{|A \cap \{1,\ldots,i\}| - |B \cap \{1,\ldots,i\}|}, \\ |E_{i-1,i}| &= q^{|A \cap \{1,\ldots,i\}| - |B \cap \{1,\ldots,i-1\}|}, \end{aligned}$$

where A and B are the first and last bases of the corresponding matroid.

For example, if C is the dual Hamming code of the preceding section, then the first base is $\{1, 2, 3\}$ and the last base is $\{4, 6, 7\}$, so we find immediately that the sizes of the vertex layers are $1, 2, 4, 8, 4, 4, 2, 1$ respectively.

8 Column permutations

The various measures of trellis size for a code differ from the more usual coding-theoretic parameters in one significant way: they may differ for equivalent codes (those obtained by column permutations). For example, if we reverse the order of the coordinates of the dual Hamming code, the first base is $\{1, 2, 4\}$ and the last base $\{5, 6, 7\}$; the size of the trellis is unaltered but the individual layers change. Swapping the fourth and fifth columns gives first base $\{1, 2, 3\}$ and last base $\{5, 6, 7\}$, so that the sizes of the layers in the minimal trellis are $1, 2, 4, 8, 8, 4, 2, 1$. We see that, to construct a small trellis for a code equivalent to C, we want to make the first base come as late as possible, and the last base come as early as possible. This is a difficult problem; it is known to be NP-complete in general (see [5]). However, we can use the geometric structure of some codes to find the smallest trellises. First a class of codes in which we have no choice. A linear code C of length n and dimension k is said to be *maximum distance separable*, or *MDS*, if the corresponding matroid is the uniform matroid $U_{n,k}$ of rank k on n elements (that is, every set of size k is a base – this is not the usual definition!) A representation of the uniform matroid $U_{n,k}$ over $\mathrm{GF}(q)$ is simply a n-arc in $\mathrm{PG}(k-1,q)$; this instance of the code–matroid connection has been the subject of a lot of research (see [2]). MDS codes are the worst with respect to trellis size:

Proposition 8.1 *Suppose that $k \le n/2$.*

(a) The number of vertices in the Muder trellis for an $[n,k]$ code is at most $(n-2k+1)q^k + 2(q^k-1)/(q-1)$.

(b) The code C has the property that the Muder trellis for any code equivalent to C has $(n-2k+1)q^k + 2(q^k-1)/(q-1)$ vertices if and only if C is MDS.

Proof The given bound is the number of vertices in the Muder trellis for a code whose first base is $\{1,\ldots,k\}$ and whose last base is $\{n-k+1,\ldots,n\}$. Clearly this is the worst case. Now if C is MDS, then every set of k elements is a base, so the first base is $\{1,\ldots,k\}$ and the last base $\{n-k+1,\ldots,n\}$ in any ordering. Conversely, suppose that the bound is attained for all codes equivalent to C. Any set of k columns can be brought to the first k positions by some permutation, and so forms a base; so C is MDS.

We conclude with the extended binary Golay code C_{24}, a $[24,12]$ binary code with minimum weight 8. Since C is self-dual, the complement of any base is a base, and we simply have to arrange the columns so that the first base occurs as late as possible. A *sextet* is a partition of the 24 coordinates into six *tetrads* or sets of 4, with the property that the union of any two tetrads supports a codeword. Permute the coordinates so that the sets $\{1,2,3,4\}$, $\{5,6,7,8\}$, ..., $\{21,22,23,24\}$ are the tetrads of a sextet. Then the first base contains $1,2,3,4,5,6,7$ but not 8, and $9,10,11$ but not 12. The same argument shows that the last base does not contain 13 or 17, so these are the remaining elements of the first base. Now we can calculate that the number of vertices of the Muder trellis is 2686. On the other hand, we cannot do better. Since the minimum weight of the code is 8, the future subcode F_i is zero for $i > 16$, and so the last possible position for an element of the first base is 17. Similarly, looking at the smallest possible support of a d-dimensional subcode for $d = 2,3,\ldots$, we find upper bounds for the positions of the elements of the first base, and we conclude that the best we can do is as given in the preceding paragraph. This example hints at a connection between the trellis parameters and the Hamming weight hierarchy of a code. Such a connection was worked out by Papadopoulos in his thesis and is given in [1]. It states:

Theorem 8.2 *The first and last base of the* $[n, k]$ *code* C *saatisfy*

$$a_i \leq n - d_{k-i+1}(C) + 1, \qquad b_i \geq d_i(C).$$

References

[1] R. A. Bailey, P. J. Cameron and C. Papadopoulos, Trellis complexity using the first and last bases, in preparation.

[2] A. A. Bruen, J. A. Thas and A. Blokhuis, On M.D.S. codes, arcs in PG(n, q) with q even, and a solution of three fundamental problems of B. Segre, *Inventiones Mathematicae* **92** (1988), 441–459.

[3] C. Greene, Weight enumeration and the geometry of linear codes, *Studia Appl. Math.* **55** (1976), 119–128.

[4] T. Helleseth, T. Kløve and Ø. Ytrehus, Generalized Hamming weights for linear codes, *IEEE Transactions on Information Theory* **38** (1992), 1133–1140.

[5] K. Jain, I. Măndoiu and V. Vazirani, The "art of trellis decoding" is computationally hard—for large fields, *IEEE Trans. Inform. Theory* **44** (1998), 1211–1214.

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Co., Amsterdam, 1977.

[7] D. J. Muder, Minimal trellises for block codes, *IEEE Transactions on Information Theory* **IT-34** (1988), 1049–1053.

[8] C. Papadopoulos, *Codes and Trellises*, Ph.D. thesis, University of London, 1999.

[9] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.

What is an Infinite Design?

P.J. Cameron, B.S. Webb*

The Open University - Milton Keynes, UK
e-mail: <B.S.Webb@open.ac.uk

It is usually assumed that *an infinite design is a design with infinitely many points,* with the added condition that no block contains every point.

This encompasses a myriad of structures, some nice and others not. We are looking at adding conditions to tighten this definition in order to exclude anomalous structures. In particular, we would expect a design to be regular, the complement of a design to be a design, and a t-design to be an s-design, for every $0 < s \leq t$. These are all properties that can be taken for granted with finite designs, and for infinite Steiner systems. Most of the work to date on infinite designs has concerned Steiner systems; they are well behaved, despite being far more numerous than finite Steiner systems (they exist for all $t < k \leq v$, large sets exist for all finite $t < k$, and any Steiner system can be extended).

In this talk, we present examples of structures that we would not like to call designs and investigate which additional conditions guarantee good behaviour.

Constructing Geometries for $PSL(2,11)$

P. Cara*, F. Buekenhout, K. Vanmeerbeek

Department of Mathematics - Vrije Universiteit Brussel
Pleinlaan 2 - B-1050 Brussels, Belgium
e-mail: pcara@vub.ac.be

We present joint work with F. Buekenhout and K. Vanmeerbeek. Computer programs allow us to construct and classify coset geometries with prescribed properties on which a given group acts flag-transitively. Computerfree proofs of existence of these geometries can then be looked for. For the group $PSL(2,11)$ a list of 23 geometries satisfying the RWPRI property was obtained. For each of these we give a geometric construction. A striking fact is that most constructions do not rely on the natural action of $PSL(2,11)$ on 12 points but rather on its sporadic action on 11 points. The set of 11 points on which $PSL(2,11)$ acts 2-transitively will be called the *short Galois line*. Our constructions also use structures on a pair of short Galois lines which are related to the Desargues configuration and the Petersen graph.

A new Family of Flocks in Characteristic 2

W. E. Cherowitzo
Denver, USA
e-mail: wcherowi@carbon.cudenver.edu

C.M. O' Keefe
University of Adelaide, Australia
e-mail: cokeefe@maths.adelaide.edu.au

T. Penttila*
University of Western Australia
e-mail: penttila@maths.uwa.edu.au

There have been few constructions of flocks of the quadratic cone in characteristic 2, with the only families previously known being the linear flocks, the Fisher-Thas-Walker-Kantor-Betten flocks, the Payne flocks, and the Subiaco flocks. There are many corresponding structures, including elation generalized quadrangles, translation planes and herds of ovals.

In the generalized quadrangle setting, the hypothesis that there is a cyclic group acting regularly on the lines through the base point is satisfied by all but the Payne family, and was shown by Payne, Penttila and Royle to lead to further examples for $q = 4^3$, 4^4, 4^5, 4^6, 4^7 and 4^8. Here we give a unified construction of the linear, FTWKB and Subiaco flocks, as well as a new family that we name the Adelaide flocks, which encompasses the examples of Payne, Penttila and Royle.

Some Plane Isoperimetric Inequalities and Applications

A.R. Chouikha

LAGA CNRS UMR 7539 - Mathematics - University of Paris-Nord
Av J.B. Clement - 93430 Villetaneuse, France
e-mail: chouikha@math.uinv-paris13.fr

We present some applications of plane Bonnesen-type isoperimetric inequalities, published in our previous paper [1]. This is related to a conjecture of Paul Levy which asserts:

Let a n-polygon Π_n of sides $a_1, a_2, ..., a_n$, of perimeter L_n and enclosing an area A_n. Define $P_n = \frac{{L_n}^2}{4}\sqrt{(1-\frac{2a_1}{L_n}).....(1-\frac{2a_n}{L_n})}$, then the followings hold $\frac{e}{\pi \leq \frac{A_n}{P_n} \leq 1}$.

This problem has interested many geometers. We propose to discuss some of their contributions and give examples.

References

[21] A. R. Chouikha: *Problems on polygons and Bonnesen-type inequalities*, Indag Math., vol 10 (4), p. 495-506, 1999.

The Steiner Ratio of Several Discrete Metric Spaces

D. Cieslik

University of Greifswald, Germany
e-mail: cieslik@mail.uni-greifswald.de

The “Problem of shortest connectivity”, usually called Steiner’s Problem, is to find for a finite set of points in metric space (X, ρ) a network interconnecting these points with minimal length. Such a network must be a tree, called a Steiner Minimal Tree (SMT). Whereas Steiner’s Problem is very hard as well in combinatorial as in computational sense, the determination of a Minimum Spanning Tree (MST) is simple. Consequently, we are interested in the greatest lower bound for the ratio between the lengths of these both trees:

$$m(X, \rho) := \inf \left\{ \frac{L(\text{SMT for } N)}{L(\text{MST for } N)} : N \subseteq (X, \rho) \text{ is a finite set} \right\},$$

which is called the Steiner ratio (of the space (X, ρ)).
This quantity is a parameter of the considered space and describes the approximation ratio for Steiner’s Problem. It will be present a overview of the exact value and lower or upper bounds for the Steiner ratio of several discrete metric spaces.

Group Testing, Combinatorial Designs and Computational Biology

Preliminary Version

C.J. Colbourn

Computer Science - University of Vermont
Burlington, VT 05405, U.S.A.
e-mail: colbourn@emba.uvm.edu

A revolution in biology is underway, as researchers examine the structure and function of complex biological molecules. Combinatorial methods have long played an important role in these researches, for example in the phylogenetic problem of tracing evolutionary paths. The recent dramatic increase in effort and interest has occurred in part as a result of the focus of the Human Genome Project. It has concurrently generated a comparable dramatic increase in the role of combinatorics in general, and combinatorial designs in particular. These notes do not serve as a detailed introduction to this emerging area. Rather they give an overview and some references for further study.

1 A Problem in Molecular Biology

Let us begin with a motivating example. DNA structure and function are the main foci of much current research. DNA can be thought of as very long but finite sequences of symbols or letters from the alphabet {A,C,G,T}. Natural goals are to first determine the particular sequence which forms the DNA of an organism, and then to relate characteristics of this sequence to biological, chemical, and physical properties, i.e. to understand the function. Simple molecular structures typically have one primary function. On the other hand, DNA exhibits complexity both of structure and of function. Functions appear to be encoded within contiguous fragments. Hence we are concerned both with global and with local structure of the DNA sequence. In general, we are able to test for the presence of certain very short sequences within a DNA fragment; the exact location of the match or matches is in general uncertain. We can also employ certain reactions to partition a long DNA sequence into many shorter ones, "cutting" the sequence whenever a certain subsequence occurs. Both of these processes ought not to be viewed with mathematical exactness. Instead, the presence or absence of certain subsequences is complicated by physical, biological, and chemical similarities to other subsequences. In this setting, locating particular fragments within a large DNA chain, to relate their presence to their function for example, is challenging. An approach which has gained acceptance is to first employ a number of different reactions to partition the same long DNA sequence into many shorter ones, called *clones.* Using multiple reaction mechanisms typically results in the DNA sequence being cut in many different locations, so that in general clones can overlap, and a particular short fragment of DNA may be covered by many clones. The clones produced in this manner form a *clone library.* Clones are chosen so that they are simple enough to analyze and sequence directly; so that they cover the entire DNA string, typically with all sections appearing in at least two clones; and so that they are long enough to be recognizable (for the most part) within the entire DNA sequence. Then to locate a particular short sequence within the DNA string, we search for similarities between this string and the clones. To do this, we employ our ability to test for the presence of very short fragments, called *sequenced tagged sites.* When one is present in the desired string, knowledge of the clones in which it appears restricts the possible locations within the entire DNA string. By comparing our target string against the clones using a number of different sequenced tagged sites, we can determine the location of our string with some exactness. ¿From a practical viewpoint, we are not finished. Testing each clone individually is time-consuming and expensive. However, we can accelerate this process dramatically by testing many clones at the same time rather than testing them one at a time. Naturally, in the process we lose our ability to distinguish *which* clone matched, but not the information that some clone of the selection matched. Our brief tour of some problems in DNA structure examination leads us then to a natural combinatorial problem, which has been studied for many years. We take up this topic next, from a mathematical viewpoint.

2 The Framework

A population $\mathcal{P}$ of b items contains a number d of *defective* items, and the remaining $b-d$ items are *good.* Items can be pooled together for testing: for a subset $X \subseteq \mathcal{P}$, the *group test* reports "yes" if X contains one or more defective elements, and reports "no" otherwise. The objective is to determine, using a number of group tests, precisely which items are defective. When group tests are all undertaken in parallel, the problem is *nonadaptive*; otherwise it is *adaptive.* Then results from one or more tests are available while constructing further pools to be tested. Among adaptive testing methods, some operate in a limited number of stages or rounds. Group testing was first studied in screening large populations for disease [15], and with the advent of large-scale HIV screening, it has grown in importance. It has also arisen in satellite communications [6, 30]. In this application, a large number of ground stations which rarely communicate share a satellite link. Rather than polling the ground stations individually, pools of the ground stations are formed as part of the system design. When the satellite enters a phase of accepting requests for reservations of time slots, it polls each pool and from the positive results on the pools it determines which ground stations wish to transmit. The satellite may have many positive responses within one pool, but detects only that there is at least one response. Hence, while cosmetically similar to the optical communication situation, this problem encounters unions rather than sums of colliding signals. A further application arises in the construction of frameproof codes, which are designed to avoid coalitions of users forging the signature of a user not in the coalition; see [27, 28]. In this paper, the primary application explored arises in mapping genomes. To determine where a particular sequence is located within the genetic material, we conduct a test to determine in which of the clones it appears. Pooling of different clones can then be used [1, 2, 3, 4, 8, 19, 21, 24, 25].

3 The Role of Combinatorial Designs

Let $\mathcal{P}$ be a set of b items, and let $\mathcal{X}$ be a collection of subsets of $\mathcal{P}$ corresponding to the group tests performed. Then $(\mathcal{P}, \mathcal{X})$ is a solution to the nonadaptive group testing problem if and only if, for any possible sets D_1 and D_2 of defective items, $\{X : D_1 \cap X \neq \emptyset,\ X \in \mathcal{X}\} = \{X : D_2 \cap X \neq \emptyset,\ X \in \mathcal{X}\}$ only if $D_1 = D_2$. The dual of a solution $(\mathcal{P}, \mathcal{X})$ is a pair $(V, \mathcal{B})$, where the v group tests of $\mathcal{X}$ are in one-to-one correspondence with the points of V, and the b items are in correspondence with the blocks of $\mathcal{B}$ (for each item, the corresponding block contains the elements corresponding to the group tests containing the item). Typically $(V, \mathcal{B})$ is referred to as a solution to the group testing problem; the goal is to maximize the number of blocks (items tested) as a function of the number of points (group tests performed). Often it is known with high probability that the number of defectives d does not exceed some threshold value p. In the *hypergeometric* problem, the number of defectives is assumed never to exceed p, and hence it is necessary that $(V, \mathcal{B})$ has the union of any two distinct sets, each containing at most p blocks, themselves distinct. In the *strict* problem, it is necessary to identify the set of defective items correctly when $d \leq p$ and to report when dp. In the latter case, the specific set of defective items need not be determined, however. Now consider a solution $(V, \mathcal{B})$ to the nonadaptive group testing problem with d defectives. Form a $|V| \times |\mathcal{B}|$ incidence matrix. This matrix has the property that the unions of two sets of at most d columns are distinct. The matrix is then called $\overline{d}$-*separable* [16], and the corresponding set system is *d-union free* [18, 20]. The columns of a $\overline{d}$-separable matrix form a superimposed code [17, 23] which permits up to d simultaneously transmitted codewords to be unambiguously decoded. The decoding technique appears somewhat involved, because we could in principle be required to examine all unions of up to d columns. Hence a related family of matrices (or codes, or set systems) arises. If the incidence matrix contains no collection of d columns whose union covers a column not in the collection, then M is a d-*disjunct* matrix. If a disjunct matrix is employed, there is a simple decoding mechanism, observing that all codewords covered by the received union are 'positive'. Equivalently, we can alter the condition on the set system to require that it is d-*cover free*, i.e. that no union of d or fewer blocks contains another. Evidently, a d-cover free family is also d-union free. Probabilistic bounds on the maximum numbers of blocks in cover free and union free families are available [16]; see [17, 26] for upper bounds for cover free families. See [13] for progress in the union free case. Erdős, Frankl, and Fűredi [18] established that among cover free families with constant block size, the maximum is realized by a Steiner t-design $\mathrm{S}(\ell, 2\ell-1, m)$; indeed Balding and Torney [3] recommend the use of an S(3,5,65) in a genetic application. For union free families, Frankl and Fűredi [20] noted that Steiner triple systems give the largest 2-union free families when the block size is three; by permitting block size *at most* three, Vakil and Parnes [29] established a somewhat larger exact bound using group divisible designs with block size three. In the *error correction* version of group testing, some group tests are permitted to report "false positives"; an *a priori* bound q on the number of such false positives is assumed. Balding and Torney [2] observed that $(V, \mathcal{B})$ is a solution to the strict group testing problem with threshold p and error correction for q false positives if and only if, for every union of p or fewer blocks, every other block contains at least $q+1$ points not in this union. Any packing $(V, \mathcal{B})$ of t-sets into k-sets having $k \geq p(t-1)+q+1$ is a solution to the strict group testing problem with threshold p and error correction for q false positives. A Steiner system $\mathrm{S}(t, 2t-1, v)$ is a solution to the strict group testing problem with $p = 2$ and $q = 0$ that has the maximum number of blocks of any solution [2]. Finally, we consider the use of combinatorial designs in two-stage group testing. Here the objective in a first stage of pools is not to identify all defectives precisely, but rather to identify a small subset of the items which is guaranteed to contain all defective items. Frankl and Fűredi call a family of sets d-*weakly union free* if, whenever two *disjoint* sets of blocks are chosen, each containing d or fewer blocks, their unions are distinct. A 2-weakly union free family with block size three provides pools for a group testing method for $d = 2$, in which a set of at most three potential defectives are identified [10]. Moreover, while union free families have no more blocks than a Steiner triple system has, weakly union free families can have twice as many blocks [20]. Chee, Colbourn, and Ling [10] established that certain twofold triple systems realize the bound. Not any twofold triple system forms a weakly union free family; four forbidden configurations of four blocks each must be avoided. Again, while the bound of Frankl and Fűredi [20] suggests that designs can realize the maximum, the particular designs needed require additional structural properties [10]. Applications of designs in general in two-stage group testing appear to be just being explored; see [5] for useful observations.

4 Closing Remarks

Nonadaptive group testing finds the most natural applications in molecular biology, as a consequence of the difficulty of each test to be performed on a pool. The close connections between applications and the combinatorial framework outlined here are already well established in communications, and are emerging in cryptography. However, the connection with the analysis of complex molecular structure appears to be the largest new source of interesting and difficult problems in design theory and related discrete mathematics.

Acknowledgments

Thanks to Jeff Bond, Alan Ling, and David Torney for stimulating discussions on this subject, and to Myra Cohen for helpful comments. The author's research is supported by ARO grant DAAG55-98-1-0272.

References

[1] D. J. Balding, W. J. Bruno, W. J. Knill, and D. C. Torney, A comparative survey of non-adaptive pooling designs, in: *Genetic Mapping and DNA Sequencing*, IMA Mathematics and Applications 81, Springer-Verlag, Berlin, pp. 133–154.

[2] D. J. Balding and D. C. Torney, Optimal pooling designs with error detection, *Journal of Combinatorial Theory (A)* **74** (1996), 131–140.

[3] D. J. Balding and D. C. Torney, The design of pooling experiments for screening a clone map, *Fungal Genetics and Biology* **21** (1997), 302–307.

[4] E. Barillot, B. Lacroix, and D. Cohen, Theoretical analysis of library screening using an n-dimensional pooling strategy, *Nucleic Acids Research* **19** (1991), 6241–6247.

[5] T. Berger and J. W. Mandell, Bounds on the efficiency of two-stage group testing, preprint, Cornell University, 1998.

[6] T. Berger, N. Mehravari, D. Towsley and J. Wolf, Random multiple-access communications and group testing, *IEEE Transactions on Communications* **32** (1984), 769–778.

[7] A. P. F. Bottoli, K. Kertesz-Chaloupkova, R. P. Bouliane, J. D. Granado, M. Aebi, and U. Kues, Rapid isolation of genes from an indexed genomic library of *C. cinereus* in a novel `pab1` cosmid, *J. Microbiological Methods 35* (1999), 129–141.

[8] W. J. Bruno, D. J. Balding, E. H. Knill, D. Bruce, C. Whittaker, N. Doggett, R. Stallings and D. C. Torney, Design of efficient pooling experiments, *Genomics* **26** (1995), 21–30.

[9] K.A. Bush, W.T. Federer, H. Pesotan and D. Raghavarao, New combinatorial designs and their applications to group testing, *Journal of Statistical Planning and Inference* **10** (1984), 335-343.

[10] Y. M. Chee, C. J. Colbourn and A. C. H. Ling, Weakly union-free twofold triple systems, *Annals Combinatorics* **1** (1997), 215–225.

[11] C. J. Colbourn and J. H. Dinitz (editors), *CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton FL, 1996.

[12] C. J. Colbourn and A. Rosa, *Triple Systems*, Oxford University Press, 1999.

[13] D. Coppersmith and J. B. Shearer, New bounds for union-free families of sets, *Electron. Journal of Combinatorics* **5** (1998), #R39.

[14] R. P. Curnow and A. P. Morris, Pooling DNA in the identification of parents, *Heredity* **80** (1998), 101–109.

[15] R. Dorfman, The detection of defective members of a large population, *Annals of Mathematical Statistics* **14** (1943), 436–440.

[16] D. Z. Du and F. K. Hwang, *Combinatorial Group Testing and Its Applications*, World Scientific, Singapore, 1993.

[17] A. D'yachkov, V. Rykov and A. M. Rashad, Superimposed distance codes, *Problems Control and Information Theory* **18** (1989), 237–250.

[18] P. Erdős, P. Frankl and Z. Fűredi, Families of finite sets in which no set is covered by the union of two others, *Journal of Combinatorial Theory (A)* **33** (1982), 158–166.

[19] M. Farach, S. Kannan, E. Knill, and S. Muthukrishnan, Group testing problems in experimental molecular biology, Technical Report, Los Alamos National Laboratory, 1994.

[20] P. Frankl and Z. Fűredi, A new extremal property of Steiner triple systems, *Discrete Mathematics* **48** (1984), 205–212.

[21] E. D. Green and M. V. Olson, Systematic screening of yeast artificial chromosome libraries by the use of the polymerase chain reaction, *Proc. Natl. Acad. Sci. U.S.A.* **87** (1990), 1213–1217.

[22] F.K. Hwang and V.T. Sós, Non-adaptive hypergeometric group testing, *Stud. Sci. Math. Hung.* **22** (1987), 257-263.

[23] W. H. Kautz and R. R. Singleton, Nonrandom binary superimposed codes, *IEEE Transactions on Information Theory* **10** (1964), 363–377.

[24] E. Knill, W. J. Bruno, and D. C. Torney, Non-adaptive group testing in the presence of errors, *Discrete Applied Math.* **88** (1998), 261–290.

[25] A. J. Macula, Probabilistic nonadaptive and two-stage group testing with relatively small pools and DNA library screening, preprint, SUNY at Geneseo, 1998.

[26] M. Ruszinkó, On the upper bound of the size of the r-cover-free families, *Journal of Combinatorial Theory (A)* **66** (1994), 302–310.

[27] D. R. Stinson, Tran van Trung and R. Wei, Secure frameproof codes, key distribution patterns, group testing algorithms, and related structures, *Journal of Statistical Planning and Inference*, to appear.

[28] D. R. Stinson and R. Wei, Combinatorial properties and constructions of traceability schemes and frameproof codes, *SIAM Journal of Discrete Mathematics* **11** (1998), 41–53.

[29] F. Vakil and M. Parnes, On the structure of a class of sets useful in nonadaptive group testing, *Journal of Statistical Planning and Inference* **39** (1994), 57–69.

[30] J. K. Wolf, Born again group testing: multiaccess communications, *IEEE Transactions on Information Theory* **IT-31** (1985), 185–191.

Linear Sections of Line Grassmannians Over Finite Fields

A. Cossidente

Università della Basilicata - Potenza, Italy

A. Siciliano*

Università "Federico II" - Napoli, Italy
e-mail: sicilian@mat.uniroma1.it

Linear sections of line Grassmannians over finite fields are studied. In a recent paper B.N. Cooperstein studied subspaces which miss these projective varieties. Using Singer Cycles, an alternative contruction of maximal dimension linear subspaces disjoint from Grassmannians is given.

Matroids and Tensor Algebra

H. Crapo*

CAMS, EHESS, 54 bd Raspail, 75230 Paris Cedex, France
e-mail: crapo@ehess.fr

W. Schmitt

University of Memphis, Memphis, TN 38152, USA
e-mail: wschmitt@memphis.edu

1 Introduction

Our topic today is a new development: the Whitney algebra of a matroid. We here present, with some indications of the role Gian-Carlo Rota played in its development, the outlines of our recent work on matroids and an associated tensor algebra. Our results were announced at the memorial session of the A.M.S. in Washington, D.C. in January 2000, and were first published [11] in the Rota Memorial issue of the JCT(A). We take the unusual measure of composing the following text in the first person of the first of the two coauthors, as he will be presenting this text at the Gaeta meeting. But rest assured that this a question of style, not content.

Let me preface our report on the Whitney algebra by remarks in a somewhat broader context, recalling work I did with Gian-Carlo Rota, work which, one November day in 1995, began to crystallize into this new subject. Gian-Carlo Rota's views on the Whitney algebra are fortunately recorded in a series of messages by electronic mail, and in the notebooks he filled during our discussions. It is a pleasure to reread Gian-Carlo's comments and advice, since they convey so keenly his enthusiasm for the subject, and provide yet another proof of his uncanny intuition for algebraic structures in combinatorics. As with so many of Rota's long range predictions, this one has taken years to sort out, but I can assure the reader that his assessment of the situation was brutally correct. As predicted, the abstract play of coordinates on a matroid points us to a natural algebraic structure – a lax Hopf algebra – that is "not quite a Hopf algebra, but a new object closely related to it", and that may find wide use far from its birthplace in matroid theory.

2 Higher Order Syzygies

Gian-Carlo and I met frequently during the past decade to discuss what we liked to call 'higher order syzygies'. Let me explain. Say you start with a finite set of n_1 vectors spanning a vector space V of rank n_0. The linear relations among those vectors will then form a vector space of rank $n_1 - n_0$. If we choose a set of n_2 vectors spanning that space, the linear relations among those n_2 vectors will form a vector space of rank $n_2 - n_1 + n_0$, ainsi de suite. The vector spaces spanned at each level of the resolution, we called the spaces of *syzygies*, respectively of order 0 (the vector space V itself), order 1 (spanned by the n_1 linear relations), order 2, etc. Fortunately, there is a natural choice of syzygies at each stage: take all relations of *minimal support.* Any linear relation of minimal support is (for any given support set) uniquely determined up to an overall scalar multiple, and is thus best considered as a *projective point.* In particular, the projective configuration whose points are the support sets of first order syzygies, that is, minimal dependent subsets of P, we called the *geometry of circuits.* borrowing the term 'circuit' from matroid theory. In this way, the study of higher order syzygies becomes the study of a sequence of configurations of projective points. These can be studied algebraically, geometrically, even combinatorially. Gian-Carlo and I sensed that there were fascinating combinatorial structures here, yet to be discerned, structures that could shed light on the deeper mysteries of representation theory. If, instead of a specific set P of vectors in a vector space, or configuration of projective points, we simply have the combinatorial information as to which subsets of P are independent, which dependent, that is, if we have only its *matroid*, then the minimal support sets of the first order syzygies are uniquely determined, but the higher order syzygies are not. A simple example: for six points a, b, c, d, e, f in the plane, the uniform matroid $M_{6,3}$, the four circuits $abcd, abef, cdef$ have rank 3 for most representations of the matroid, but have rank 2, and become collinear in the geometry of circuits, if and only if the lines ab, cd, ef are concurrent in the plane. This distinction is *not* carried by the matroid. The idea of the geometry of circuits of a configuration of points came out of earlier (1983) work on rigidity and scene analysis [4]. If the matroid in question is the uniform matroid $M_{p,n}$ on a set P of p points in general position, rank n, then the circuits are all $(n+1)$-element subsets of P, supports of the 'elementary' first order syzygies. The geometry of circuits is the Dilworth completion of the n-fold lower truncation of the Boolean algebra $B(P)$. The combinatorics of the Dilworth completion, where flats are defined by a clever minimization of rank sums over partitions, thus provided the first practical information about the structure of second order syzygies in simple configurations [5]. Gian-Carlo and David Anick made a big step forward in 1991, with their resolution of the bracket ring [7]. For uniform matroids they identified spanning sets of syzygies of all orders, of a particularly simple form. Syzygies of order k can always be written as linear combinations of syzygies of order $k-1$, using 'scalar' coefficients from the bracket ring. Anick and Rota restricted their attention to a class of linear combinations with *single bracket coefficients*. These syzygies they found to be in natural bijection with a well-defined class of *non-standard tableaux*. They characterized an appropriate boundary operator acting on non-standard tableau that 'returned' the syzygy in question. They provided me with an advance copy of their article; I set to work rewriting it [9]. I was able to show that the boundary operator could be expressed as the action of a sum of certain products of elementary straightening operations (working on various pairs of consecutive rows of the tableau). The products (of idempotent operators) in question are those produced by a finite state automaton. One biproduct of this adventure was a computer program for the Anick-Rota resolution. To avoid the doubly exponential behavior of the usual straightening algorithms, I implemented the Rutherford method of *interpolation*, used by Jacques Désarménien in his work with Rota on bitableaux [2][3], and as promoted and improved by Christophe Carré, Alain Lascoux, and Bernard Leclerc [8]. We will come back to this below, since it is the also the key to straightening in Whitney algebras. In the early 1990's, we worked mostly on what Gian-Carlo dubbed the 'resolving bracket', a way of turning the geometry of circuits into a Peano space [10]. We often looked for ways to unify this approach with the Anick-Rota resolution, or better, to carry out the necessary calculations using a meet operator in an appropriate Cayley algebra. Gian-Carlo and I met whenever and wherever we could, usually twice a year, in Milano, in Firenze, in Strasbourg, in Los Angeles, or of course in Cambridge.

3 Tensor expressions for linear dependence

What turned out eventually to be the main line of attack arose quite unexpectedly. Gian-Carlo realized he could build a new geometric theory around one simple idea: that linear dependencies are more naturally expressed as *equations in the tensor algebra of an exterior algebra,* rather than as linear combinations of points over the bracket ring. In prior work, Gian-Carlo and his coauthors had expressed the fact that a set, say *abcde*, was dependent by writing

$$[abcd]\, e \;-\; [abce]\, d \;+\; [abde]\, c \;-\; [acde]\, b \;+\; [bcde]\, a \;=\; 0,$$

a reasonable expression if the five points span a space of rank 4. If three points a, b, c are collinear (of rank 2) in a space of rank 4, Rota *et al* were forced to employ two extraneous general points d, e, to express this fact in the form

$$[abde]\, c \;-\; [acde]\, b \;+\; [bcde]\, a \;=\; 0,$$

using a procedure they called 'filling brackets'. But in fact it's both simpler and more natural to write

$$ab \otimes c \;-\; ac \otimes b \;+\; bc \otimes a \;=\; 0, \qquad (1)$$

where ab, ac, bc are *extensors*, wedge products of points. Let's see what this means. Consider a matrix C, whose rows coordinatize three collinear points:

$$C \;=\; \begin{array}{c} a \\ b \\ c \end{array} \begin{pmatrix} 0 & -3 & -5 & 9 \\ 9 & 6 & 4 & 0 \\ 5 & 2 & 0 & 4 \end{pmatrix}$$

The row vectors are dependent, for example with $4a + 5b - 9c = 0$. The scalar coefficients of the linear relation among these three points can be computed as *minors* in any two independent columns of the matrix C, as in the calculation

$$a \begin{vmatrix} 9 & 4 \\ 5 & 0 \end{vmatrix} \;-\; b \begin{vmatrix} 0 & -5 \\ 5 & 0 \end{vmatrix} \;+\; c \begin{vmatrix} 0 & -5 \\ 9 & 4 \end{vmatrix} \;=\; 0,$$

where we formed the minors using columns 1 and 3. This is just Cramer's rule, as Gian-Carlo liked to say. But these minors are Grassmann coordinates; rewrite this as:

$$a\,(bc)_{13} \;-\; b\,(ac)_{13} \;+\; c\,(ab)_{13} \;=\; 0$$

This equation holds for *all* pairs of indices (trivially so for indices of dependent pairs of columns):

$$a\,(bc)_{jk} \;-\; b\,(ac)_{jk} \;+\; c\,(ab)_{jk} \;=\; 0$$

so we arrive at the equation (1), an equation in tensor products of extensors. By symmetry of point of view relative to the two tensor 'positions', equation (1) also yields a spanning set of linear relations among the three extensors ab, ac, bc. Since the three pairs of points all have the same span, the extensors ab, ac, bc differ from each other only by a scalar multiple. In Grassmann coordinates they are, respectively, $-9, -5$, and 4 times the vector

$$\begin{array}{cccccc} 12 & 13 & 14 & 23 & 24 & 34 \\ \end{array}$$
$$\begin{pmatrix} -3 & -5 & 9 & -2 & 6 & 4 \end{pmatrix}$$

The space of linear relations among ab, ac, bc has rank 2, spanned by any of the columns of matrix C, that is:

$$a_i\,(bc) \;-\; b_i\,(ac) \;+\; c_i\,(ab) \;=\; 0,$$

expressions obtained by acting on equation (1) by a linear functional: $i^{\mathbf{th}}$ coordinate projection of the vector in the first tensor position. Another way of interpreting the tensor equation (1), that better explains how it arises, is to observe that the scalar expression

$$a_i \circ (bc)_{jk} - b_i \circ (ac)_{jk} + c_i \circ (ab)_{jk}$$

is a Laplace expansion of $(abc)_{ijk}$, the ijk-coordinate of the wedge product abc. Since the set $\{a, b, c\}$ is linearly dependent, the product abc is zero, so all its coordinates (3×3 minors of the matrix C) are zero. Equation (1) is thus keeping track of those algebraic relations among *non-zero* coordinates of vectors and wedge products of vectors that follow from the fact that $abc = 0$. The origins of tensor equations such as (1) are most clearly revealed, however, by the Hopf algebra structure of the exterior algebra $\Lambda = \bigoplus \Lambda^k$. Recall that the coproduct $\delta : \Lambda \to \Lambda \circ \Lambda$ is the multiplicative map determined by $\delta(a) = a \circ 1 + 1 \circ a$, for all vectors $a \in \Lambda^1$; for example,

$$\begin{aligned} \delta(abc) &= \delta(a)\,\delta(b)\,\delta(c) \\ &= abc \circ 1 \;+\; ab \circ c \;-\; ac \circ b \;+\; bc \circ a \\ &\qquad\qquad +\; c \circ ab \;-\; b \circ ac \;+\; a \circ bc \;+\; 1 \circ abc, \end{aligned}$$

for vectors a, b, c (where the signs are determined by anticommutativity). Now if the set $\{a, b, c\}$ is dependent, then the wedge product abc is equal to zero in Λ, and hence the coproduct $\delta(abc)$ is also zero. Since Λ is graded by the nonnegative integers $\mathbf{N}$, the tensor product $\Lambda \circ \Lambda$ is thus graded by $\mathbf{N} \times \mathbf{N}$, and an element of $\Lambda \circ \Lambda$ is equal to zero if and only if all its $(\mathbf{N} \times \mathbf{N})$-homogeneous components are zero. Hence, in particular, if $\{a, b, c\}$ is linearly dependent, then the homogeneous component $a \circ bc - b \circ ac + c \circ ab$ of *shape* $(1, 2)$ in the coproduct $\delta(abc)$ is equal to zero; in other words, Equation (1) holds. We obtain similar relations in each component $T^k(\Lambda) = \Lambda \circ \cdots \circ \Lambda$ of the tensor algebra $T(\Lambda) = \bigoplus T^k(\Lambda)$ from the fact that the iterated coproduct $\delta^k(a_1 \cdots a_r)$ is zero for any dependent set of vectors $\{a_1, \ldots, a_r\}$. So that's ultimately what's hidden in that innocent-looking tensor equation!

4 A flurry of electronic mail

In November 1995 Gian-Carlo and I began to take seriously the idea that the abstract 'play of coordinates' in a geometric configuration was best expressed in a tensor product of exterior algebras. It was the possible connection between Hopf algebras and combinatorial geometry that whetted Gian-Carlo's appetitite. We began an exchange of electronic mail on what Gian-Carlo soon dubbed *the Whitney algebra of a matroid*. Work began in earnest over the winter holidays, and reached a climax in January 1966, thanks to a heavy snowfall that stranded Rota in Cambridge for several days. By October of that year, our correspondence ran to some 100 pages of text.

18 November, 1995 — Telephone call from Rota. He finds that the 'tensor-product' approach to non-spanning syzygies is correct, that is, that

$$a \otimes bc - bc \otimes ac + c \otimes ab$$

is the zero *tensor* whenever a, b, c are collinear points (dependent vectors) in *any* space, and gives a Hopf-algebra structure on an arbitrary matroid, potentially replacing the 'bracket ring', which had the disadvantage of being commutative. Idea: in an exterior algebra generated by formally independent points, set to zero all joins of dependent sets of points, and their coproducts.

> **22 November, 1995** — I just read your fax, it is exactly what I was thinking. I have gone a little further in the formalization of the Hopf algebra of a matroid, so far everything checks beautifully. The philosophical meaning of all this is that every matroid has a natural coordinatization ring, which is the infinite product of copies of a certain quotient of the free exterior algebra generated by the points of the matroid (loops and links allowed, of course). This infinite product is endowed with a coproduct which is not quite a Hopf algebra, but a new object closely related to it. Roughly, it is what one obtains when one mods out all coproducts of minimal dependent sets, and this, remarkably, give all the exchange identities. I now believe that everything that can be done with the Grassmann-Cayley algebra can also be done with this structure, especially meets.
>
> **28 November, 1995** — I will send you material as soon as I physically can. Everything works beautifully, and we have defined a new concept of independent algebraic interest: Whitney algebras, which generalize Hopf algebra in a way that is so natural that it will make the Hopf algebraists envious. Your latest fax was very helpful, but I will have to explain to you the main idea. I think there may be even an interpretation of the critical problem for general matroids! This is an idea of yours that is really bearing fruit.
>
> **29 November, 1995** — I will try to write down something tonight and send it to you by latex. I still think this is the best idea we have been working on in years, and all your past work on syzygies will fit in beautifully.
>
> **20 December, 1995** — I am working on your ideas, trying to recast them in letterplace language. I tried to write down something last night, but I was too tired. Things are getting quite rough around here.
>
> **9 January, 1996** — Thanks for the message. I am snowbound in Cambridge, and won't be leaving for Washington until Friday, at least, so I hope to redraft the remarks on Whitney algebras I have been collecting. It seems that we will have to translate Tutte's homotopy

> theorem into the language of Whitney algebras, using circuits instead of copoints. Has the theorem been restated in terms of circuits (as it can, by taking complements)? If it has, I would appreciate your sending me the statement, it will save me quite a bit of work. Neil White has a translation into the language of brackets, and I am working with his translation.
>
> Here are some philosophical remarks. First, all of linear algebra should be done with the Whitney algebra, no scalars ever mentioned. Second, there is a new theorem to be stated and proved preliminarily, which seems to be a vast generalization of the second fundamental theorem of invariant theory. (Why, Oh why, did I not see this before?!)[1] I think this is the first step towards proving the big theorem. It is already difficult, and I would appreciate your help.
>
> Another priority is to see following your lead how to completely get rid of meets, using Whitney algebra techniques. The point is to prove classical determinant identities, such as Jacobi's identity, using only Whitney algebra methods (with an eye towards their quantum generalizations!) Only by going through the Whitney algebra proofs will we see how to carry out a quantum generalization of all this stuff.
>
> It is of the utmost importance that you familiarize yourself with the letterplace representation of the Whitney algebra, through the Feynman operators, and I will write up this stuff first and send it to you.

Two days later, still snowbound in Cambridge, Gian-Carlo composed a long piece on his strategy for the Whitney algebra. I'll show you this in at the end of the talk, but first we should bring the story quickly up to date, and take a closer look at the Whitney algebra. It was a busy Spring, with many visitors arriving at M.I.T. for the RotaFest. In September, Bill Schmitt, an expert on Hopf algebras in combinatorics, made a stop-over in Paris, enroute for a fall term visit at M.I.T. At the conclusion of this visit, he and I proposed to collaborate with Gian-Carlo in an effort to develop the theory of Whitney algebras. The three of us met in Gian-Carlo's Cambridge apartment late in October 1996, to map out the project. This was regrettably to be our only three-way discussion of the subject. It was not until the summer of 1997 that Bill and I had the occasion to work together over an extended period. We found a basic cancellation property in exterior algebra, which we call the 'Zipper lemma'. From this we were able to derive the exchange relations for a Whitney algebra. We then set out to settle the question: in precisely what

[1] Gian-Carlo here suggests a comparison between the Whitney algebra of a vector space, when viewed as a matroid, and its exterior algebra.

sense is the Whitney algebra a generalization of a Hopf algebra? The resulting categorical setting, and in particular the concept of lax Hopf algebra, are quite recent developments due to Bill Schmitt.

5 The free exterior algebra on a finite set

Given a linearly ordered finite set S of *letters*, the *free R-exterior algebra* $E(S)$ is the free R-algebra on S, with concatenation product of words, modulo the ideal I generated by squares aa of letters a and sums $ab + ba$ for pairs a, b in S. The free exterior algebra $E(S)$ is freely generated as an R-module by monotone words. $E(S)$ is a Hopf algebra, with coproduct $\delta a = a \otimes 1 + 1 \otimes a$ and antipode $\chi(w) = (-1)^{|w|}\, w$. If S is a basis for a finite dimensional vector space V, then $E(S)$ is isomorphic to the exterior algebra $\Lambda(V)$. The zipper lemma, below, is expressed in terms of generalized binomial coefficients $\binom{n}{k}$ with value 0 for negative k, but with appropriate non-zero values for negative values of n. These are given by

$$\binom{n}{k} \;=\; \begin{cases} \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots(1)} & \text{for } k > 0 \\ 1 & \text{for } k = 0 \end{cases}$$

This means that for $n \geq 0$, $\binom{n}{k}$ counts, as usual, k-element subsets of an n element set, while for $n \leq 0$, it is equal to

$$(-1)^k \binom{k + |n|}{k},$$

and counts k element multi-sets formed from an n-element set. These generalized binomial coefficients still obey the usual recursion

$$\binom{n}{k} \;=\; \binom{n-1}{k-1} \;+\; \binom{n-1}{k}.$$

An alternating sum of these recursion steps produces the usual cancellation: for all integers n, k, p, with $p \geq 0$,

$$\sum_{i=0}^{p} (-1)^i \binom{n}{k+i} \;=\; \binom{n-1}{k-1} \;+\; (-1)^p \binom{n-1}{k+p}. \tag{2}$$

For small values of n and k, they are given by the array

$$\begin{array}{rc|rrrr|}
n & k & 0 & 1 & 2 & 3 \\
3 & & 1 & 3 & 3 & 1 \\
2 & & 1 & 2 & 1 & 0 \\
1 & & 1 & 1 & 0 & 0 \\
0 & & 1 & 0 & 0 & 0 \\
-1 & & 1 & -1 & 1 & -1 \\
-2 & & 1 & -2 & 3 & -4 \\
-3 & & 1 & -3 & 6 & -10
\end{array} \tag{3}$$

The following cancellation theorem, holding in the free exterior algebra on a set, considered as a Hopf algebra, will lead us directly to the exchange relations that hold in Whitney algebras. For any subwords (not necessarily consecutive letters) u and v of a monotone word $w = a_1 \cdots a_r$, write $u \prec v$ to indicate that if $u = a_{i_1} \cdots a_{i_k}$ then v is equal to $a_{i_k+1} \cdots a_r$, the final word in w, following all elements of u.

Theorem 1 (The Zipper Lemma) *For $0 \leq k \leq r$, and for any word w of length r,*

$$\begin{aligned} \sum_{\substack{(w)_{(r-k+1,\cdot,\cdot)} \\ w_{(1)} \prec w_{(2)}}} \delta(w_{(1)}) \, (\, \chi(w_{(2)}) \circ w_{(3)}) &= \sum_{j=0}^{r} \binom{j-1}{k-1} \, \delta_{r-j,j} \, (w) \\ &= (-1)^{k-1} \, w \circ 1 \; + \; \delta_{r-k,k} \, (w) \\ &\qquad + \{\textit{terms of shape } (r-l,l) \textit{ for } l > k\} \end{aligned} \tag{4}$$

Granted, this is not the sort of formula one digests at first glance. A few examples will illustrate the extensive cancellation which there occurs, and the reason for the appearance of the binomial coefficients. It may then be clear why the Zipper (itself a theorem in exterior algebra) becomes the key to exchange properties in the Whitney algebra, where the terms of shape $(r-l,l)$, for $l > k$, will all be zero. The simplest non-trivial case of the Zipper is that for $r = k = 2$, where

$$\delta(a)\,(b \circ 1) \; + \; \delta(b)\,(1 \circ a) \; = \; (ab \circ 1 - b \circ a) \; + \; (b \circ a - 1 \circ ab) \; = \; ab \circ 1 \; - \; 1 \circ ab$$

For $r = 4$, $k = 3$, all monomial terms cancel except for those of shapes $(4,1)$, $(1,3)$, and $(1,4)$:

$$\begin{aligned} & + \delta(ab)\,(cd \circ 1) \; - \; \delta(ac)\,(d \circ b) \; + \; \delta(bc)\,(d \circ a) \\ & + \delta(ad)\,(1 \circ bc) \; - \; \delta(bd)\,(1 \circ ac) \; + \; \delta(cd)\,(1 \circ ab) \\ = \quad & abcd \circ 1 \; + \; (a \circ bcd - b \circ acd + c \circ abd - d \circ abc) \; + \; 3\,(1 \circ abcd) \\ = \quad & (\delta_{(4,1)} \; + \; \delta_{(1,3)} \; + \; 3\delta_{(1,4)})\; abcd. \end{aligned}$$

The full extent of cancellation in the zipper lemma is best revealed in tabular form, below. Take $r = 5$, $k = 4$. The columns of the table are labelled by the expressions abbreviated as follows:

$ab:$	$+\,\delta(ab)\,(cde \circ 1)$	$ac:$	$+\,\delta(ac)\,(de \circ b)$
$bc:$	$-\,\delta(bc)\,(de \circ a)$	$ad:$	$+\,\delta(ad)\,(e \circ bc)$
$bd:$	$-\,\delta(bd)\,(e \circ ac)$	$cd:$	$+\,\delta(cd)\,(e \circ ab)$
$ae:$	$+\,\delta(ae)\,(1 \circ bcd)$	$be:$	$-\,\delta(be)\,(1 \circ acd)$
$ce:$	$+\,\delta(ce)\,(1 \circ abd)$	$de:$	$-\,\delta(de)\,(1 \circ abc)$,

respectively, and contain the signs of the various monomials (given as row labels) occurring in the expansions of those expressions. The total coefficient of each monomial is shown in the final column T.

	ab	ac	bc	ad	bd	cd	ae	be	ce	de	T
$abcde \circ 1$	$+$										$+1$
$acde \circ b$	$-$	$+$									0
$bcde \circ a$	$+$		$-$								0
$ade \circ bc$		$-$		$+$							0
$bde \circ ac$			$+$		$-$						0
$cde \circ ac$	$+$	$-$	$-$			$+$					0
$ae \circ bcd$				$-$			$+$				0
$be \circ acd$					$+$			$-$			0
$ce \circ abd$						$-$			$+$		0
$de \circ abc$		$-$	$-$	$+$	$+$	$+$				$-$	0
$a \circ bcde$							$-$				-1
$b \circ acde$								$+$			$+1$
$c \circ abde$									$-$		-1
$d \circ abce$										$+$	$+1$
$e \circ abcd$				$+$	$+$	$+$	$-$	$-$	$-$	$-$	-1
$1 \circ abcde$							$-$	$-$	$-$	$-$	-4

so the sum is equal to

$$(\delta_{(5,1)} \;-\; \delta_{(1,4)} \;-\; 4\delta_{(1,5)})\; abcde.$$

Notice that the non-zero signs in any row, for blocks of columns labelled by terms in which the coproduct acts on words with the same last letter, are constant, and that the number of such signs is a binomial coefficient. The cancellations giving 0 in column T are in this way the result of formula (2). The coefficients in column T, for any block of rows labelled by monomials of the same shape, combine those labels into a coproduct slice. The coefficients thus obtained for the various coproduct slices, $1, 0, 0, 0, -1, -4$, form an interval in column 3 of the display (3) of generalized binomial coefficients. In accordance with Taoist tradition, it is the 0's in this expression that 'matter': the extensive cancellation which takes place for monomials of 'middle' shapes.

6 The Whitney algebra of a matroid.

We develop a symbolic calculus based directly on a matroid $M = M(S)$, a calculus of independent sets for M that is the analogue of the exterior algebra of a vector space. Start with the free exterior algebra E, over the integers, generated by the set of points S; hence E consists of $\mathbf{Z}$-linear combinations of anticommutative words on S, and is a graded Hopf algebra, with coproduct determined just as for the exterior algebra of a vector space. For example,

$$adceb \;=\; -abcde, \;\; abda \;=\; 0$$
$$(1 + ad)\,(c - ef + ab) \;=\; -acd - adef + ab + c - ef$$

We then construct the tensor algebra $T(E) = \bigoplus T^k(E)$, consisting of linear combinations of tensor products of anticommutative words on S. and, finally, divide out *the ideal generated by all words formed from dependent sets in M and all homogeneous components (homogeneous by shape) of coproducts of such words.* In this manner we impose those algebraic relations on $T(E)$ that necessarily would hold if 'dependence in M' meant 'linear dependence over $\mathbf{Z}$', but without imposing specific $\mathbf{Z}$-linear relations on the points of M. We call the resulting structure $W(M)$ the *Whitney algebra* of the matroid M. The defining ideal D is homogeneous relative to the grading of $T(E)$ by number of tensor positions, so the quotient structure W is a direct sum of quotient algebras:

$$W = T(E)/D = \bigoplus_{k \geq 0} T^k(E)/D^k,$$

the ideals D^k being the intersections with $D \cap T^k$. For example, if M is the matroid of rank 3 on five points $abcde$, with circuits $abc, ade, bcde$, then we have relations such as

$$0 \;=\; (1 \circ bc)\, \delta_{2,1} ade \;=\; ad \circ bce \;-\; ae \circ bcd$$

the term $de \circ abc$ disappearing because abc is dependent. In addition to the product (which we denote by $\circ$, rather than $\otimes$) that a Whitney algebra W inherits as a quotient of $T(E)$, each component W^k has an *internal product*, induced by the product on $T^k(E)$. For example, in W^3, the internal product w of $u = ad \circ cdf \circ a$ and $v = be \circ ae \circ b$ is

$$(ad \circ cdf \circ a)\,(be \circ ae \circ b) \;=\; -\, abde \circ acdef \circ ab. \tag{5}$$

The algebra W is also graded by *shape*, the sequence of ranks of the tensor factors in a monomial, and by *content*, the multiset of letters in a monomial. Thus, in product (5),

$$\begin{aligned} \sigma(u) + \sigma(v) \;&=\; (2,3,1) + (2,2,1) \;=\; (4,5,2) \;=\; \sigma(w) \\ |u| \cdot |v| \;&=\; (a^2cd^2f) \cdot (ab^2e^2) \;=\; (a^3b^2cd^2e^2f) \;=\; |w| \end{aligned}$$

In the grading by tensor power, $W^0 = Z$, while $W^1 = E/D$ is freely generated, having as basis the set of monotone independent words. The passage from matroids to their Whitney algebras is functorial with respect to weak maps of matroids. Any representation of a matroid M in a vector space V induces a unique morphism from the Whitney algebra $W(M)$ to the tensor algebra of the exterior algebra $T(\Lambda(V))$. The coproduct on E induces a map $\delta : W^1 \to W^2$, to which we also refer as a coproduct, which is coassociative in the appropriate sense and respects internal products, that is, $\delta(uv) = \delta(u)\delta(v)$ in W^2, for all $u, v \in W^1$. In fact, W has precisely the same algebraic structure as the tensor algebra of a commutative Hopf algebra H, where W^k plays the role of the tensor power $T^k(H)$, but with the crucial distinction that W^k is not equal to $T^k(W^1)$. A good deal of elementary matroid theory is transported to Whitney algebra by the following device. For a word $w = b_1 \cdots b_k$ and a letter a, write $w_{i,a}$ for the word $b_1 \cdots b_{i-1} a b_{i+1} \cdots b_k$. If the letter a is in the closure of the word w, then the equality

$$w \circ a \;=\; \sum_{i=1}^{k} w_{i,a} \circ b$$

holds in $W(M)$. Whenever a matroid is represented in a vector space V, the bracket in V converts this abstract information into concrete information about linear relations among points. More generally, if $w = b_1 \cdots b_k$ and $v = a_1 \cdots a_k$ are words in W with all a_i in the closure of w, then, setting

$$w_{i,j} \;=\; b_1 \cdots b_{i-1} a_j b_{i+1} \cdots b_k,$$

the equality

$$\overbrace{w \circ \cdots \circ w}^{k-1} \circ v \;=\; \det\,(w_{i,j})_{1 \leq i,j \leq k}$$

holds in $W(M)$. This is the Whitney algebra analogue of Bazin's theorem. For instance, under the above hypotheses,

$$b_1b_2b_3 \circ b_1b_2b_3 \circ a_1a_2a_3 \;=\; \begin{vmatrix} a_1b_2b_3 & a_2b_2b_3 & a_3b_2b_3 \\ b_1a_1b_3 & b_1a_2b_3 & b_1a_3b_3 \\ b_1b_2a_1 & b_1b_2a_2 & b_1b_2a_3 \end{vmatrix}$$

7 The Fano matroid

It takes a bit of work to show it, along lines first developed by Peter Vamos, but a matroid M is representable if and only if no product $w_1 \circ \cdots \circ w_k$ of independent words w_i is zero in $W(M)$. Suppose that there exists a product m of independent words in $W(M)$ and some integer $r > 1$ such that $rm = 0$. If M is representable over some field K, then the characteristic of K divides the integer r. We can see this at work in the Whitney algebra of the Fano matroid, the matroid of seven nonzero vectors in a vector space of rank 3 over the two-element field $GF(2)$. It has circuits

$$\begin{array}{ccccccc} abc & ade & afg & bdg & bef & cdf & ceg \\ defg & bcfg & bcde & acef & acdg & abeg & abdf \end{array}$$

Given the high degree of symmetry in this matroid, there is essentially only one type of non-zero monomial m, up to linear isomorphism, of shape $(1, 3, 3)$, content $abcdefg$. Each point gives rise to a partition of the complementary set of six points into three pairs, the pairs of points collinear with the given point. For instance, the point a gives rise to the partition bc, de, fg. The only way to form a non-zero monomial of shape $(1, 3, 3)$ with a in position 1 is to keep two of the three pairs bc, de, fg together, splitting the other pair into the two final tensor factors. Thus, without loss of generality, we may assume $m = a \circ bcf \circ deg$. Consider the three syzygies:

$$\begin{array}{rll} \gamma_1 : & (1 \circ bc \circ de)\, \delta_{1,1,1}\, afg & = +\, a \circ bcf \circ deg \;-\; a \circ bcg \circ def, \\ \gamma_2 : & (a \circ b \circ eg)\, \delta_{0,2,1}\, cdf & = -\, a \circ bcd \circ efg \;-\; a \circ bcf \circ deg, \\ \gamma_3 : & (a \circ c \circ ef)\, \delta_{0,2,1}\, bdg & = -\, a \circ bcd \circ efg \;+\; a \circ bcg \circ def. \end{array}$$

Note that many monomials potentially occurring in these syzygies are zero because of their inclusion of dependent words. Syzygies $\gamma_1 = 0$ and $\gamma_3 = 0$ establish that the three monomials

$$a \circ bcf \circ deg, \;\; a \circ bcd \circ efg, \;\; a \circ bcg \circ def$$

are equal in the Whitney algebra of the Fano matroid. Syzygy $-\gamma_2$ then establishes that $a \circ bcf \circ deg$, and thus each of these monomials, becomes zero when multiplied by 2. By the symmetry noted above, any monomial of shape $(1, 3, 3)$, content $abcdefg$, becomes zero when multiplied by 2. It follows that the Fano matroid is representable only over fields of characteristic 2.

8 Categorical setting

The categorical interpretation for Whitney algebras is as follows. We will see that a Whitney algebra has the structure of a generalized Hopf algebra. The generalization in question is called a lax Hopf algebra. Now R-Hopf algebras are themselves the cogroup objects in a certain category, the category $\mathbf{ComAlg}_R$ of commutative R-algebras (see below). Cogroup objects in a category $\mathbf{C}$ can in turn be defined as sum-preserving functors to $\mathbf{C}$ from a category, say $\mathbf{T}$, with a single cogoup object. This permits us to define a *lax R-Hopf algebra* as arbitrary functors from $\mathbf{T}$ to $\mathbf{ComAlg}_R$, that is, functors not necessarily preserving sums. Lets go back over this bit by bit. A graded R-algebra A is *commutative* if $\mu_A\, \tau = \mu_A$; in other words, if $xy = Sign|x||y|yx$, for all homogeneous $x, y \in A$. (In general, the notion of commutativity for algebras in a symmetric monoidal category depends on the choice of twist map τ; this form of commutativity, familiar to topologists, is referred to in many contexts as *anticommutativity.*) The category $\mathbf{ComAlg}_R$ of graded commutative R-algebras, and degree zero homogeneous R-algebra maps, is not only symmetric monoidal, but has finite sums given by the tensor product operation. Let $\mathbf{T}$ be the free category with finite sums generated a single cogroup object. There is then a one-one correspondence between cogroup objects in a category $\mathbf{C}$ and sum-preserving functors from $\mathbf{T}$ to $\mathbf{C}$. The cogroup objects themselves form a category, isomorphic to the category $(\mathbf{T} \to \mathbf{C})$, in which the maps are natural transformations. In particular, taking $\mathbf{C}$ to be the category $\mathbf{ComAlg}_R$ of commutative R-algebras, we obtain the category of R-Hopf algebras. Adopting this point of view, we define a *lax Hopf algebra* as any functor from $\mathbf{T}$ to the category of commutative R-algebras, not necessarily preserving sums. More precisely, a *lax R-Hopf algebra* is a functor H from $\mathbf{T}$ to the category $\mathbf{ComAlg}_R$ of graded commutative R-algebras that satisfies $H(1) = R$. Let H be a lax R-Hopf algebra, L a lax S-Hopf algebra. A *morphism* $f : H \to L$ is a sequence of ring homomorphisms $f : H^k \to L^k$ that commute with the structure maps (coproduct $\delta : H_1 \to H^2$, counit $\epsilon : H^1 \to R$, antipode $\chi : H^1 \to H^1$, products $\mu^k : H^k \to H^k$, units $v^k : R \to H^k$). It follows that the pairs (f^0, f^k) are algebra morphisms from (R, H^k) to (S, L^k) for each $k \geq 0$, that is, a morphism of lax Hopf algebras is a natural transformation of the corresponding functors from $\mathbf{T}$ to the category $\mathbf{ComAlg}$. We identify a lax Hopf algebra H with the direct sum $\hat{H}$ of the H^k. A lax Hopf algebra H is *of quotient type* if the natural mapping from the tensor algebra $T(H^1)$ into $\hat{H}$ is surjective. Any morphism f defined on a Hopf algebra of quotient type is determined by the maps f^0, f^1 on H^0, H^1. If H is a Hopf algebra and $I \subseteq H$ is an ideal (not necessarily a coideal) of H such that $\epsilon(I) = 0$ and $\chi(I) \subseteq I$, then we obtain a lax Hopf algebra $\hat{H}$ by letting $H^0 = R$, $H^1 = H$ modulo the ideal I^1 generated by the homogeneous components of I, $H^2 = H \circ H$ modulo the ideal I^2 generated by homogeneous components of $\delta(I)$, etc. (If I is already homogeneous, then $I^1 = I$.) Furthermore, the direct sum of the I^k's is an ideal I^∞ of the tensor algebra $T(H)$, and $\hat{H} = T(H)/I^\infty$.

9 The Geometric Product

The fundamental exchange relations for Whitney algebra are expressible in terms of a geometric product, an operator on pairs of words that generalizes the join and meet operations in the Cayley algebra of a Peano space. In what follows, for any word w in the free monoid on the set of elements of a matroid M, let $\rho(w)$ denote the rank in M of the set w. Thus for the matroid of three collinear points a, b, c, the rank $\rho(bacb)$ is equal to 2.

Definition 1 *For words $u, v \in W^1$, with $|u| = r$, $|v| = s$, let $k = r + s - \rho(uv)$. The geometric product of u and v in W, written $u \diamond v$, is given by the expression*

$$u \diamond v = \sum_{(u)_{r-k,k}} u_{(1)} v \circ u_{(2)}$$

Whenever a matroid is represented, the geometric product $u \diamond v$ of bases u and v for flats U and V is the tensor product of a basis for the join of U and V with a basis for the meet, *in the ambient space*, of U and V. When the pair U, V of flats is not modular in M, this 'intersection' will not be present as a flat of the matroid. For any represented matroid, all words $u_{(1)}v$ occurring in the first tensor position of the geometric product will be scalar multiples of each other, so we can express the geometric product $u \diamond v$ as the tensor product of an *extensor*, representing the subspace spanned by uv, with a linear combination f of extensors of step k. In this sense the geometric product furnishes a convenient algebraic sustitute for the missing 'intersection' of u and v, and 'restores modularity': $\rho(u) + \rho(v) = \rho(uv) + \rho(f)$. The following theorem, which provides an alternative expression for the geometric product, is the Whitney algebra analogue of the basic properties of the meet operation in a Cayley algebra.

Theorem 2 (Exchange Relations) *For words $u, v \in W^1$, with $|u| = r$, $|v| = s$, let $k = r + s - \rho(uv)$; then*

$$\sum_{(u)_{r-k,k}} u_{(1)}v \circ u_{(2)} = \sum_{(v)_{k,s-k}} uv_{(2)} \circ v_{(1)}.$$

The commutativity of the geometric product is an immediate consequence. For words u, v, and integer k as above,

$$u \diamond v = (-1)^{(r-k)(s-k)} \, v \diamond u.$$

From this, we can pass directly to questions of commutativity of the tensor, or external product in the Whitney algebra. At least for matroids M in which we are sure that the product $u \circ v$ of independent words is non-zero (such as in all representable matroids), then two non-zero words (necessarily of the same length) commute if and only if they span the same flat in M. In particular, words formed from bases for M commute, and generate a commutative subring called the *basis ring*, a ring intimately related with Neil White's bracket ring. For any matroid represented in (and spanning) a vector space V, the basis ring maps into the pseudoscalar algebra of V, and conversely, any such map that is nonzero on each basis of M determines a representation of M (up to choices of bases for M and V, just as for maps of White's bracket ring into a field.

10 Straightening in the Whitney algebra of a uniform matroid

In his proofs of the fundamental theorems in invariant theory, Gian-Carlo had frequent recourse to straightening algorithms, claiming for these methods of proof the virtue of being characteristic free. The idea is to arrange all monomials of a homogeneous component in lexicographic order, to determine the lexicographically-first basis, and to design an algorithm that will express any given monomial in terms of that basis.

For the Whitney algebra of a matroid, the straightening process should be carried out in each homogeneous component in the grading by shape and content. In general, as we have seen in the case of the Fano matroid, there will be a non-zero *torsion* submodule, generated by monomials w such that $kw = 0$ for some non-zero integer k. But even when there is no torsion, it may be difficult to characterize the monomials residing in the lexicographically-first basis. These problems do not arise in *uniform* matroids: matroids $M_{n,k}$ on an n-element set P, where the circuits are precisely all $(k+1)$-element subsets of P. Such matroids are described geometrically as 'n points in general position, rank k'. We can present their straightening method today, a variant of Rutherford's interpolation algorithm [1].

So, choose a uniform matroid $M_{n,k}$ on an n-element set P, and single out a homogeneous component $W_{\lambda,c}$ of shape λ and matching content c. In what follows, all *words* are assumed to be monotone, with distinct letters. A *inverted split* of a word $A \subseteq P$ is any tensor product $A_j \circ \cdots \circ A_2 \circ A_1$ of words A_i such that $A_1 A_2 \cdots A_j = A$ in the concatenation product. For example, $st \circ ir \circ f$ is an inverted split of the monotone word $first$. We call a monomial w is *standard* in the Whitney algebra $W(M_{n,k})$ if and only if no factor of w is an inverted split of a $(k+1)$-element word, that is, of a circuit of M. For example, the monomial $ac \circ e \circ bd$ is standard in $M_{5,3}$, but $cd \circ b \circ ae$ is not.

We now assign a 'best standard tableau', which we call 'standard form', to each monomial. The notion of the 'depth' of a letter in a particular tensor position in a monomial will turn out to be particularly helpful concept. The *j-truncation* $w_{|_j}$ of a monomial $w = w_1 \circ \cdots \circ w_q$ is equal to $w_1 \circ \cdots \circ w_j$ if $j \le q$, and is equal to w if $j > q$. Since letters (elements of P) can be repeated in different tensor positions of a monomial in W, we use the word *token* to refer to a letter in a tensor position in a monomial. A token in a monomial w, written as l_j, say, to denote the letter l in tensor position j of w, is of *depth* $d = d(l_j)$ if and only if d is the maximum value such that some inverted split of a word y of length d beginning with the letter l is a factor of the j-truncation $w_{|_j}$ of w. A monomial w is of *depth* d, written $d(w) = d$, if and only if d is the maximum depth of tokens in w. The *standard form* $[\![w]\!]$ of a monomial $w \in W^{(q)}$ is a $q \times d$ array partially filled by the tokens of w, such that each token l_j occurs in row j, column $d(l_j)$, the columns being numbered (exceptionally) *from right to left.* The integer d, the number of columns, is the depth of w. Positions in the $q \times d$ array that are not filled are called *holes.* For example, the monomials $bd \circ ad \circ bc$ and $bd \circ bc \circ ad$ have standard forms

$$[\![bd \circ ad \circ bc]\!] \;=\; \begin{pmatrix} \bullet & b & d \\ a & \bullet & d \\ b & c & \bullet \end{pmatrix}, \qquad [\![bd \circ bc \circ ad]\!] \;=\; \begin{pmatrix} \bullet & \bullet & b & d \\ \bullet & b & c & \bullet \\ a & \bullet & \bullet & d \end{pmatrix}.$$

The token b_2 in the second monomial is of depth 3 because the inverted split $d \circ bc \circ 1$ divides the monomial $bd \circ bc \circ ad$.

Proposition 3 *The standard form of any monomial is strictly increasing across each row, and weakly increasing down each column. A monomial w in $W(M_{n,k})$ is standard if and only if its standard form has no more than k columns.*

Proof: The rows of $[\![w]\!]$ are monotone words (possibly with holes) because if e_j

and f_j are consecutive tokens in the tensor position j, and if f is the initial letter of a d-letter word y for which an inverted split $y_1 \circ \cdots \circ y_j$ divides w, then $y_1 \circ \cdots \circ ey_j$ also divides w, and ey is a $(d+1)$-letter word for which an inverted split divides w. If f_i is a token of depth d, let $y = y_1 \circ \cdots \circ y_i$ be an inverted split of a d-letter word beginning with f. If e_j is a token in a later tensor factor $(i < j)$ such that e is earlier in the alphabet than f, then ey is a $(d+1)$-letter word for which the inverted split $y_1 \circ \cdots \circ y_i \circ 1 \circ \cdots \circ 1 \circ e$ divides w, and $d(e_j) > d(f_i)$. So no inversion of alphabetical order is possible in any column. A monomial is non-standard in $W(M_{n,k})$ if and only if it contains an inverted split $y_1 \circ \cdots \circ y_i$ of a $(k+1)$-letter word y, if and only if some token (the first letter of the word y_i) is of depth $k+1$. □
If $y = y_1 \circ \cdots \circ y_q$ is a standard monomial of depth d in a homogeneous component $W_{\lambda,c}$ of $W(M_{n,k})$, so $d \leq k$, and if $w = w_1 \circ \cdots \circ w_q$ is any monomial in $W_{\lambda,c}$, an *interpolant from w to y*, written $U : w \to y$, is any $d \times q$ array U partially filled with content c such that

(1) the row contents of U are the respective tensor factors of w, and

(2) the columns of $\|y\|$ are obtained from the respective columns of U by a permutation of *letters only*, leaving all holes in place.

The *sign* of an interpolant $U : w \to y$ is the product of the signs ±1 of the individual row permutations used to pass from the tensor factors of w to the rows of U (irrespective of holes). Define an integer value $\tau(w, y)$ to be the integer sum of the signs of all interpolants U from w to y. Observe that if the content c has no repeated letters then an interpolant U, if it exists, is unique, so the integers $\tau(w, y)$ will be in the set $\{-1, 0, +1\}$.

Proposition 4 *If w is a monomial, z a standard monomial, and $\tau(w, z) \neq 0$, then $z \leq w$ in lexicographic order. For any standard monomial y, $\tau(y, y) = 1$.*

Proof: Let $U : w \to y$ be an interpolant from a monomial $w \in W^q$ to a standard monomial y, say of depth d. Let $Y = \|y\|$. Create a $d \times q$ array V with holes in the same positions as in Y, but with row words equal to the corresponding tensor factors of w. Let p_i be the first token in V that is different from the corresponding token q_i in Y. Since all tokens in tensor positions prior to i, and all tokens to the left of p_i in row i, are fixed in the passage via V to Y, the letter p can only be moved to the right in passing from V to U, and can only be fixed or move downward in the passage from U to Y. The letter p thus occupies a position SE of that of q_i in the standard form Y. Since $p \neq q$, we have $p > q$, so $y < w$ in the lexicographic order on monomials. For any standard monomial y, the identity permutation on rows provides an interpolant of sign +1 from y to y. Since no column content is modified in passing from $\|y\|$ to $\|y\|$, only the identity interpolant is available, and $\tau(y, y) = 1$. □

Let be *Mon* (λ, c) be the set of monomials of shape λ, content c, and $Mon_{st}(\lambda, c) \subseteq$ *Mon* (λ, c) the subset of standard monomials. Let $F = F(Mon\ (\lambda, c))$ be the Z-module freely generated by *Mon* (λ, c), and $F_{st} = F(Mon_{st}(\lambda, c))$ the submodule freely generated by the subset $Mon_{st}(\lambda, c)$.

Define a function τ_y on generators w of F by $\tau_y(w) \ = \ \tau(w, y)$, and extend it by Z-linearity to a linear form, also denoted τ_y, from F to Z, an element of the dual module F^*.

Proposition 5 *Ker* τ_y *contains all elementary syzygies of* $W_{\lambda,c}$, *so* τ_y *is well-defined as a linear form on* $W_{\lambda,c}$, *an element of* $W^*_{\lambda,c}$.

Proof: In any elementary syzygy $x \cdot \delta z$, where z is a word of length $k+1$ and $x \cdot \delta z$ is homogeneous of shape λ, content c, two monomials differing only by the exchange of two letters in z have opposite sign. Because $[\![y]\!]$ has at most k columns there is a pair a_i, b_j of tokens from z in the same column of $[\![y]\!]$. If w is any term in the syzygy $x \cdot \delta z$ such that w has an interpolant U to y, then, exchanging the letters a and b which interpolate to a_i and b_j in y, we obtain another monomial summand w' of $x \cdot \delta z$, with opposite sign, and which has an interpolant U' to y obtained by exchanging the tokens a_i and b_j. Since the row permutations used to pass from w and w' to U and U', respectively, are the same, the interpolants U and U' have the same sign, and their contributions to $\tau_y(x \cdot \delta z)$ cancel. Thus $\tau_y(x \cdot \delta z) = 0$. □

Now define a function τ on generators w of F by

$$\tau(w) \ = \ \sum_y \ \tau(w, y) \ y,$$

the sum being over all standard monomials $y \in Mon_{st}(\lambda, c)$, and extend it by Z-linearity to a map from F to F_{st}.

Proposition 6 *Ker* τ *contains all elementary syzygies of* $W_{\lambda,c}$, *so* τ *is well-defined as a linear map from* $W_{\lambda,c}$ *to* F_{st}.

Proof: Since $\tau \ = \ \sum_y \ \tau_y(y)$, and since by Proposition (-1), $\tau_y(x \cdot \delta z) = 0$ for every elementary syzygy $x \cdot \delta z$, all defining syzygies of $W_{\lambda,c}$ are in the kernel of τ. □

Let σ be the restriction of τ to F_{st}. Consider the matrix of τ relative to the basis $Mon_{st}(\lambda, c)$, in lexicographic order. By Proposition (-2), the matrix is lower triangular, with ones on the diagonal, and thus is invertible. The inverse matrix defines a Z-linear transformation σ^{-1} from F_{st} to F_{st}. Define a Z-linear map ρ from F to F_{st} as the composite $\tau\sigma^{-1}$ (τ acts, then σ^{-1}). For any fixed standard monomial z, define ρ_z as the projection of ρ on the z-component of F_{st}. Thus

$$\rho_z(w) \ = \ \sum_y \ \tau(w, y)\sigma^{-1}(y, z),$$

the sum being over all standard monomials y.

Proposition 7 *The homogeneous component $W_{\lambda,c}$ of the Whitney algebra of the uniform matroid $M_{n,k}$ is isomorphic to the Z-module F_{st} freely generated by the standard monomials of shape λ, content c.*

Proof: For any standard monomial z, the linear form r_z maps z to 1, and all other standard monomials y to 0. So the standard monomials are independent in $W_{\lambda,c}$. Any non-standard monomial w is expressible the internal product $w = x \cdot z'$ for some monomial x and some inverted split z' of a $(k+1)$-element set z. The elementary syzygy $x \cdot \delta z$ expresses w as a linear combination of monomials earlier in lexicographic order. Repeating this reduction process a finite number of times produces an expression for w as a Z-linear combination of monomials not further reducible, that is, as a linear combination of standard monomials. □

Proposition 8 *The linear map $\rho : W_{\lambda,c} \to F_{st}$ straightens the homogeneous component of the Whitney algebra, expressing each element uniquely as a Z-linear combination of standard monomials.*

Proof: The map ρ, followed by the inclusion map of F_{st} in $W_{\lambda,c}$, is an isomorphism. □

Let's look at one example of the straightening algorithm in action, for the uniform matroid $M_{4,2}$, a figure of four collinear points, and with a choice of shape $(1,2,1)$, content *abcd*. The complete interpolation table is in Figure 1. The row and column labels for the following matrices are to be found in that figure.

The matrix σ of interpolation coefficients from standard monomials to standard monomials, is

$$\begin{pmatrix} +1 & 0 & 0 & 0 & 0 \\ +1 & +1 & 0 & 0 & 0 \\ 0 & 0 & +1 & 0 & 0 \\ 0 & 0 & +1 & +1 & 0 \\ 0 & 0 & +1 & 0 & +1 \end{pmatrix} \qquad (\sigma)$$

with inverse matrix

$$\begin{pmatrix} +1 & 0 & 0 & 0 & 0 \\ -1 & +1 & 0 & 0 & 0 \\ 0 & 0 & +1 & 0 & 0 \\ 0 & 0 & -1 & +1 & 0 \\ 0 & 0 & -1 & 0 & +1 \end{pmatrix} \qquad (\sigma^{-1})$$

The matrix of interpolation coefficients from non-standard monomials to standard

	$\begin{pmatrix} \bullet & a \\ b & c \\ \bullet & d \end{pmatrix}$	$\begin{pmatrix} \bullet & a \\ b & d \\ c & \bullet \end{pmatrix}$	$\begin{pmatrix} \bullet & b \\ a & c \\ \bullet & d \end{pmatrix}$	$\begin{pmatrix} \bullet & b \\ a & d \\ c & \bullet \end{pmatrix}$	$\begin{pmatrix} \bullet & c \\ a & d \\ b & \bullet \end{pmatrix}$
$\begin{pmatrix} a & \bullet \\ b & c \\ d & \bullet \end{pmatrix}$	$\begin{pmatrix} \bullet & a \\ b & c \\ \bullet & d \end{pmatrix}$				
$\begin{pmatrix} a & \bullet \\ b & d \\ c & \bullet \end{pmatrix}$	$\begin{pmatrix} \bullet & a \\ b & d \\ \bullet & c \end{pmatrix}$	$\begin{pmatrix} \bullet & a \\ b & d \\ c & \bullet \end{pmatrix}$			
$\begin{pmatrix} b & \bullet \\ a & c \\ d & \bullet \end{pmatrix}$			$\begin{pmatrix} \bullet & b \\ a & c \\ \bullet & d \end{pmatrix}$		
$\begin{pmatrix} b & \bullet \\ a & d \\ c & \bullet \end{pmatrix}$			$\begin{pmatrix} \bullet & b \\ a & d \\ \bullet & c \end{pmatrix}$	$\begin{pmatrix} \bullet & b \\ a & d \\ \bullet & c \end{pmatrix}$	
$\begin{pmatrix} c & \bullet \\ a & d \\ b & \bullet \end{pmatrix}$			$\begin{pmatrix} \bullet & c \\ a & d \\ \bullet & b \end{pmatrix}$		$\begin{pmatrix} \bullet & c \\ a & d \\ b & \bullet \end{pmatrix}$
$\begin{pmatrix} a & \bullet \\ c & d \\ b & \bullet \end{pmatrix}$		$\begin{pmatrix} \bullet & a \\ c & d \\ b & \bullet \end{pmatrix}$			
$\begin{pmatrix} b & \bullet \\ c & d \\ a & \bullet \end{pmatrix}$				$\begin{pmatrix} \bullet & b \\ c & d \\ a & \bullet \end{pmatrix}$	
$\begin{pmatrix} c & \bullet \\ a & b \\ d & \bullet \end{pmatrix}$	$\begin{pmatrix} \bullet & c \\ b & a \\ \bullet & d \end{pmatrix}$		$\begin{pmatrix} \bullet & c \\ a & b \\ \bullet & d \end{pmatrix}$		
$\begin{pmatrix} c & \bullet \\ b & d \\ a & \bullet \end{pmatrix}$	$\begin{pmatrix} \bullet & c \\ b & d \\ \bullet & a \end{pmatrix}$				$\begin{pmatrix} \bullet & c \\ b & d \\ a & \bullet \end{pmatrix}$
$\begin{pmatrix} d & \bullet \\ a & b \\ c & \bullet \end{pmatrix}$	$\begin{pmatrix} \bullet & d \\ b & a \\ \bullet & c \end{pmatrix}$	$\begin{pmatrix} \bullet & d \\ b & a \\ c & \bullet \end{pmatrix}$	$\begin{pmatrix} \bullet & d \\ a & b \\ \bullet & c \end{pmatrix}$	$\begin{pmatrix} \bullet & d \\ a & b \\ c & \bullet \end{pmatrix}$	
$\begin{pmatrix} d & \bullet \\ a & c \\ b & \bullet \end{pmatrix}$		$\begin{pmatrix} \bullet & d \\ c & a \\ b & \bullet \end{pmatrix}$	$\begin{pmatrix} \bullet & d \\ a & c \\ \bullet & b \end{pmatrix}$		$\begin{pmatrix} \bullet & d \\ a & c \\ b & \bullet \end{pmatrix}$
$\begin{pmatrix} d & \bullet \\ b & c \\ a & \bullet \end{pmatrix}$	$\begin{pmatrix} \bullet & d \\ b & c \\ \bullet & a \end{pmatrix}$			$\begin{pmatrix} \bullet & d \\ b & c \\ a & \bullet \end{pmatrix}$	$\begin{pmatrix} \bullet & d \\ b & c \\ a & \bullet \end{pmatrix}$

Figure 1: Interpolation table for shape $(1, 2, 1)$, content *abcd* in $M_{4,2}$

monomials, is

$$\begin{pmatrix} 0 & +1 & 0 & 0 & 0 \\ 0 & 0 & 0 & +1 & 0 \\ -1 & 0 & +1 & 0 & 0 \\ +1 & 0 & 0 & 0 & +1 \\ -1 & -1 & +1 & +1 & 0 \\ 0 & -1 & +1 & 0 & +1 \\ +1 & 0 & 0 & -1 & +1 \end{pmatrix} \qquad (\tau)$$

The product matrix $\tau\sigma^{-1}$ is the matrix for straightening:

$$\begin{array}{c|ccccc|} & a\circ bc\circ d & a\circ bd\circ c & b\circ ac\circ d & b\circ ad\circ c & c\circ ad\circ b \\ a\circ cd\circ b & -1 & +1 & 0 & 0 & 0 \\ b\circ cd\circ a & 0 & 0 & -1 & +1 & 0 \\ c\circ ab\circ d & -1 & 0 & +1 & 0 & 0 \\ c\circ bd\circ a & +1 & 0 & -1 & 0 & +1 \\ d\circ ab\circ c & 0 & -1 & 0 & +1 & 0 \\ d\circ ac\circ b & +1 & -1 & 0 & 0 & +1 \\ d\circ bc\circ a & +1 & 0 & 0 & -1 & +1 \end{array} \qquad (\rho)$$

11 On the Feynman entangling operator

On 11 January, 1996, during that snowstorm in Cambridge, Gian-Carlo sent me a long and detailed email message proposing to represent any Whitney algebra as a quotient of a supersymmetric letter-place algebra, via the Feynman entangling operator.

Specifically, Gian-Carlo explained that the Whitney algebra $W(M)$ of any matroid $M = M(S)$ can be faithfully represented as a quotient of the supersymmetric algebra $\mathit{Super}[S^- \mid P^+]$. He mapped each monomial $w_1 \otimes w_2 \otimes \cdots w_k$ in $W(M)$ to the product

$$(w_1 \,|\, p_1^{(|w_1|)})\,(w_2 \,|\, p_2^{(|w_2|)})\,\cdots\,(w_k \,|\, p_k^{(|w_k|)}),$$

where the words $p_i^{(|w_i|)}$ are divided powers of positive letters representing the different possible positions in the tensor product. (The letter-place pairs $(a \,|\, p)$ are thus anticommutative.) The linear extension of this definition to a map on $W(M)$, he termed the *Feynman entangling operator*.

As Gian-Carlo later insisted on several occasions, the exchange relations for Whitney algebra should in principle be proved using straight-forward properties of the Feynman entangling operator, along the lines of the simple proof of the superalgebra exchange property, Theorem 10 of [6], noting in passing that the coproduct operators of the Whitney algebra correspond, under entangling, to polarizations of positive places.

This important task has not yet been carried out; I seize the present occasion to enlist the aid, in particular, of our friends from Bologna. I would be delighted to share the original texts of these messages and notes on the Feynman entangling operator with anyone willing to pursue this research.

References

[1] Daniel Edwin Rutherford, Substitutional Analysis, Edinburgh University Press, 1948, and Hafner Publishing Company, New York, 1968.

[2] Jacques Désarménien, Joseph P. S. Kung, Gian-Carlo Rota, *Invariant Theory, Young Bitableaux and Combinatorics*, Advances in Mathematics **27**, (1978), 63-92.

[3] Jacques Désarménien, *An algorithm for the Rota straightening formula*, Discrete Math. **30** (1980), 51-68.

[4] Henry Crapo, *Concurrence Geometries,* Advances in Mathematics **54** (1984), 278-301.

[5] Henry Crapo, *The Combinatorial Theory of Structures: Lectures on the application of combinatorial geometry in architecture and structural engineering,* Colloq. Math. Soc. János Bolyai **40**, North Holland, Amsterdam - New York (1985), 107-213.

[6] Frank D. Grosshans, Gian-Carlo Rota and Joel Stein, *Invariant Theory and Superalgebras* Conference Series in Mathematics, no. 69, American Mathematical Society, 1987.

[7] David Anick and Gian-Carlo Rota, *Higher-order syzygies for the bracket ring and for the ring of coordinates of the Grassmannian,* Proc. Nat. Acad. Sci. **88** (1991), 8087-8090.

[8] Christophe Carré, Alain Lascoux and Bernard Leclerc, *Turbo-straightening for decomposition into standard bases,* LITP, 1991

[9] Henry Crapo, *On the Anick-Rota Resolution of the Bracket Ring of the Grassmannian*, Advances in Mathematics **99** (1993), 97-123.

[10] Henry Crapo and Gian-Carlo Rota, *The Resolving Bracket*, in Invariant Methods in Discrete and Computational Geometry, Neil White, ed., Kluwer Academic Publishers, 1995, pp 197–222.

[11] Henry Crapo and William Schmitt, *The Whitney algebra of a matroid*, to appear in the Journal of Combinatorial Theory (A), 2000.

Partial and Semipartial Geometries: an Update

F. De Clerck

University of Ghent - Department of Pure Mathematics and Computer Algebra
Galglaan 2, B-9000 Gent, Belgium
e-mail: fdc@cage.rug.ac.be

The Handbook of Incidence Geometry [6] appeared in 1995. In chapter 12, *On some rank two geometries*, an almost complete overview was given on the status of the theory on partial and semipartial geometries. Now, five years later, it is maybe a good time to give an update of this status. Indeed a lot of things have happened during these years. Moreover we take the opportunity to give complete parameter lists of all known examples of partial and semipartial geometries known so far.

1 Introduction

An (α, β)-geometry $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ is a connected partial linear space of order (s, t) (i.e. two points are incident with at most one line, each point is incident with $t + 1$ ($t \geq 1$) lines, and each line is incident with $s + 1$ ($s \geq 1$) points), with the property that for every anti-flag (x, L) there are either α or β lines through x intersecting L.

The point graph $\Gamma(\mathcal{S})$ of an (α, β)-geometry is the graph with vertex set the set of points of $\mathcal{S}$; two vertices are adjacent if and only if they are different and collinear in $\mathcal{S}$. The *block graph* of an (α, β)-geometry is the graph whose vertices are the lines, and vertices are adjacent if and only if the corresponding lines are concurrent.

If $\alpha = \beta$, $\mathcal{S}$ is called a *partial geometry* with parameters s, t, α, which we denote by $\mathrm{pg}(s, t, \alpha)$ [1]. In this case the graph $\Gamma(\mathcal{S})$ is a strongly regular graph $\mathrm{srg}(v, k, \lambda, \mu)$; more precisely it is a

$$\mathrm{srg}((s+1)\frac{st+\alpha}{\alpha}, s(t+1), s-1+t(\alpha-1), \alpha(t+1)).$$

A strongly regular graph Γ with these parameters (which are satisfying $t \geq 1, s \geq 1$, and $1 \leq \alpha \leq \min\{s+1, t+1\}$) is called a *pseudo–geometric* (s, t, α)–graph. If the graph Γ is indeed the point graph of at least one partial geometry then Γ is called *geometric.*

Note that a graph can be pseudo–geometric for at most one set of values s, t, α and assuming $\alpha \neq s+1$, the cliques of size $s+1$ corresponding to potential lines must be maximal. However, there can exist several non-isomorphic partial geometries with the same graph as point or block graph. A pseudo-geometric graph is called *faithfully* geometric if and only if there is up to isomorphism exactly one partial geometry with this graph as point graph.

Another important family of (α, β)-geometries is given by the so-called $(0, \alpha)$-geometries (i.e. $\beta = 0$). Here the point graph is not necessarily a strongly regular graph. Those $(0, \alpha)$-geometries which have a strongly regular point graph are called *semipartial geometries* and are denoted by $\mathrm{spg}(s, t, \alpha, \mu)$ and were introduced in [17]. Note that the parameter μ is the parameter of the strongly regular point graph, which counts the number of vertices adjacent to two non-adjacent vertices. If $\alpha = 1$ these semipartial geometries are better known as *partial quadrangles* which are introduced by P. J. Cameron [8].

Remarks

1. Special classes of partial geometries are the generalized quadrangles ($\alpha = 1$) introduced by Tits, see [28]; the 2–$(v, s+1, 1)$ designs ($\alpha = s+1$) and their duals ($\alpha = t+1$); the *Bruck nets* ($\alpha = t$) and dual Bruck nets ($\alpha = s$). In this overview we will restrict ourselves to the so-called *proper partial geometries*, which are the partial geometries with $1 < \alpha < \min\{s, t\}$.

2. A *proper semipartial geometry* is a semipartial geometry which is not a partial geometry.

3. For the description of the examples of partial and semipartial geometries known until 1995, we refer to [16]. In the sequel we will give an overview of some new constructions of partial geometries having sometimes new parameters. In section 4 we will give complete parameter lists of the examples of the proper partial and semipartial geometries known at present.

2 New constructions of partial geometries

2.1 The partial geometry constructed from the Hermitian two-graph

A *two-graph* [30] (Ω, Δ) is a pair of a vertex set Ω and a triple set $\Delta \subset \Omega^{(3)}$, such that each 4-subset of Ω contains an even number of triples of Δ. A two-graph is called *regular* whenever each pair of elements of Ω is contained in the same number a of triples of Δ.

Given any graph $\Gamma = (X, \sim)$, one can construct a new graph by using *Seidel-switching*. For this, partition the vertex set X as $X = X_1 \cup X_2$, leave the adjacencies inside X_1 and X_2 as they are and interchange edges and non-edges between vertices of X_1 and X_2. Graphs which can be mapped to each other by Seidel-switching are called *switching equivalent*. It is known [30] that, given v there is a one-to-one correspondence between the two-graphs and the switching classes of graphs on the set of v elements. If the two-graph (Ω, Δ) is regular and if $(\Omega, \sim)$ is any graph in its switching class which has an isolated vertex $\omega \in \Omega$, then $(\Omega \setminus \{\omega\}, \sim)$ is a strongly regular graph.

Let $\mathcal{H}$ be the Hermitian curve in $\mathrm{PG}(2, q)$, q odd, defined by the Hermitian bilinear form $H(x, y)$. The Hermitian two-graph (Ω, Δ) is defined by taking as a vertex set Ω the set of $q^3 + 1$ points of $\mathcal{H}$ and a triple $\{x, y, z\} \in \Omega^{(3)}$ is an element of Δ if and only if $H(x, y)H(y, z)H(z, x)$ is a square (if $q \equiv -1 \pmod 4$) or a non-square (if $q \equiv 1 \pmod 4$) [34]. This two-graph appears to be regular with $a = \frac{(q^2+1)(q-1)}{2}$ and in its switching class there is indeed a graph which has an isolated vertex. This yields a strongly regular graph $\mathcal{H}(q)$ which is an $\mathrm{srg}(q^3, \frac{(q^2+1)(q-1)}{2}, \frac{(q-1)^3}{4} - 1, \frac{(q^2+1)(q-1)}{4})$ and is pseudo-geometric with parameters $s = q - 1, t = \frac{q^2-1}{2}, \alpha = \frac{q-1}{2}$. If $q = 3$ this graph is the point graph of the unique generalized quadrangle of order $(2, 4)$. Although it has been proved (computer search) by Spence [33] that $\mathcal{H}(q)$ is not geometric for $q = 5$ and $q = 7$ it is remarkable that the graph is indeed geometric if $q = 3^{2m}$ which has been proved by Mathon; we refer to [25] for more details. So far, a pure geometric construction of this partial geometry is not known. However, see [24] for some more geometric background.

2.2 Partial geometries from perp-systems

R. Mathon announced in June 1999 during the 2nd Pythagorean Conference (Samos, Greece) the existence of a set $\mathcal{R}$ of 21 lines of $\mathrm{PG}(5, 3)$ that are pairwise skew (hence form a partial line-spread) with the property that every plane of $\mathrm{PG}(5, 3)$ through one of the 21 lines of $\mathcal{R}$ intersects exactly two other lines of $\mathcal{R}$. Actually it is an SPG 1-regulus in the sense of Thas [38] (a brief description can also be found in [16]) with no tangent planes. The construction by R. Mathon is a computer construction. It yields a new partial geometry with parameters $s = 8, t = 20, \alpha = 2$. Embed $\mathrm{PG}(5, 3)$ as a hyperplane Π in $\mathrm{PG}(6, 3)$. The points of the partial geometry are the 3^6 points of $\mathrm{AG}(6, 3) = \mathrm{PG}(6, 3) \setminus \Pi$, the lines of the partial geometry are the affine planes of $\mathrm{AG}(6, 3)$ having as line at infinity one of the 21 elements of $\mathcal{R}$. Although quite some other nice properties of this SPG 1-regulus $\mathcal{R}$ in $\mathrm{PG}(5, 3)$ are known, there is so far no computer free construction known. However these properties have led to a new concept, namely *Perp-systems* which we shortly describe here. For more details we refer to [11].

Consider a $\mathrm{PG}(N, q)$ equipped with a polarity ρ. Define a *partial perp-system* $\mathcal{R}(r)$ to be any set $\{\pi_1, \ldots, \pi_k\}$ of $k(> 1)$ totally non-singular r-spaces of $\mathrm{PG}(N, q)$ such that no π_i^ρ meets an element of $\mathcal{R}(r)$. One easily proves that

$$|\mathcal{R}(r)| \leq \frac{q^{\frac{N-2r-1}{2}}(q^{\frac{N+1}{2}}+1)}{q^{\frac{N-2r-1}{2}}+1}. \tag{2.1}$$

We will only deal with systems $\mathcal{R}(r)$ such that equality holds in (2.1), such a system is called a *perp-system.*

Theorem 1 *Let $\mathcal{R}(r)$ be a perp-system of* $\mathrm{PG}(N,q)$ *equipped with a polarity ρ and let $\overline{\mathcal{R}(r)}$ denote the union of the point sets of the elements of $\mathcal{R}(r)$. Then $\overline{\mathcal{R}(r)}$ has two intersection sizes with respect to hyperplanes.*

This implies that $\overline{\mathcal{R}(r)}$ yields a two-weight code and a strongly regular graph $\Gamma^*(\overline{\mathcal{R}(r)})$ [7]. The graph is constructed by embedding $\mathrm{PG}(N,q)$ as a hyperplane Π in $\mathrm{PG}(N+1,q)$. The vertices of the graph are the q^{N+1} points of $\mathrm{AG}(N+1,q) = \mathrm{PG}(N,q) \setminus \Pi$, two vertices are adjacent whenever the line of $\mathrm{PG}(N+1,q)$ joining them is intersecting Π in an element of $\overline{\mathcal{R}(r)}$.

One easily checks that this graph is a pseudo-geometric

$$\left(q^{r+1}-1, \frac{q^{\frac{N-2r-1}{2}}(q^{\frac{N+1}{2}}+1)}{q^{\frac{N-2r-1}{2}}+1}-1, \frac{q^{r+1}-1}{q^{\frac{N-2r-1}{2}}+1}\right)\text{-graph.}$$

One can prove some restrictions on the parameters. More precisely one can prove the following theorem.

Theorem 2 *Let $\mathcal{R}(r)$ be a perp-system of* $\mathrm{PG}(N,q)$ *equipped with a polarity ρ. Then*

- $2r+1 \leq N \leq 3r+2$;
- *If $N = 2r+1$ then q is odd and $\Gamma^*(\overline{\mathcal{R}(r)})$ is the point graph of a net with q^{r+1} points on a line and $\frac{q^{r+1}+1}{2}$ lines through a point.*
- *Assume that $N \neq 2r+1$ then $\frac{r+1}{N-2r-1}$ is a positive integer; if N is even then q has to be a square. The graph $\Gamma^*(\overline{\mathcal{R}(r)})$ is the point graph of a partial geometry*

$$\mathrm{pg}\left(q^{r+1}-1, \frac{q^{\frac{N-2r-1}{2}}(q^{\frac{N+1}{2}}+1)}{q^{\frac{N-2r-1}{2}}+1}-1, \frac{q^{r+1}-1}{q^{\frac{N-2r-1}{2}}+1}\right).$$

One can construct perp-systems from other perp-systems. More precisely the next theorems are proved in [11].

Theorem 3 *Let $\mathcal{R}(r)$ be a perp-system with respect to some polarity of* $\mathrm{PG}(N,q^n)$*, then there exists a perp-system $\mathcal{R}'((r+1)n-1)$ with respect to some polarity of* $\mathrm{PG}((N+1)n-1,q)$.

Theorem 4 *If the classical polar space P admits a perp-system $\mathcal{R}(r)$, then the polar space Q admits a perp-system $\mathcal{R}(2r+1)$, for $(P,Q) =$*
$(\mathrm{H}(2n,q^2), \mathrm{Q}^-(4n+1,q))$
$(\mathrm{H}(2n+1,q^2), \mathrm{Q}^+(4n+3,q))$*,*
$(\mathrm{Q}(2n,q^2), \mathrm{Q}^+(4n+1,q))$ *for q odd,*
$(\mathrm{Q}(2n,q^2), \mathrm{Q}(4n,q))$ *for q even,*
$(\mathrm{Q}^-(2n+1,q^2), \mathrm{Q}^-(4n+3,q))$*,*
$(\mathrm{H}(2n,q^2), W_{4n+1}(q))$*.*

Remarks

1. A net with the parameters as in theorem 2 and coming from a perp-system does exist for every odd q.
2. If N is maximal i.e. if $N = 3r+2$ then r is odd and the partial geometry is a
$$\mathrm{pg}(q^{r+1}-1, q^{\frac{r+1}{2}}(q^{r+1}-q^{\frac{r+1}{2}}+1), q^{\frac{r+1}{2}}-1).$$
This partial geometry has the parameters of a partial geometry $T_2^*(\mathcal{K})$, with $\mathcal{K}$ a maximal arc of degree $q^{\frac{r+1}{2}}$ in a $\mathrm{PG}(2,q^{r+1})$. A selfpolar maximal arc of degree q^n in a $\mathrm{PG}(2,q^{2n})$ is a maximal arc $\mathcal{K}$ such that each point $p \in \mathcal{K}$ is mapped by a polarity ρ of the plane on an exterior line p^ρ of $\mathcal{K}$. If q is even, there exist selfpolar maximal arcs of Denniston type; they yield a perp-system $\mathcal{R}(0)$. Applying theorem 3 this gives a perp-system with $r = n-1$ in $\mathrm{PG}(3n-1,q^2)$ and a perp-system with $r = 2n-1$ in $\mathrm{PG}(6n-1,q)$.
3. The set of 21 lines in $\mathrm{PG}(5,3)$ found by Mathon is a perp-system $\mathcal{R}(1)$ in $\mathrm{PG}(5,3)$. The polarity evolved can be either the symplectic polarity or the elliptic orthogonal polarity. In this case $N = 5$ and $r = 1$, hence N is maximal and the partial geometry has the parameters of a $T_2^*(\mathcal{K})$, with $\mathcal{K}$ a maximal arc of degree 3 in $\mathrm{PG}(2,9)$; however such a maximal arc does not exist.
4. So far, there is no example known of a perp-system in $\mathrm{PG}(N,q)$ with $2r+1 < N < 3r+2$.
5. The results in theorem 4 are results that are of the same type as known results on m-systems, introduced by Thas and Shult [31, 32]. There are indeed connections with m-systems. For more details we refer to [11].

2.3 Partial geometries with $t = s + 1$

2.3.1 Derivation of partial geometries

Let Φ be a pg–*spread* of a $\mathrm{pg}(s,t,\alpha)$ $\mathcal{S} = (\mathcal{P},\mathcal{L},\mathrm{I})$, that is a (maximal) set of $\frac{st}{\alpha}+1$ lines partitioning the point set. Assume $t > 1$ and let L be any line of $\mathcal{L} \setminus \Phi$. Let

Φ_L be the set of $s+1$ lines of Φ intersecting L. Then L is called *regular with respect to* Φ if and only if there exists a set of $s+1$ lines $\mathcal{L}(L) = \{L_0 = L, L_1, \ldots, L_s\}$ that partitions the set $\mathcal{P}(\Phi_L)$ of points covered by Φ_L, and each element of $\mathcal{L}\backslash(\mathcal{L}(L)\cup\Phi)$ is intersecting $\mathcal{P}(\Phi_L)$ in at least one point and at most s points.

It is easy to prove (see [13]) that if a pg(s, t, α) $\mathcal{S}$ has a regular line L with respect to a pg–spread Φ, then $t \geq s + 1$. If $t = s + 1$ then every line M not being an element of the pg–spread Φ neither of $\mathcal{L}(L)$ intersects $\mathcal{P}(\Phi_L)$ in α points. Now assume that Φ is a pg–spread of a pg$(s, s + 1, \alpha)$ such that every line is regular with respect to Φ. Then $\mathcal{L} \setminus \Phi$ is partitioned in $\frac{s(s+1)}{\alpha} + 1$ sets $\mathcal{L}_i$ ($i = 1, \ldots, \frac{s(s+1)}{\alpha} + 1$) each containing $s+1$ mutually skew lines. The spread Φ is called a *replaceable spread* and can be used to construct the following incidence structure $\mathcal{S}_\Phi = (\mathcal{P}_\Phi, \mathcal{L}_\Phi, \mathrm{I}_\Phi)$. The elements of $\mathcal{P}_\Phi$ are on the one hand the points of $\mathcal{S}$ and on the other hand the sets $\mathcal{L}_i$ ($i = 1, \ldots, \frac{s(s+1)}{\alpha} + 1$), $\mathcal{L}_\Phi = \mathcal{L} \setminus \Phi$. Finally $p \;\mathrm{I}_\Phi\; L$ is defined by $p \;\mathrm{I}\; L$ if $p \in \mathcal{P}$ and by $L \in p$ if $p \in \{\mathcal{L}_i \mid i = 1, \ldots, \frac{s(s+1)}{\alpha} + 1\}$. Generalizing a construction of Mathon and Street [26], one can prove (see [13]) that $\mathcal{S}_\Phi$ is a pg$(s + 1, s, \alpha)$. The partial geometry $\mathcal{S}_\Phi$ (and its dual) is called a *partial geometry derived from* $\mathcal{S}$ *with respect to* Φ.

Note that the set $\phi = \{\mathcal{L}_i \mid i = 1, \ldots, \frac{s(s+1)}{\alpha} + 1\}$ is a replaceable spread of $\mathcal{S}_\Phi^D$ and that the derived partial geometry $(\mathcal{S}_\Phi^D)_\phi$ is isomorphic to the partial geometry $\mathcal{S}^D$ [9]

2.3.2 The derived partial geometries of $\mathrm{PQ}^+(4n-1, q)$ ($q = 2$ or 3)

It has been checked by computer (see [26]) that the partial geometry $\mathrm{PQ}^+(7, 2)$ constructed by De Clerck, Dye and Thas [14] (but other constructions do exist, see [16] for details) has exactly 3 replaceable spreads yielding (after dualizing) 3 non-isomorphic partial geometries pg$(7, 8, 4)$. De Clerck [13] proved this result geometrically for both $q = 2$ and $q = 3$. Actually, Mathon and Street [26] have constructed by computer seven new partial geometries pg$(7, 8, 4)$ by starting from the partial geometry $\mathrm{PQ}^+(7, 2)$ and by using derivation with respect to a suitable replaceable spread. They give in [26] information on the order of the automorphism groups of the geometries as well as information on the point and block graphs of these geometries. They remarked that the point graphs of four of the geometries pg$(7, 8, 4)$ constructed by them, are isomorphic graphs while their block graphs all are different. Actually that point graph was not a new graph, it is the complement of the graph constructed in [3]. It is an element of the class of graphs called the graphs on a quadric with a hole. Such a graph has vertex set the points of a quadric $\mathrm{Q}^+(2m - 1, q) \setminus M$, M a generator of the quadric and vertices x and y are defined to be adjacent whenever $\langle x, y\rangle \subset \mathrm{Q}^+(2m - 1, q) \setminus M$. This graph is strongly regular for general dimensions and general q.

Klin and Reichard [23, 29] found, again by computer, but independently from Mathon and Street, that the complement of the graph on $Q^+(7,2)$ with a hole, is indeed the point graph of exactly four partial geometries $\mathrm{pg}(7,8,4)$.

In [9] it has been proved that from the eight known partial geometries $\mathrm{pg}(7,8,4)$, four of them are the smallest member of an infinite class of $\mathrm{pg}(2^{2n-1}-1, 2^{2n-1}, 2^{2n-2})$ and all of them are constructed using derivation.

Remarks

1. For quite a long time it was conjectured that there is only one $\mathrm{pg}(7,8,4)$ up to isomorphism. This conjecture has turned out to be false. However in [15] it has been proved that the point graph of the partial geometry $\mathrm{PQ}^+(7,2)$ is faithfully geometric. This does not guarantee that the block graph is also faithfully geometric. But, in [27] Panigrahi proves, using combinatorial arguments, that the block graph $\Gamma'(7,2)$ of the partial geometry $\mathrm{PQ}^+(7,2)$ is faithfully geometric indeed. Actually the graph $\Gamma'(7,q)$ is the graph $\Gamma^c(Q^+(7,q))$ with vertices the points on the hyperbolic quadric $Q^+(7,q)$, two vertices being adjacent if and only if they are on a secant of the quadric (see [22]). In [9] a shorter proof based on the triality property of the quadric $Q^+(7,q)$ has been given for the result of Panigrahi and has been extended for the case $q = 3$.

2. Kantor [22] also proved that if $n \neq 2$, then the block graph of the partial geometry $\mathrm{PQ}^+(4n-1,q)$, ($q = 2$ or 3) is not isomorphic to the graph $\Gamma^c(Q^+(4n-1,q))$. Note that the graph $\Gamma^c(Q^+(2m-1,q))$ is pseudo-geometric with parameters $s = q^{m-1}$, $t = q^{m-1}-1$, $\alpha = q^{m-2}(q-1)$, for any q. The graph $\Gamma^c(Q^+(3,q))$, is the complement of the $(q+1) \times (q+1)$–grid, hence is geometric if and only if there exists a projective plane of order $q+1$. It is not known whether $\Gamma^c(Q^+(5,q))$, $q \geq 4$, is geometric. The graph $\Gamma^c(Q^+(5,2))$ is a pseudo-geometric $(4,3,2)$-graph but a $\mathrm{pg}(4,3,2)$ does not exist (see for instance [12]). As explained in [27], it can be read off from the computer aided results of M. Hall, Jr. and R. Roth in [20] that $\Gamma^c(Q^+(5,3))$ is not geometric. As remarked in [27] the graph $\Gamma^c(Q^+(2m-1,q))$ with $m \geq 5$ is not geometric for $q = 2$, but the question is still open for $q > 2$. Hence, the fact that the graph $\Gamma^c(Q^+(7,q))$ is geometric for $q = 2,\ 3$ is quite remarkable indeed; see also theorem 7.

3. Brouwer, Haemers and Tonchev [2] have proved that the $\mathrm{pg}(7,8,4)$ $\mathrm{PQ}^+(7,2)$ is embeddable into a Steiner system $S(2,8,120)$. This result has been extended for the three partial geometries directly derived from $\mathrm{PQ}^+(7,2)$ in [10].

4. In some cases derivation of the partial geometry can be rephrased in terms of Seidel switching of graphs. We refer to [10] for the technical details.

3 New constructions of semipartial geometries

3.1 The semipartial geometries $\mathrm{spg}(q-1, q^2, 2, 2q(q-1))$

A very interesting example of semipartial geometry is the semipartial geometry by R. Metz (private communication). We recall his construction. Let $\mathrm{Q}(4,q)$ be a non-singular quadric of the projective space $\mathrm{PG}(4,q)$. If we define $\mathcal{P}$ as the set of the elliptic quadrics $Q^-(3,q)$ on $Q(4,q)$, $\mathcal{L}$ as the set of all pencils of such elliptic quadrics which are pairwise tangent in a common point, and I as the natural incidence relation then $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ is an $\mathrm{spg}(q-1, q^2, 2, 2q(q-1))$.

Let $\mathrm{Q}^-(5,q)$ be an elliptic quadric of $\mathrm{PG}(5,q)$ and p be a point of $\mathrm{PG}(5,q)$ not on $\mathrm{Q}^-(5,q)$. Let Π be a hyperplane of $\mathrm{PG}(5,q)$ not containing p. Let $\overline{\mathcal{P}}_1$ be the projection of the point set of $\mathrm{Q}^-(5,q)$ from p on Π and let $\overline{\mathcal{P}}_2$ be the set of points of Π on a tangent of $\mathrm{Q}^-(5,q)$ through p. Let $\mathcal{S}$ be the geometry with point set $\mathcal{P} = \overline{\mathcal{P}}_1 \setminus \overline{\mathcal{P}}_2$, whereas the line set $\mathcal{L}$ is the set of all projections on Π of the lines of $\overline{\mathcal{S}}$, excluding the projections completely contained in $\overline{\mathcal{P}}_2$. The incidence is the one of the projective space. Then Hirschfeld and Thas [21] have proved that this is a semipartial geometry $\mathrm{spg}(q-1, q^2, 2, 2q(q-1))$ isomorphic to the one by Metz.

It has been observed by Brown [4] that one does not need necessarily the GQ $\mathrm{Q}^-(5,q)$ for this construction. Indeed if a GQ $\mathcal{S}$ of order (s, s^2) contains a subquadrangle $\mathcal{S}'$ of order s, then every point x of $\mathcal{S} \setminus \mathcal{S}'$ is collinear with the s^2+1 points of an ovoid, denoted by $\mathcal{O}_x$, of $\mathcal{S}'$. The ovoid $\mathcal{O}_x$ is said to be *subtended by* x. If it happens to be that every such subtended ovoid $\mathcal{O}_x$ is also a subtended ovoid $\mathcal{O}_y$ for another point $y \in \mathcal{S} \setminus \mathcal{S}'$, then the ovoid is called *doubly subtended* and is denoted by $\mathcal{O}_{x,y}$. If every subtended ovoid of $\mathcal{S}'$ is doubly subtended, then the subGQ $\mathcal{S}'$ is called *doubly subtended* in the GQ $\mathcal{S}$.

Theorem 5 ([4]) *Assume $\mathcal{S}$ is a GQ of order (s, s^2) containing a subGQ $\mathcal{S}'$ that is doubly subtended in $\mathcal{S}$; then the incidence structure with points the subtended ovoids of $\mathcal{S}'$, lines the rosettes of subtended ovoids (a rosette is a set of s subtended ovoids containing a common point x and having two by two just x in common), incidence the natural incidence, is a semipartial geometry* $\mathrm{spg}(s-1, s^2, 2, 2s(s-1))$.

The generalized quadrangle $\mathrm{Q}(4,q)$ is indeed doubly subtended in $\mathrm{Q}^-(5,q)$ and this yields the construction of R. Metz. However Brown [4] remarks that $\mathrm{Q}(4,q)$ is also doubly subtended in the GQ of order (q, q^2) (q odd) related to the flock $K1$ of Kantor, and hence yields a semipartial geometry.

It is worthwhile to remark that the construction by Hirschfeld and Thas of the semipartial geometry of Metz, implies that for q even, this semipartial geometry $\mathrm{spg}(s-1, s^2, 2, 2s(s-1))$ is embedded in $\mathrm{AG}(4,q)$. All semipartial geometries embedded in an affine space $\mathrm{AG}(n,q)$ for $n = 2, 3$ are classified. For $n > 3$ the question is however open. Assuming $q > 2$, then apart of the partial quadrangle $T_3^*(O)$, two models of semipartial geometries embeddable in $\mathrm{AG}(4,q)$ are known.

On the one hand there is the semipartial geometry $T_3^*(\mathcal{B})$ with $\mathcal{B}$ a Baer subspace of $\mathrm{PG}(3,q)$, q a square. On the other hand there is the semipartial geometry $\mathrm{spg}(q-1,q^2,2,2q(q-1))$ of Metz, q even. Recently the following results on affine embeddings have been proved. For more details we refer to [5].

Theorem 6 *Let $\mathcal{S}$ be a semipartial geometry* $\mathrm{spg}(q-1,q^2,2,2q(q-1))$ *embedded in* $\mathrm{AG}(4,q)$. *Then $q=2^h$, and $\mathcal{S}$ is the Hirschfeld-Thas model of the semipartial geometry of Metz.*

Corollary

Let $\mathcal{S}$ be a semipartial geometry embedded in $\mathrm{AG}(4,q)$, such that the lines of $\mathcal{S}$ through a point x of $\mathcal{S}$ induce an ovoid θ_x at the hyperplane at infinity, then $\alpha=1$ or 2.

(i) If $\alpha=1$ then $\mu=q(q-1)$, $\theta_x=\theta$ for any point x of $\mathcal{S}$ and $\mathcal{S}$ is isomorphic to $T_3^*(\theta)$.

(i) If $\alpha=2$ then $\mu\leq 2q(q-1)$. If equality holds then $q=2^h$, and $\mathcal{S}$ is the Hirschfeld-Thas model of the semipartial geometry of Metz.

We will see in the next section that the semipartial geometry of Metz is part of bigger family, namely of the family of semipartial geometries constructed from an SPG system.

3.2 SPG systems and semipartial geometries

Very recently Thas [39] has generalized the concept of SPG regulus of a polar space P to SPG systems of P. Without any doubt this concept will open new perspectives in the near future. We will restrict ourselves here to this part of the theory that yield semipartial geometries with new parameters. It is however important to underline that some of the examples (including the partial geometries $\mathrm{PQ}^+(4n-1,2)$ and $\mathrm{PQ}^+(4n-1,3)$) can be constructed from SPG systems.

3.2.1 Definition of an SPG-system and construction of the semipartial geometry

Let $\mathrm{Q}(2n+2,q)$, $n\geq 1$ be a nonsingular quadric of $\mathrm{PG}(2n+2,q)$. An SPG system of $\mathrm{Q}(2n+2,q)$ is a set $\mathcal{D}$ of $(n-1)$-dimensional totally singular subspaces of $\mathrm{Q}(2n+2,q)$ such that the elements of $\mathcal{D}$ on any nonsingular elliptic quadric $\mathrm{Q}^-(2n+1,q)\subset\mathrm{Q}(2n+2,q)$ constitute a spread of the quadric $\mathrm{Q}^-(2n+1,q)$.

Let $\mathrm{Q}^+(2n+1,q)$ be a nonsingular hyperbolic quadric of $\mathrm{PG}(2n+1,q)$, $n\geq 1$. An SPG system of $\mathrm{Q}^+(2n+1,q)$ is a set $\mathcal{D}$ of $(n-1)$-dimensional totally singular subspaces of $\mathrm{Q}^+(2n+1,q)$ such that the elements of $\mathcal{D}$ on any nonsingular quadric $\mathrm{Q}(2n,q)\subset\mathrm{Q}^+(2n+1,q)$ constitute a spread of $\mathrm{Q}(2n,q)$.

Let $\mathrm{H}(2n+1,q)$ be a nonsingular Hermitian variety of $\mathrm{PG}(2n+1,q)$, $n \geq 1$, q a square. An SPG system of $\mathrm{H}(2n+1,q)$ is a set $\mathcal{D}$ of $(n-1)$-dimensional totally singular subspaces of $\mathrm{H}(2n+1,q)$ such that the elements of $\mathcal{D}$ on any nonsingular Hermitian variety $\mathrm{H}(2n,q) \subset \mathrm{H}(2n+1,q)$ constitute a spread of $\mathrm{Q}(2n,q)$.

One can prove that in each case the number of elements in $\mathcal{D}$ equals the number of points of the polar space.

The construction by Thas of the semipartial geometry is as follows. Let P be one of the above polar spaces, i.e. $\mathrm{Q}(2n+2,q)$, $\mathrm{Q}^+(2n+1,q)$, $\mathrm{H}(2n+1,q)$ $(n \geq 1)$. Let $\mathrm{PG}(d,q)$ be the ambient space of P. Hence in the first case $d = 2n+2$, in the other two cases $d = 2n+1$. Let $\mathcal{D}$ be an SPG system of P and let P be embedded in a nonsingular polar space $\bar{P}$ with ambient space $\mathrm{PG}(d+1,q)$ of the same type as P and with projective index n. Hence for $P = \mathrm{Q}(2n+2,q)$, we have $\bar{P} = \mathrm{Q}^-(2n+3,q)$; for $P = \mathrm{Q}^+(2n+1,q)$, we have $\bar{P} = \mathrm{Q}(2n+2,q)$ and for $P = \mathrm{H}(2n+1,q)$, we have $\bar{P} = \mathrm{H}(2n+2,q)$. If $\bar{P}$ is not symplectic and $y \in \bar{P}$, then let τ_y be the tangent hyperplane of $\bar{P}$ at y; if $\bar{P}$ is symplectic and θ is the corresponding symplectic polarity of $\mathrm{PG}(d+1,q)$, then let $\tau_y = y^\theta$ for any $y \in \mathrm{PG}(d+1,q)$.

For $y \in \bar{P} \setminus P$ let $\bar{y}$ be the set of all points z of $\bar{P} \setminus P$ for which $\tau_z \cap P = \tau_y \cap P$. Note that no two distinct points of $\bar{y}$ are collinear in $\bar{P}$. If P is orthogonal then $|\bar{y}| = 2$ except when $P = \mathrm{Q}^+(2n+1,q)$ and q even, in which case $|\bar{y}| = 1$. If P is Hermitian then $|\bar{y}| = \sqrt{q}+1$.

Let ξ be any maximal totally singular subspace of $\bar{P}$, not contained in P, such that $\xi \cap P \in \mathcal{D}$ and let $y \in \xi \setminus P$. Further let $\bar{\xi}$ be the set of all maximal totally singular subspaces η of $\bar{P}$, not contained in P, for which $\xi \cap P = \eta \cap P$ and $\eta \cap \bar{y} \neq \emptyset$.

Let $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ be the incidence structure with $\mathcal{P} = \{\bar{y} \| y \in \bar{P} \setminus P\}$; $\mathcal{L}$ contains all the sets $\bar{\xi}$ as defined above; if $\bar{y} \in \mathcal{P}$ and $\bar{\xi} \in \mathcal{L}$ then $\bar{y} \,\mathrm{I}\, \bar{\xi}$ if and only if for some $z \in \bar{y}$ and some $\eta \in \bar{\xi}$, one has that $z \in \eta$.

In [39] it is proved that this incidence structure is a $(0,\alpha)$-geometry of order (s,t) with $s+1 = q^n$ and $t+1$ the number of elements in a spread of P. The parameter α equals to q^{n-1} times the number of points of $\bar{P}$ in any set $\bar{y} \in \mathcal{P}$.

Theorem 7

1. *If P is the polar space $\mathrm{Q}(2n+2,q)$ then $\mathcal{S}$ is a semipartial geometry $\mathrm{spg}(q^n-1, q^{n+1}, 2q^{n-1}, 2q^n(q^n-1))$.*

2. *If P is the polar space $\mathrm{Q}^+(2n+1,q)$ then the point graph $\Gamma(\mathcal{S})$ is strongly regular if and only if $q = 2$ or $q = 3$. In these cases $\mathcal{S}$ is a partial geometry.*

3. *If P is the polar space $\mathrm{H}(2n+1,q)$ then $\mathcal{S}$ is a semipartial geometry $\mathrm{spg}(q^n - 1, q^n\sqrt{q}, q^{n-1}(\sqrt{q}+1), q^{n-1}(q^n-1)\sqrt{q}(\sqrt{q}+1))$.*

Corollaries

1. Let P be the polar space $\mathrm{Q}(2n+2,q)$. The geometry will be denoted by $TQ(2n+2,q)$.

   If $n=1$ the SPG system is the complete set of points of $\mathrm{Q}(4,q)$ and the semipartial geometry was known before, it is the semipartial geometry of Metz, see [16].

   Assume $n=2$. It is proved in [39] that there are exactly two SPG systems on $\mathrm{Q}(6,q)$. One arises from a spread of $\mathrm{Q}(6,q)$, the other arises from the classical general hexagon of order q.

   For any $n\geq 3$, any spread of $\mathrm{Q}(2n+2,q)$ defines an SPG system. Such a spread is known to exist if q is even.

   In [18] Delanote gives a construction of a semipartial geometry with point graph the graph on the internal points of a quadric $\mathrm{Q}(4m+2,3)$, (vertices are adjacent when non-orthogonal) under the condition of existence of an orthogonal spread. His arguments can easily be generalized for any odd q and in fact, his semipartial geometry is isomorphic to $TQ(2n+2,q)$ with $n=2m$.

2. Let P be the polar space $\mathrm{Q}^+(2n+1,q)$; $q=2$ or 3.

   If $n=2m-1$ is odd and $q=2$ then $\mathrm{Q}^+(2n+1,2)$ has a spread and the partial geometry is isomorphic to the partial geometry $\mathrm{PQ}^+(4m-1,2)$ of De Clerck, Dye and Thas [14].

   If $n=2m-1$ is odd and $q=3$ then the partial geometry is isomorphic to the partial geometry $\mathrm{PQ}^+(4m-1,3)$ of Thas, which only exists if $\mathrm{Q}^+(4m-1,3)$ has a spread; the existence of such a spread is open for $m\geq 3$.

3. Let P be the polar space $\mathrm{H}(2n+1,q)$. The geometry will be denoted by $TH(2n+1,q)$.

   Unfortunately, if $n\geq 2$ then no SPG system of $\mathrm{H}(2n+1,q)$ is known. If $n=1$, then $\mathcal{D}$ =is the set of points of $\mathrm{H}(3,q)$ and the semipartial geometry is the one of Thas as described in [16].

4 Parameter lists

4.1 The known partial geometries (up to duality)

Notation	s	t	α	Remarks and references
$\mathcal{S}(\mathcal{K})$	$2^h - 2^m$	$2^h - 2^{h-m}$	$(2^m - 1)(2^{h-m} - 1)$	$0 < m < h$ and $h \neq 2$, [35, 36]
$T_2^*(\mathcal{K})$	$2^h - 1$	$(2^h + 1)(2^m - 1)$	$2^m - 1$	$0 < m < h$, [35, 36]
$\mathcal{M}_3(n)$	3^{2n-1}	$\frac{1}{2}(3^{4n} - 1)$	$\frac{1}{2}(3^{2n} - 1)$	[25]
$\mathrm{PQ}^+(4n-1, 2)$ (and derivations)	$2^{2n-1} - 1$	2^{2n-1}	2^{2n-2}	$1 < n$, [14]; [9]
$\mathrm{PQ}^+(7, 3)$ (and derivations)	26	27	18	[37]
vL-S	5	5	2	[40]
Haemers	4	17	2	[19]
Mathon	8	20	2	[11]

4.2 The known semipartial geometries

Notation	s	t	α	μ	Remarks and references
$M(r)$	1	$r-1$	1	1	Moore graph $r=2,3,7$
$\overline{M(r)}$	$r-1$	$r-1$	$r-1$	$(r-1)^2$	$r=2,3,7$, [17]
$U_{2,3}(n)$	2	$n-3$	2	4	$n \geq 4$ [17]
$LP(n,q)$	$q(q+1)$	$\frac{q^{n-1}-1}{q-1}-1$	$q+1$	$(q+1)^2$	$n \geq 4$, [17]
$\overline{W(2n+1,q)}$	q	$q^{2n}-1$	q	$q^{2n}(q-1)$	$n \geq 1$,[17]
$\mathrm{NQ}^{+}(2n-1,2)$	2	$2^{2n-3}-2^{n-2}-1$	2	$2^{2n-3}-2^{n-1}$	$n \geq 3$, [16]
$\mathrm{NQ}^{-}(2n-1,2)$	2	$2^{2n-3}+2^{n-2}-1$	2	$2^{2n-3}+2^{n-1}$	$n \geq 3$, [16]
H_q^{n*}	q^2-1	$\frac{q^{n-1}-1}{q-1}-1$	q	$q(q+1)$	$n \geq 4$, [17]
$T_3^*(\mathcal{O})$	$q-1$	q^2	$q(q-1)$	1	[8]
$T_2^*(\mathcal{U})$	q^2-1	q^3	$q^2(q^2-1)$	q	[17]
$T_n^*(\mathcal{B})$	q^2-1	$\frac{q^{n+1}-1}{q-1}-1$	q	$q^2(q^2-1)$	$n \geq 2$, [17]

$TQ(2n+2,q)$	q^n-1	q^{n+1}	$2q^{n-1}$	$2q^n(q^n-1)$	for $n=1$ see also [4] and section 3.1
					if $n \geq 3$ then $q=2^h$ [39]

$TH(3,q^2)$	q^2-1	q^3	$q+1$	$q(q+1)(q^2-1)$	[16]
$\mathrm{RQ}^{-}(2n+3,q)$	$q^{n+1}-1$	q^{n+2}	q^n	$q^{n+1}(q^{n+1}+1)$	q prime power for $n=1$, $q=2^h$ for $n \geq 2$ [38]
Gew(56)	1	9	1	2	$v=56$; Gewirtz graph
HS(77)	1	15	1	4	$v=77$; Higman-Sims family
HS(100)	1	21	1	6	$v=100$ Higman-Sims family
$T_4^*(\mathcal{K}(11))$	2	10	1	2	$v=243$; $\mathcal{K}(11)$ the 11-cap in PG$(4,3)$
$T_5^*(\mathcal{K}(56))$	2	55	1	20	$v=729$; $\mathcal{K}(56)$ the 56-cap in PG$(5,3)$
$T_5^*(\mathcal{K}(78))$	3	77	1	14	$v=1024$; $\mathcal{K}(78)$ the 78-cap of Hill in PG$(5,4)$

References

[1] R. C. Bose. Strongly regular graphs, partial geometries and partially balanced designs. *Pacific J. Math.*, 13:389–419, 1963.

[2] A. E. Brouwer, W. H. Haemers, and V. D. Tonchev. Embedding partial geometries in Steiner designs. In J. W. P. Hirschfeld, S.S. Magliveras, and M.J. de Resmini, editors, *Geometry, Combinatorial Designs and Related Structures*, pages 33–41, Cambridge, 1997. Cambridge University Press.

[3] A. E. Brouwer, A. V. Ivanov, and M. H. Klin. Some new strongly regular graphs. *Combinatorica*, 9:339–344, 1989.

[4] M. Brown. Semipartial geometries and generalized quadrangles of order (r, r^2). *Bull. Belg. Math. Soc. – Simon Stevin*, 5:187–206, 1998.

[5] M. Brown, F. De Clerck, and M. Delanote. Affine semipartial geometries and projections of quadrics. Preprint, 2000.

[6] F. Buekenhout, editor. *Handbook of Incidence Geometry, Buildings and Foundations*. North-Holland, Amsterdam, 1995.

[7] A. R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bull. London Math. Soc.*, 18:97–122, 1986.

[8] P. J. Cameron. Partial quadrangles. *Quart. J. Math. Oxford Ser. (2)*, 26:61–73, 1975.

[9] F. De Clerck and M. Delanote. Partial geometries and the triality quadric. To appear in J. Geometry, 2000.

[10] F. De Clerck and M. Delanote. Two-weight codes, partial geometries and Steiner systems. To appear in Des. Codes Cryptogr., 2000.

[11] F. De Clerck, M. Delanote, N. Hamilton, and R. Mathon. Perp-systems and partial geometries. Preprint, 2000.

[12] F. De Clerck. The pseudo–geometric $(t, s, s-1)$–graphs. *Simon Stevin*, 53:301–317, 1979.

[13] F. De Clerck. New partial geometries derived from old ones. *Bull. Belg. Math. Soc. – Simon Stevin*, 5:255–263, 1998.

[14] F. De Clerck, R. H. Dye, and J. A. Thas. An infinite class of partial geometries associated with the hyperbolic quadric in $\mathrm{PG}(4n-1, 2)$. *European J. Combin.*, 1:323–326, 1980.

[15] F. De Clerck, H. Gevaert, and J. A. Thas. Partial geometries and copolar spaces. In A. Barlotti, G. Lunardon, F. Mazzocca, N. Melone, D. Olanda, A. Pasini, and G. Tallini, editors, *Combinatorics '88*, pages 267–280, Rende (I), 1991. Mediterranean Press.

[16] F. De Clerck and H. Van Maldeghem. Some classes of rank 2 geometries. In F. Buekenhout, editor, *Handbook of Incidence Geometry, Buildings and Foundations*, chapter 10, pages 433–475. North-Holland, Amsterdam, 1995.

[17] I. Debroey and J. A. Thas. On semipartial geometries. *J. Combin. Theory Ser. A*, 25:242–250, 1978.

[18] M. Delanote. A new semipartial geometry. *J. Geometry*, 67:89–95, 2000.

[19] W. Haemers. A new partial geometry constructed from the Hoffman–Singleton graph. In P. J. Cameron, J. W. P. Hirschfeld, and D. R. Hughes, editors, *Finite Geometries and Designs*, volume 49 of *London Math. Soc. Lecture Note Ser.*, pages 119–127, Cambridge, 1981. Cambridge University Press.

[20] M. Hall, Jr. and R. Roth. On a conjecture of R. H. Bruck. *J. Combin. Theory Ser. A*, 37:22–31, 1984.

[21] J. W. P. Hirschfeld and J. A. Thas. The characterizations of projections of quadrics over finite fields of even order. *J. London Math. Soc. (2)*, 22:226–238, 1980.

[22] W. M. Kantor. Strongly regular graphs defined by spreads. *Israel J. Math.*, 41:298–312, 1982.

[23] M. H. Klin. On new partial geometries pg(8,9,4), 1998. contributed talk, 16th British Combinatorial Conference.

[24] E. Kuijken. A geometric description of Hermitian two-graphs and its applications. Talk at Combinatorics'2000.

[25] R. Mathon. A new family of partial geometries. *Geom. Dedicata*, 73:11–19, 1998.

[26] R. Mathon and A. Penfold Street. Overlarge sets and partial geometries. *J. Geom.*, 60(1–2):85–104, 1997.

[27] P. Panigrahi. *On the geometrisability of some strongly regular graphs related to polar spaces.* PhD thesis, Indian Statistical Institute, Bangalore, 1997.

[28] S. E. Payne and J. A. Thas. *Finite Generalized Quadrangles*, volume 110 of *Research Notes in Mathematics.* Pitman, Boston, 1984.

[29] S. Reichard. An algorithm for the construction of partial geometries with given point graphs. Preprint of the Technische Universität Dresden, 1997.

[30] J. J. Seidel. A survey of two-graphs. In *Teorie Combinatorie, Proc. Intern. Colloq. (Roma 1973)*, volume I, pages 481–511. Accad. Naz. Lincei, 1976.

[31] E. E. Shult and J. A. Thas. m-systems of polar spaces. *J. Combin. Theory Ser. A*, 68(1):184–204, 1994.

[32] E. E. Shult and J. A. Thas. m-systems and partial m-systems of polar spaces. *Des. Codes Cryptogr.*, 8(1-2):229–238, 1996. Special issue dedicated to Hanfried Lenz.

[33] E. Spence. Is Taylor's graph geometric? *Discrete Math.*, 106/107:449–454, 1992.

[34] D. E. Taylor. Regular 2-graphs. *Proc. London Math. Soc.*, 35:257–274, 1977.

[35] J. A. Thas. Construction of partial geometries. *Simon Stevin*, 46:95–98, 1973.

[36] J. A. Thas. Construction of maximal arcs and partial geometries. *Geom. Dedicata*, 3:61–64, 1974.

[37] J. A. Thas. Some results on quadrics and a new class of partial geometries. *Simon Stevin*, 55:129–139, 1981.

[38] J. A. Thas. Semi-partial geometries and spreads of classical polar spaces. *J. Combin. Theory Ser. A*, 35:58–66, 1983.

[39] J. A. Thas. SPG systems and semipartial geometries. Preprint, 2000.

[40] J. H. van Lint and A. Schrijver. Construction of strongly regular graphs, two–weight codes and partial geometries by finite fields. *Combinatorica*, 1:63–73, 1981.

Affine Semipartial Geometries and Projections of Quadrics

M. Delanote

Department of Pure Mathematics and Computer Algebra
University of Ghent
Galglaan 2, B-9000 Gent - Belgium
e-mail: md@cage.rug.ac.be

A *semipartial geometry* with parameters s, t, α, μ, denoted by $\mathrm{spg}(s, t, \alpha, \mu)$, is a partial linear space of order (s, t) such that for all antiflags (x, L) the incidence number $\alpha(x, L)$ equals 0 or a constant α $(\neq 0)$ and such that for any two points which are not collinear, there are μ (> 0) points collinear with both points. Debroey and Thas introduced semipartial geometries and raised the question of finding a classification of semipartial geometries embedded in $\mathrm{AG}(n, q)$. A complete answer was given when $n = 2, 3$. For $n > 3$ the question is open. We prove that an $\mathrm{spg}(q-1, q^2, 2, 2q(q-1))$ embedded in $\mathrm{AG}(4, q)$ must be the known model coming from the projection of the elliptic quadric $Q^-(5, q)$, q even, from a point off the quadric.

Ovoidal Linear Spaces

P. De Vito*, N. Melone

Università di Napoli, Italy

e-mail: devito@matna2.dma.unina.it

An interesting problem in Incidence Geometry consists in the characterization of linear spaces satisfying suitable combinatorial conditions [1, 4, 5].

As in the classical case, a cap in a finite linear space is a subset Ω of points meeting every line in at most two points. The tangent set to a point $x \in \Omega$ is the union of the one-secant lines through x. Results on finite planar spaces with caps are obtained in the papers [2, 3, 6].

The aim of this paper is to prove that a finite linear space, not generated by three points, in which a cap Ω exists, with few exterior lines and such that the tangent sets satisfy suitable conditions, is either a double near-pencil and Ω consists of two points or the 3-dimensional Galois space $PG(3, q)$ and Ω is an ovoid.

References

[22] A. Beutelspacher, K. Metsch: *Embedding finite linear spaces in projective planes*, Ann. Discrete Math., **30**, (1986), 43-61.

[23] P. Biondi: *An embedding theorem for finite planar spaces*, Rend. Circolo matematico di Palermo, Serie II, Tomo **XLVII** (1998), 265-276.

[24] P. Biondi, P.M. Lo Re: *Generalized Q-sets in a finite locally projective planar space*, Discrete Math., **208-209**, (1999), 85-102.

[25] J. Kahn: *Locally projective planar lattices which satisfies the bundle theorem*, Math. Z., **175**, (1980), 219-247.

[26] W.M. Kantor: *Dimension and embedding theorems for geometric lattices*, J. Combin.Theory, A, **17**, (1974), 173-195.

[27] G. Tallini: *Ovoids and caps in planar spaces*, Ann. Discrete Math., **30**, (1986), 347-354.

Pappus' Configuration in non Commutative Projective Geometry with Applications to a Theorem of A. Schleiermacher

G. Donati

Università di Napoli "Federico II" - Napoli
e-mail: donati@matna2.dma.unina.it

In non commutative projective geometry there exist Pappus' configuration whose diagonal points are not collinear. We consider two lines r and s in a projective plane and the points A, B on r, A', B', C'on s, and we investigate which points X on r lead to collinear diagonal points in corresponding Pappus' configuration. A geometric interpretation is given, showing that these are exactly all the fixed points of a projectivity ω of the line r. Further the system of fixed points of a large class of projectivities of the line r may be seen as the set of points X on r such that the diagonal points of Pappus' configuration defined by X and other points, are collinear. Finally, with the help of the projectivity ω, which is product of three perspectivities, we are able to improve a result of Schleiermacher ([3] or [2]) proving that every desarguesian projective plane satisfying the property $P_{n,3}$ (that is a projectivity of a line into itself which is product of at most three perspectivities with n fixed points is the identity)is a pappian plane.

References

[28] G. Donati: *On Pappus' configuration in non commutative projective geometry*, Submitted.

[29] G. Pickert: *Projectivities in Projective Planes*, In: *Geomerty: von Staudt point of view.* D. Reidel Publ. Co., 1981, 1-49.

[30] A. Schleiermacher: *Über projective Ebenen, in denen jede Projectivität mit sechs Fixpunkten die Identität*, ist. *MZ* **114** 313-320 (1971).

Blocking Semiovals in *PG*(2,7) and Beyond

J. Dover
U.S. Dept. of Defense
9800 Savage Rd. Ft. George G. Meade, MD 20755-6000, USA
e-mail: jdover@aol.com

A blocking semioval in a projective plane is a set with is both a blocking set and a semioval (i.e. there exists a unique tangent at each point). In this talk, we discuss a search for all blocking semiovals in $PG(2,7)$, as well as some infinite families which have arisen from the results of this search.

Polarity-paired Spreads of PG(3,q), q Odd

G. Ebert, C. Culbert*

University of Delaware, USA
e-mail: culbert@math.udel.edu

In PG$(3, q)$ there exist spreads where each line is fixed by a symplectic polarity. Are there spreads where the symplectic polarity acts on the spread and fixes no line of the spread, thereby pairing the lines? Such a spread will be called *polarity-paired*. These spreads can only exist if q is odd. The search for symplectic polarity-paired spreads was motivated by J.W.P. Hirschfeld, who raised the question of their existence. Such spreads do exist for all odd q, the Hall spread being one such example. For $q \equiv 3 \mod 4$ a "special" spread corresponding to a certain flag-transitive plane is always symplectically paired. Polarity-paired spreads also exist for orthogonal polarities. The regular spread is an example for an elliptic polarity and the Hall spread for a hyperbolic polarity. Other examples of spreads have also been obtained.

On Construction of Bound Graphs

H. Era, S.-I.Iwai, K.Ogawa, M.Tsuchiya*

Department of Mathematical Sciences, Tokai University
e-mail: tsuchiya@ss.u-tokai.ac.jp

In this talk, we consider construction of upper bound graphs and double bound graphs. An upper bound graph can be transformed into a nova by contractions and a nova also can be transformed into an upper bound graph by splits. These results induce a characterization on upper bound graphs as follows:

Let G be a connected graph. G is a upper bound graph if and only if the graph obtained by successive contractions of all pairs of adjacent non-simplicial vertices u, v adjacent to a simplicial vertex w in G is a nova. We also consider construction of double bound graphs. A double bound graph can be transformed into a bipartite graph by deletions and a bipartite graph also can be transformed into a double bound graph by additions. These results induce a characterization on double bound graphs.

A Construction of Arcs in High–dimensional Projective Spaces

G. Faina, Gy. Kiss*, S. Marcugini, F. Pambianco

University of Budapest, Hungary
e-mail: kissgy@cs.elte.hu

The n–dimensional finite projective space, $PG(n,q)$ admits a cyclic model, in which the set of points of $PG(n,q)$ is identified with the elements of the group $\mathbf{Z}_{q^n+q^{n-1}+\ldots+q+1}$. It was proved by M. Hall that in the cyclic model of $PG(2,q)$, the additive inverse of a line is a conic. The following generalization of this result is proved:

In the cyclic model of $PG(n,q)$, the additive inverse of a line is a $(q+1)$-arc if $n+1$ is a prime and $q+1>n$.

It is also shown that in any dimension almost all of the lines have the property that its additive inverse is an arc. A line ℓ is called *exceptional,* if $-\ell$ is also a line. The number of exeptional lines in $PG(n,q)$ is determined, and it is proved that the exceptional lines form interesting objects.

Dividing Cyclotomic Polynomials

G. Falcone

Dipartimento Matematica e Applicazioni - Università di Palermo
Viale delle scienze, Palermo
e-mail: falcone@mi.uni-erlangen.de

Given two cyclotomic polynomials $\Phi_n(x), \Phi_m(x)$ $(n \neq m)$, an integer k and two integral polynomials $a(x), b(x)$ exist, such that

$$k = a\Phi_n + b\Phi_m,$$

for $\Phi_n(x), \Phi_m(x)$ are irreducible. Determining k is our goal.

An Intrinsic Characterisation of Quadrics

E. Ferrara Dentice
Napoli, Italy
e-mail: Eva.FerraraDentice@unina2.it

Quadrics of a projective space $PG(n, K)$ of finite dimension n over a field K are widely studied. Some results about elliptic quadrics in $PG(n, q)$ have been obtained by A. Barlotti and G. Panella in 1955, and, about general quadrics, by G. Tallini in 1956/57. In this context, the notion of Tallini set (name suggested by C. Lefèvre in 1975) naturally arose, and we can find many characterisations of quadrics as Tallini sets satisfying suitable arithmetic or incidence conditions (see Tallini, 1956/57; Buekenhout-Lefèvre, 1976; Lefèvre-Percsy, 1980; Ferrara Dentice-Lo Re-Melone, 1996). In this talk I point out my attention on the point-line geometry of a quadric within semilinear spaces, in which the incidence geometry of ruled algebraic varieties is naturally studied.

A **semilinear space** is a point-line geometry such that any two distinct points lie on at most one line, any line contains at least two points and any point lies on at least one line. Two distinct points are said to be **collinear** if there exists a line containing them, and two subsets of points are collinear if each point of one of them is collinear with all points of the other one. A **subspace** is a subset W of pairwise collinear points such that the line joining two of them is contained in W. The **rank** of the semilinear space is the maximum lenght of all saturated chains of subspaces $W_0, \dots, W_k$, such that W_0 is a point and W_k is a maximal subspace with respect to inclusion. Finally, the semilinear space is said to be **non singular** if it does not contain any point collinear with all the others, and **connected** if for any pair of points p, q there exists a finite chain of points $p = p_1, p_2, \dots, p_t = q$ such that p_i is collinear with $p_i + 1$, for $i = 1, \dots, t$.

Using the characterisation of polar spaces of Buekenhout-Shult (1974) and the notion of Tallini set of a desarguesian projective space, I prove the following Theorem.

THEOREM. *Let P be a connected and non singular semilinear space of rank $d \geq 4$, whose lines are not maximal subspaces and satisfying the following condition:*

> *For every pair L, M of non collinear disjoint lines, the set W of all the points collinear with L and M contains at least one point external to L and M and, if W contains at least one point of $L \cup M$, then it is a subspace intersecting L and M.*

Then there exist a field K and a projective space $PG(n, K)$ such that P is a quadric of $PG(n, K)$.

Unitary Polarities in non Commutative Twisted Field Plane

E. Francot

Università di Lecce, Italy
e-mail: francot@ilenic.unile.it

A parabolic unital of an affine plane π^{l_∞} is the affine restriction of a unital of π with exactly one point L_∞ on l_∞. So l_∞ is the tangent of the unital at this point. A transitive parabolic unital is a parabolic unital which is invariant under a collineation group of π fixing L_∞ and transitive on the remaining q^3 affine points.

Examples of transitive parabolic unitals embedded in $PG(2, q^2)$ are the Hermitian unitals and the Buekenhout-Metz unitals arising from elliptic quadrics of $PG(3, q)$ [1].

Further examples of transitive parabolic unitals are given by Ganley in [5] and by Korchmaros with other authors in [2]. They consist of the absolute points and non absolute lines of a unitary polarity in a plane over a Dickson semifield of odd order q^2 and in a commutative twisted field plane respectively . In fact, by [4], it is easily to prove that every plane over a commutative semifield with an involutory automorphism admits transitive parabolic unitals. In a recent paper [3], Biliotti, Jha and Johnson devoted their attention to generalized twisted field planes in order to examine carefully the properties of the collineations and the correlations of these planes, in particular they determined all the possible polarities. Besides the known ones, in commutative twisted field planes, another class of polarities has been exhibited in suitable non commutative twisted field planes. In the paper, starting from the results given in [3], the polarities in non commutative twisted field planes are investigated in details; it is proved that these polarities are unitary and conjugate under the collineation group on the plane. In particular it is proved that the associated unitals are transitive parabolic unitals. To the author's knowledge these are the first examples of transitive parabolic unitals in non commutative semifield planes. They are also the first examples of transitive parabolic unitals in non desarguesian planes of even order.

References

[31] Abatangelo, V. - Larato, B.: *A group-theoretical characterization of parabolic Buekenhout-Metz unitals*, Boll. Un. Mat. It. (7) **5-A** (1991), 195-206.

[32] Abatangelo, V. - Enea, M.R., - Korchmaros, G. - Larato, B.: *Ovals and unitals in commutative twisted field planes*, Discr. Math. **208** (1999), 3-8.

[33] Biliotti, M. - Jha, V. - Johnson, N. L.: *The collineation groups of generalized twisted field planes*, Geom. Dedicata **76** (1999), 97-126.

[34] Ganley, M.J.: *Polarities in translation planes*, Geom. Dedicata **1** (1972), 103-116.

[35] Ganley, M.J.: *A class of unitary block designs*, Math. Z. **128** (1972), 34-42.

On 2–factor Hamiltonian Bipartite Graphs

M. Funk, D. Labbate*

Università degli Studi della Basilicata - Potenza, Italy
e-mail: `ld487sci@unibas.it`

W. Jackson

London, UK

J. Sheehan

Aberdeen, UK

A graph G is 2–*factor hamiltonian* if every 2–factor of G is a Hamilton circuit, whereas a k–regular bigraph H is *minimally 1–factorable* if every 1–factor of H is contained in a unique 1–factorization of H. We are interested in determining which regular graphs can be 2–factor hamiltonian. We prove that if H is minimally 1–factorable and $k \geq 2$ then H is 2–factor hamiltonian. In particular, if $k = 3$, then H is minimally 1–factorable if and only if H is 2–factor hamiltonian. Furthermore, we show that there are no 2–factor hamiltonian k–regular bigraphs for $k \geq 4$.

Canonically Pfaffian Cubic Bigraphs and Blocking–set–free Configurations

M. Funk*, D. Labbate

Università degli Studi della Basilicata - Potenza, Italy
e-mail: funk@unibas.it

W. Jackson

London, UK

J. Sheehan

Aberdeen, UK

Recently N. Robertson, P. D. Seymour, R. Thomas and, independently, W. McCuaig found a good characterization of bipartite graphs admitting a *Pfaffian* orientation, i.e an orientation where every central circuit has an odd number of edges in both directions. We investigate the class of cubic bigraphs G where a Pfaffian orientation is obtained by orienting each edge in the same way, say from X to Y, with respect to the bipartition $V(G) = X \cup Y$. If G is 3–connected, a characterization has already been given by W. McCuaig. We prove that all such 2–connected graphs can be obtained from cubic bigraphs with a Pfaffian orientation by substituting edges not oriented from X to Y by a suitable combination of copies of the Heawood graph. This result completes the classification of all blocking-set-free symmetric configurations of type n_3.

Actions of Permutation Groups

D.A. Gewurz

Università di Roma "La Sapienza", Italy
e-mail: gewurz@mat.uniroma1.it

We are interested in actions induced by permutation groups (other than the natural one), mainly on the set of cycles appearing in their elements. This can always be done for finite groups and, with some care, for infinite ones: some similarities and differences among the two situations will be presented.

Upper and Lower Chromatic Numbers for P_3-Designs

L. Gionfriddo

Department of Mathematics, University of Catania
Viale A. Doria, 6 – 95125 Catania, Italy.
e-mail: lucia@dipmat.unict.it

A *mixed hypergraph* is a triple $\mathcal{H} = (X, \mathcal{C}, \mathcal{D})$ where X is the vertex set and each of $\mathcal{C}, \mathcal{D}$ is a list of no-empty subsets of X, called $\mathcal{C} - edges$ and $\mathcal{D} - edges$ respectively. In a *proper k-coloring* of $\mathcal{H}$, any $\mathcal{C}-edge$ has at least two vertices with the same color and any $\mathcal{D}-edge$ has at least two vertices colored with different colors. The minimum number k of colors for which there exists a proper k-coloring of $\mathcal{H}$ is called the *lower chromatic number* χ, the maximum number is called the *upper chromatic number* $\bar{\chi}$. The theory of mixed hypergraphs was introduced by V. Voloshin (*The mixed hypergraphs* Computer Sciences Journal of Moldova, 1993) and it had a great development. Many authors studied this kind of coloring, also for Steiner systems. Actually, the study regards the determination of hypergraphs with $\chi = \bar{\chi}$, of uncolorable hypergraphs and hypergraphs with broken-spectrum (i.e. $\chi < \bar{\chi}$ and no-existence of some proper k-coloring with $\chi < k < \bar{\chi}$). Recently, we have constructed same classes of uncolorable $P_3 - designs$, other classes of uniquely $P_3 - designs$ and classes of $P_3 - designs$ having broken–spectrum.

On Complete Arcs Arising from Plane Curves

M. Giulietti*, F. Pambianco, F. Torres, E. Ughi

Dipartimento di Matematica - Università degli Studi di Perugia - Perugia, Italy
e-mail: giuliet@dipmat.unipg.it

A (k,d)-*arc* $\mathcal{K}$ in $\mathbf{P}^2(\mathbf{F}_q)$, $\mathbf{F}_q$ being the finite field with q elements, is a set of k elements such that no line in $\mathbf{P}^2(\mathbf{F}_q)$ meets $\mathcal{K}$ in more than d points. The (k,d)-arc is *complete* if it is not contained in a $(k+1,d)$-arc.

A natural example of a (k,d)-arc is the set $\mathcal{X}(\mathbf{F}_q)$ of $\mathbf{F}_q$-rational points of a plane curve $\mathcal{X}$ defined over $\mathbf{F}_q$, where k is the number of $\mathbf{F}_q$-rational points of $\mathcal{X}$ and d is the degree of $\mathcal{X}$.

Only few examples of plane curves giving rise to complete arcs are known. Here we show that the set of $\mathbf{F}_q$-rational points of either certain Fermat curves or certain $\mathbf{F}_q$-Frobenius non-classical plane curves is a complete (k,d)-arc in $\mathbf{P}^2(\mathbf{F}_q)$.

Maximal Partial t-spreads and Minimal t-covers in Finite Projective Spaces

P. Govaerts*

Ghent University - Dept. of Pure Mathematics and Computer Algebra
Krijgslaan 281, 9000 Gent, Belgium
e-mail: `pg@cage.rug.ac.be`

L. Storme

University of Gent - Dept. of Pure Maths and Computer Algebra
Krijgslaan 281 - 9000 Gent, Belgium
e-mail: `ls@cage.rug.ac.be`

A *t-spread* of $\mathrm{PG}(N,q)$, $(t+1)|(N+1)$, is a partitioning of the point set of $\mathrm{PG}(N,q)$ into t-dimensional subspaces. A *partial t-spread* in $\mathrm{PG}(N,q)$, $(t+1)|(N+1)$, is a set of pairwise disjoint t-dimensional subspaces. A partial t-spread is called *maximal* when it cannot be extended to a larger partial t-spread. The *deficiency* δ of a partial t-spread is the number of t-dimensional spaces it has less than a t-spread.

For $\delta \leq \sqrt{q}$, it is known that partial t-spreads of deficiency δ are uniquely extendable to a t-spread. We improve on this result.

We also study t-covers of $\mathrm{PG}(N,q)$. A *t-cover* of $\mathrm{PG}(N,q)$, $(t+1)|(N+1)$, is a set of t-dimensional subspaces covering all the points of $\mathrm{PG}(N,q)$. A t-cover is called *minimal* when it has no proper subset that is still a t-cover. The excess r of a t-cover is the number of t-dimensional spaces it has more than a t-spread.

For small excess r, we describe the configuration of points covered by more than one element of the t-cover.

On some Generalizations of Symmetric Designs

H. Gropp

Mühlingstr. 19, D-69121 Heidelberg, Germany
e-mail: d12@ix.urz.uni-heidelberg.de

Definition: A *symmetric (v,k,λ)-design* is a finite incidence structure of v elements and v blocks such that each block contains k elements, each element occurs on k blocks, and (*) 2 different elements occur in a common block exactly λ times. This talk will discuss some of the following generalizations of this concept and investigate further properties of these discrete structures. Concerning the time restrictions I shall mainly focus on recent results on configurations.

Tactical Configurations: Without the above condition (*) we obtain a *tactical configuration TC(v,k).*

Even Designs: For *even designs ED(v,k)* condition (*) is replaced by (**) 2 different elements occur in a common block an even number of times.

Symmetric Configurations: For *symmetric configurations* v_k condition (*) is replaced by (***) 2 different elements occur in a common block at most once.

Orbital Matrices: All the structures above can be described by square incidence matrices of entries 0 and 1 denoting the incidence of elements and blocks in the usual way. An *orbital matrix $OM(v,k,x;\lambda)$* is described by a corresponding matrix A of size v with non-negative integer entries and row and column sum k such that $AA^t = (k+x-\lambda)I_v + \lambda J_v$ where I_v and J_v denote the identity matrix and the all-one-matrix of size v and A^t denotes the transpose of A.

The Combinatorics of Generators for Galois Fields

Dirk Hachenberger

Institut für Mathematik der Universität Augsburg,
D-86135 Augsburg, Germany
e-mail: `hachenberger@math.uni-augsburg.de`

We report on recent results concerning generators for algebraic extensions of Galois fields.

Keywords. Finite (Galois) field, irreducible polynomial, primitive element, normal element, normal basis, complete normal basis, completely normal element.

Mathematics Subject Classification: 11T, 12E20.

1 Introduction and outline

Galois fields (or finite fields) are a fundamental algebraic structure of Discrete Mathematics. They are important for Algebraic and Finite Geometry and have become an established tool in applied disciplines like Coding Theory, Cryptography or Signal Processing. Concerning the existence of particular generators for algebraic extensions of finite fields, considerable progress has been achieved in the last years, and it is our aim to report on these new developments by emphasizing the combinatorial aspects underlying these generators. In particular we shall discuss the following topics:

- the explicit construction of normal bases (Section 4);
- the existence of primitive normal bases with precribed trace or norm (Section 5);
- cyclotomic polynomials and their (additive) q-analogues (Section 6, introduced in Section 3);
- the structure of cyclotomic modules under the complete point of view (Section 7);

- the enumeration of completely normal elements (Section 8);
- the existence of primitive complete normal bases (Section 9).

We shall not discuss generators for infinite algebraic extensions of finite fields, here, and refer to [Ha1 (Section 26), Ha3, Ha4, Sche], instead. In Section 2 and Section 3 of the present work we shall start with some classical results on the theory of finite fields and thereby fix our notation. Most of these facts are well-known and may be found in several texts on algebra or number theory. The standard reference for finite field theory is Lidl and Niederreiter [LiNi]. For the early history of Galois fields we refer to the recent paper of Lüneburg [Lü].

The contents of Section 2 and Section 3 are presented as variations of a fundamental combinatorial theme, namely Möbius inversion over partially ordered sets (see Rota [Ro]). The variations concern three objects which are of fundamental importance for the theory of finite fields, namely

- irreducible polynomials,
- primitive elements, and
- normal bases.

The rest of this section is devoted to introduce the unifying combinatorial theme.

Consider a triple $(S, \mathcal{A}, \subseteq)$, where S is a nonempty set and $\mathcal{A}$ is a nonempty collection of finite subsets of S such that $S = \cup_{A\in\mathcal{A}} A$. We assume further that $\cap_{G\in\mathcal{G}} G \in \mathcal{A}$ for all nonempty subsets $\mathcal{G}$ of $\mathcal{A}$. The symbol $\subseteq$ indicates that $\mathcal{A}$ is considered as a partially ordered set with respect to set inclusion. For every $x \in S$ the *subset of S (in $\mathcal{A}$) generated by x* is defined by

$$\langle x\rangle_{S,\mathcal{A}} := \bigcap_{A\in\mathcal{A},\ x\in A} A.$$

Observe that $\langle x\rangle_{S,\mathcal{A}}$ is in fact a member of $\mathcal{A}$. The *Euler function* $\phi_{S,\mathcal{A}}$ for $(S, \mathcal{A}, \subseteq)$ is defined by

$$\phi_{S,\mathcal{A}} : \mathcal{A} \to \mathbb{N}_0, A \mapsto |\{x \in S : \langle x\rangle_{S,\mathcal{A}} = A\}|,$$

(where $|X|$ denotes the cardinality of the set X and $\mathbb{N}_0$ the set of nonnegative integers). Now, we have

$$|A| = \sum_{B\in\mathcal{A},\ B\subseteq A} \phi_{S,\mathcal{A}}(B),$$

and therefore Möbius inversion yields

$$\phi_{S,\mathcal{A}}(A) = \sum_{B\in\mathcal{A},\ B\subseteq A} |B| \cdot \mu_{S,\mathcal{A}}(B, A),$$

where $\mu_{S,\mathcal{A}}$ denotes the *Möbius function* for the partially ordered set $(\mathcal{A}, \subseteq)$.

If $\phi_{S,\mathcal{A}}(A) \geq 1$ for all $A \in \mathcal{A}$ then one has $\mathcal{A} = \{\langle x \rangle_{S,\mathcal{A}} : x \in S\}$, whence $(S, \mathcal{A}, \subseteq)$ might be called *cyclic.* The latter situation will be met when dealing with finite fields.

2 The basic structure of Galois fields

The cardinality of a finite field F is a power $q = p^m$ $(m \geq 1)$ of a prime p (the characteristic of the field). Conversely, for any prime power q there exists a field with q elements and any two such fields are isomorphic. The unique field F with q elements is also denoted by $\mathrm{GF}(q)$.

Given a finite field F it is convenient to work in an algebraic closure $\bar{F}$ of F. Let $\mathcal{E}$ denote the collection of all finite subfields of $\bar{F}$ which are extensions of F. We here consider the triple $(\bar{F}, \mathcal{E}, \subseteq)$.

For any integer $n \geq 1$ there exists exactly one extension E_n in $\bar{F}$ with degree n over F. E_n is thus a field with q^n elements and we have $\mathcal{E} = \{E_n | n \in \mathbb{N}\}$ (where $\mathbb{N}$ denotes the set of positive integers). If $v \in \bar{F}$ then $\langle v \rangle_{\bar{F},\mathcal{E}} = F(v)$ is the field obtained by adjoining v to F. If $F(v) = E_n$, then n is called the *degree of* v *over* F. One has $E_d \subseteq E_n$ if and only if d divides n, and therefore an application of Möbius inversion yields that the number of $\gamma_q(n) := \phi_{\bar{F},\mathcal{E}}(n)$ of $v \in \bar{F}$ having degree n over F is equal to

$$\gamma_q(n) = \sum_{d|n} \mu(\frac{n}{d}) q^d. \tag{2.1}$$

(The sum runs over all positive divisors of n and μ denotes the classical Möbius function for the partially ordered set (with respect to divisibility) of natural numbers, i.e., $\mu(1) = 1$, $\mu(k) = 0$ if k is divisible by the square of a prime and $\mu(k) = (-1)^r$ if k is square-free and r is the number of distinct prime divisors of k.) It is easily seen that

$$\gamma_q(n) \geq q^n - \frac{q^n - 1}{q - 1} \geq 1.$$

The *minimal polynomial* ν_v *(over* F*) of* $v \in \bar{F}$ is the monic $f \in F[x]$ of least degree such that $f(v) = 0$. It is clear that ν_v is irreducible over F, and the degree of v, say n, is equal to the degree of ν_v. Conversely, if $\iota \in F[x]$ is monic and irreducible of degree n, then all roots of ι have degree n over F (whence E_n is the splitting field of ι and thus is isomorphic to the residue ring $F[x]/\iota F[x]$). Therefore, using (2.1), we conclude that the number $i_q(n)$ of monic irreducible $\iota \in F[x]$ of degree n is equal to

$$i_q(n) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d. \tag{2.2}$$

The determination of an irreducible ι in $F[x]$ with specified degree n is necessary to obtain a concrete description of E_n as a residue ring of $F[x]$. Unfortunately, no deterministic algorithm is known which, for a general pair (q, n), produces a monic irreducible $\iota \in F$ (of degree n) and runs in polynomial time (in n and $\log(q)$). However, as there are plenty of irreducible polynomials and since testing irreducibility is easy, such polynomials can efficiently be determined at random. For algorithmic versions and the complexity status of the fundamental results from finite fields we refer to Lenstra [Le].

We finally mention that the roots (in $\bar{F}$) of the polynomial $x^{q^n} - x \in F[x]$ are exactly the elements of E_n (the latter polynomial is the basic example of a q-linearized polynomial). Let $I_{q,n}$ be the product of all $\iota \in F[x]$ which are monic and irreducible of degree n. Since $x^{q^n} - x$ is square-free we obtain

$$x^{q^n} - x = \prod_{d|n} I_{q,n}, \tag{2.3}$$

and therefore a further application of the Möbius inversion principle (in a version for polynomials) yields

$$I_{q,n} = \prod_{d|n} (x^{q^d} - x)^{\mu(n/d)}. \tag{2.4}$$

3 The multiplicative and the additive group

As in Section 2 let $F = \mathrm{GF}(q)$ be a finite field (with characteristic p) and $\bar{F}$ the algebraic closure of F. In the present section we investigate the multiplicative group $\bar{F}^*$ and the additive group $(\bar{F}, +)$ of $\bar{F}$.

We start with the multiplicative group by considering the triple $(\bar{F}^*, \mathcal{U}, \subseteq)$ where $\mathcal{U}$ denotes the collection of all finite subgroups of $\bar{F}^*$. The members of $\mathcal{U}$ correspond bijectively to the positive integers which are not divisible by p: the subgroup corresponding to N is

$$U_N := \{v \in \bar{F}^* | v^N = 1\}, \tag{3.1}$$

i.e., U_N consists of all *Nth roots of unity.* By the choice of N the cardinality of U_N is equal to N. Furthermore, any such group is cyclic, i.e., free on one generator as a module over the ring of integers. For $v \in \bar{F}^*$ the *(multiplicative) order of* v is defined to be the smallest integer $k \geq 1$ such that $v^k = 1$ (it is denoted by $\mathrm{ord}(v)$). The generators of U_N are exactly the elements whose order is equal to N, i.e., $\langle v \rangle_{\bar{F}^*, \mathcal{U}} = U_N$ if and only if $\mathrm{ord}(v) = N$. If $\mathrm{ord}(v) = N$ then v is also called a *primitive Nth roots of unity.* Since $U_D \subseteq U_N$ if and only if D divides N, Möbius inversion yields that the number $\varphi(N) := \phi_{\bar{F}^*, \mathcal{U}}(N)$ of $v \in \bar{F}$ with $\mathrm{ord}(v) = N$ is equal to

$$\varphi(N) = \sum_{D|N} \mu(\frac{N}{D}) D, \tag{3.2}$$

i.e., φ is the classical Euler totient function counting the number of $D \leq N$ ($D \in \mathbb{N}$) which are relatively prime to N.

Concerning the multiplicative structure of finite fields, the most interesting objects are the *primitive elements*: $v \in \bar{F}^*$ is called *primitive for* E_n, if $\operatorname{ord}(v) = q^n - 1$, i.e., if v generates $U_{q^n-1} = E_n^*$, which is the multiplicative group of the unique n-dimensional extension E_n of F.

Let us now turn to polynomials associated to the multiplicative structure. For N as above, the roots of $x^N - 1$ in $\bar{F}$ are exactly the elements of U_N. The *Nth cyclotomic polynomial* Φ_N *over* F is defined as the product of all $x - \zeta$ where ζ runs over all $\varphi(N)$ primitive Nth roots of unity (in $\bar{F}$). Then Φ_N has in fact coefficients in the prime field of F. Since $x^N - 1$ is square-free, we obtain

$$x^N - 1 = \prod_{D|N} \Phi_D, \tag{3.3}$$

and a further application of Möbius inversion gives

$$\Phi_N = \prod_{D|N} (x^D - 1)^{\mu(N/D)}. \tag{3.4}$$

We will next turn to the additive group of $\bar{F}$ and shall see that the structure is quite similar to that of the multiplicative group. Most of the following material is taken from [Ha1] which is a recent monograph on the additive structure of finite fields with particular emphasis on normal bases and complete normal bases (see Section 7).

First of all, the Frobenius automorphism of $\bar{F}$ over F is the mapping σ defined by

$$\sigma : \bar{F} \to \bar{F},\ w \mapsto w^q. \tag{3.5}$$

The Frobenius automorphism fixes F elementwise and leaves every subfield of $\bar{F}/F$ invariant. The restriction of σ onto E_n (which is likewise denoted by σ) is a (canonical) generator of the Galois group of E_n/F, which is cyclic. For any polynomial $f \in F[x]$ and any field element $w \in \bar{F}$, we define another field element by

$$f \circ w := f(\sigma)(w), \tag{3.6}$$

i.e., by evaluating the polynomial f at the Frobenius automorphism and by applying the resulting F-endomorphism $f(\sigma)$ of $\bar{F}$ to w. With respect to the operation $\circ$, $(\bar{F}, +)$ turns into a module over the Euclidean domain $F[x]$. Any σ-invariant F-subspace of $\bar{F}$ is called an *F-module*. Let us therefore consider the triple $(\bar{F}, \mathcal{M}, \subseteq)$ where $\mathcal{M}$ denotes the collection of finite F-modules.

The structure of the members in $\mathcal{M}$ is summarized in Theorem 3.1. Here, μ_q denotes the Möbius function for the partially ordered set of monic polynomials in

$F[x]$ (i.e., $\mu_q(1) = 1$, $\mu_q(h) = 0$ if h is divisible by the square of an irreducible polynomial and $\mu_q(h) = (-1)^r$ if h is square-free and r is the number of distinct monic irreducibles which divide h) and ϕ_q denotes the corresponding Euler function.

We need further notation. For any monic $g \in F[x]$ which is not divisible by x we define the set M_g by

$$M_g := \{v \in \bar{F} | g \circ v = 0\}. \tag{3.7}$$

For every w of $\bar{F}$ the mapping

$$\alpha_w : F[x] \to \bar{F},\ f(x) \mapsto f \circ w \tag{3.8}$$

is a homorphism of rings. The unique monic $g \in F[x]$ such that the kernel of α_w is equal to $gF[x]$ is called the *(additive) q-order of w* (recall that q is the cardinality of F); it is denoted by $\mathrm{Ord}_q(w)$. The image of α_w is equal to $\langle w \rangle_{\bar{F},\mathcal{M}}$, i.e., the (finite) F-module of $\bar{F}$ which is generated by w.

Theorem 3.1 *If M is a finite F-module of $\bar{F}$, then there is a unique monic $g \in F[x]$ which is not divisible by x such that $M = M_g$. Conversely, every M_g is finite (and thus $\mathcal{M}$ consists of all sets of the form M_g).*

The cardinality of M_g is equal to $q^{\deg(g)}$ and one has $M_h \subseteq M_g$ if and only if h divides g. Moreover, M_g is cyclic (i.e., free on one generator as an F-module), and M_g is generated by w if and only if $g = \mathrm{Ord}_q(w)$. The number $\phi_q(g)$ of $v \in \bar{F}$ with $\mathrm{Ord}_q(v) = g$, i.e., the number of generators of M_g is equal to

$$\phi_q(g) = \sum_{h|g} \mu_q(\frac{g}{h}) q^{\deg(g)}, \tag{3.9}$$

where the sum runs over all monic F-divisors of g. □

Observing that $E_n = M_{x^n-1}$, the part of Theorem 3.1 concerning the cyclicity of the finite F-modules generalizes the famous *normal basis theorem*, which for finite fields was first proved by Hensel (1888).

Normal Basis Theorem. *For any extension E_n/F of Galois fields there exists an element $w \in E_n$ such that $\{w, \sigma(w), ..., \sigma^{n-1}(w)\}$ is an F-basis of E_n.* □

A basis of the latter kind is called a *normal basis of E_n/F*, while w is called *normal in E_n/F*. (Unfortunately the terminology is not consistent; sometimes w is also called a *free* element in E_n/F. We here shall use the term *normal*.) We conclude that the normal elements for E_n/F are exactly the elements in $\bar{F}$ whose q-order is equal to $x^n - 1$.

In [Ha2] we have introduced the (additive) q-analogues of the cyclotomic polynomials, which we are going to describe next. First, we have to recall from Ore [Or] the notion of a *linearized q-polynomial* (these objects are intimately related to the modules in $\mathcal{M}$). For a polynomial $h = h_n x^n + h_{n-1}x^{n-1} + ... + h_1 x + h_0$ the *associated (linearized) q-polynomial* is defined by

$$\alpha_q(h) := h_n x^{q^n} + h_{n-1}x^{q^{n-1}} + ... + h_1 x^q + h_0 x. \tag{3.10}$$

Now, if $g \in F[x]$ is monic and not divisible by x then define Ψ_g to be the product of all linear factors $x - w$ where $\mathrm{Ord}_q(w) = g$. Then Ψ_g in fact has coefficients in F. Since $g \circ v = 0$ if and only if v is a root of $\alpha_q(g)$ and as $\alpha_q(g)$ is square-free, we see that

$$\alpha_q(g) = \prod_{w \in M_g} (x - w) = \prod_{h|g} \Psi_h, \tag{3.11}$$

and Möbius inversion yields a formula for the Ψ_g in terms of linearized q-polynomials:

$$\Psi_g = \prod_{h|g} \alpha_q(h)^{\mu_q(g/h)}. \tag{3.12}$$

In Section 6 we shall return to cyclotomic polynomials and their q-analogues. For the time being we summarize that besides the degree, to any nonzero field element $w \in \bar{F}$ there are associated two fundamental parameters, the multiplicative and the (additive) q-order. It is a fundamental (and in general unsolved) problem to decide which pairs $(\mathrm{Ord}_q(v), \mathrm{ord}(v))$ of orders can occur.

Problem 3.2 *Given the field F with q elements, what are the possible pairs (f, N) ($f \in F[x]$ monic, not divisible by x, $N \geq 1$ an integer not divisible by the characteristic p of F) such that there exist elements $v \in \bar{F}$ satisfying $\mathrm{ord}(v) = N$ and $\mathrm{Ord}_q(v) = f$?* □

In the following two sections we shall discuss results which are related to that fundamental problem. To conclude the present section we remark that the degree of an element $v \in \bar{F}$ is determined by its multiplicative order as well as by its additive order (see [LeSc]). For an explanation we have to introduce yet another type of order, namely the order of units in certain residue rings. First, if k, l are nonzero relatively prime integers then the *order of k modulo l* is the least integer $\alpha \geq 1$ such that $k^\alpha \equiv 1 \bmod l$ (this number is denoted by $\mathrm{ord}_l(k)$). Similarly, if $f, g \in F[x]$ are relatively prime polynomials then the *order of f modulo g* is the least integer $\beta \geq 1$ such that $f^\beta \equiv 1 \bmod g$ (by abuse of notation this number is denoted by $\mathrm{ord}_g(f)$). Now, for $v \in \bar{F}$ the degree of v (say n) satisfies $n = \mathrm{ord}_N(q) = \mathrm{ord}_f(x)$ where $N = \mathrm{ord}(v)$ and where $f = \mathrm{Ord}_q(v)$.

4 Explicit construction of normal bases

In the last section we have introduced the mappings ϕ_q which are the additive analogues of Euler's totient φ. In the present section we discuss some properties of these functions and show how normal bases for arbitrary extensions over finite fields can be constructed explicitly. The present section is mainly based on [Ha1, Chapter II and Chapter VI].

Let again F be a finite field with q elements and characteristic p. For a monic $G \in F[x]$ which is relatively prime to x, we have defined $\phi_q(G)$ to be the number of generators of the F-module M_G (i.e., the number of v with $\mathrm{Ord}_q(v) = G$). Define

$$\Omega_q(G) := \{v \in \bar{F} \mid \mathrm{Ord}_q(v) = G\}. \tag{4.1}$$

If $\nu(G)$ is the square-free part of G (i.e., the product of all distinct monic irreducible divisors of G), then one has

$$\phi_q(G) = q^{\deg(G)-\deg(\nu(G))} \cdot \phi_q(\nu(G)). \tag{4.2}$$

The analogous condition of (4.2) for Euler's φ is

$$\varphi(N) = \frac{N}{\nu(N)} \cdot \varphi(\nu(N)).$$

A further important property of ϕ_q is its *multiplicativity*: if $G = \prod_i g_i$ is a decomposition of G into monic pairwise relatively prime polynomials, then

$$\phi_q(G) = \prod_i \phi_q(g_i). \tag{4.3}$$

The latter formula reflects the corresponding decompositions of M_G and Ω_G:

$$M_G = \bigoplus_i M_{g_i} \quad \text{and} \quad \Omega_q(G) = \bigoplus_i \Omega_q(g_i), \tag{4.4}$$

where the direct sum (as usual) indicates that the representation of an element as a sum is unique.

For a special case which is important for constructions of normal bases, formula (4.2) as well has an interesting algebraic interpretation (a proof will be given in [Ha5]): assume that $G = g^\pi$ where π is a power of the characteristic p, then

$$\Omega_q(G) = \alpha\Omega_q(g) \oplus M_{g^{\pi-1}} \ \text{ for any } \alpha \in \Omega_q(x^\pi - 1). \tag{4.5}$$

We now turn to the construction of normal bases for finite extensions over F. Let $n \geq 1$ be an integer which is not divisible by p and let π be a power of p. In $F[x]$ one has $x^{n\pi} - 1 = (x^n - 1)^\pi$, whence by (3.3) we have

$$x^{n\pi} - 1 = \prod_{d|n} \Phi_d^\pi. \tag{4.6}$$

Because of this (canonical) decomposition into cyclotomic polynomials, the determination of an element of $\Omega_q(x^{n\pi} - 1)$ is reduced to the determination of elements of $\Omega_q(\Phi_m^\pi)$, m a divisor of n. Moreover, by (4.5) it is sufficient to study sets of the type $\Omega_q(x^\pi - 1)$ and $\Omega_q(\Phi_m)$, where p does not divide m.

A classical result of Perlis [Pe] says that $w \in E_\pi$ is normal over F if and only if the (E_π, F)-trace of w is nonzero, and therefore an element $w \in \Omega_q(x^\pi - 1)$ can easily be obtained by Linear Algebra (see [Ha1, Section I.5]). We thus arrive at a core problem, namely the determination of generators for M_{Φ_m} (where $m \in \mathbb{N}$ is not divisible by p). In this context the notion of *regularity* as well as the determination of the q-orders of certain roots of unity is of fundamental interest.

Definition 4.1 For an integer N let N' denote the largest divisor of N which is not divisible by the characteristic p of F. The pair (q, N) is called *regular* if $\mathrm{ord}_{\nu(N')}(q)$ and N are relatively prime. In this case, the field extension E_N/F as well as all its F-submodules are called *regular.* □

Let us return to the situation above. In [Ha1, Chapter VI], there is an explicit description of elements from $\Omega_q(\Phi_m)$ when (q, m) is regular. In order to avoid the distinction of several cases, below we have restricted our attention to a certain class of regular pairs. For the general situation we refer to [Ha1].

Theorem 4.2 *Assume that (q, m) is regular and that $q \equiv 1$ mod 4 if m is even and q is odd. Let $s := \mathrm{ord}_{\nu(m)}(q)$ and let $\rho = \rho(m, q)$ denote the largest divisor of $q^s - 1$ such that $\nu(\rho) = \nu(m)$. If $\eta \in \bar{F}$ is a primitive $(m\rho)$th root of unity (i.e., if $\mathrm{ord}(\eta) = m\rho$), then $\mathrm{Ord}_q(\eta) = f(x^s)$ where f is some irreducible F-divisor of Φ_m.* □

Now, in the situation of Theorem 4.2 one has the following.

Theorem 4.3 *Let $a = \gcd(m, \rho)$. Then the group $\mathcal{U}_a$ of units modulo a acts on the set of primitive $(m\rho)$th roots of unity by exponentiation. Let Q be the subgroup of $\mathcal{U}_a$ generated by q modulo a, and let $\mathcal{R}$ be a complete set of coset representatives of Q in $\mathcal{U}_a$. Then $v := \sum_{i\in\mathcal{R}} \eta^i$ has q-order equal to $\Phi_m(x^s)$. Finally, under the regularity assumption for (q, m), the (E_{ms}, E_m)-trace of v has q-order equal to Φ_m, i.e.,*

$$\sum_{j=0}^{s-1} \Big(\sum_{i\in\mathcal{R}} \eta^i\Big)^{q^{mj}} = \sum_{i\in\mathcal{R}} \sum_{j=0}^{s-1} \eta^{iq^{mj}} \in \Omega_q(\Phi_m). \quad \Box \tag{4.7}$$

In order to complete the construction of normal bases for arbitrary extensions of finite fields (including those with non-regular parameters), it is important to know that the class of regular pairs is quite large, e.g., (q, m) is always regular when $m = r^k$ is a power of a prime r (for further examples see Section 9). One can therefore cover all values of m with the help of the following *product construction* (see [Ha1, Section 25]):

$$\Omega_q(\Phi_k) \cdot \Omega_q(\Phi_l) \subseteq \Omega_q(\Phi_{kl}) \quad \text{if } k \text{ and } l \text{ are relatively prime.} \tag{4.8}$$

The inclusion in (4.8), however, is always proper, whence in contrast to (4.4) and (4.5) there is a loss of information in (4.8).

We conclude this section with an example.

Example 4.4 Let $F = \mathrm{GF}(2)$ be the Galois field with 2 elements. We will determine a normal element for E_{84}/F. Since $x^{84} - 1 = (x^{21} - 1)^4$ over F, we first consider the set $\Omega_2(x^{21} - 1)$ which is equal to $\Omega_2(x - 1) \oplus \Omega_2(\Phi_3) \oplus \Omega_2(\Phi_7) \oplus \Omega_2(\Phi_{21})$ (by (4.4)). Let α be any nonzero element of F, then $\mathrm{Ord}_2(\alpha) = x - 1$. If η is a primitive 9th root of unity then (according to Theorem 4.1) $\mathrm{Ord}_2(\eta) = \Phi_3(x^2)$, and by Theorem 4.2, $\beta := \eta + \eta^8 \in \Omega_2(\Phi_3)$. Next, let ζ be a primitive 49th root of unity. Yet an application of Theorem 4.2 and Theorem 4.3 shows that $\gamma := (\zeta + \zeta^3) + (\zeta + \zeta^3)^{2^7} + (\zeta + \zeta^3)^{2^{14}} = \zeta + \zeta^3 + \zeta^5 + \zeta^{41} + \zeta^{18} + \zeta^{30}$ is an element of $\Omega_2(\Phi_7)$. Since the pair $(2, 21)$ is not regular, we use (4.8) to obtain that $\delta := \beta\gamma \in \Omega_2(\Phi_{21})$. Finally, if ρ is a 5th root of unity, then ρ is normal in E_4/F and with (4.5) we therefore conclude that $\rho(\alpha + \beta + \gamma + \beta\gamma)$ is normal in E_{84}/F. □

We finally give the well-known formula for the number of normal elments of E_n/F. Let $n = m\pi$ as above. For each divisor d of m, Φ_d over F splits into $\varphi(d)/\mathrm{ord}_d(q)$ irreducible polynomials of degree $\mathrm{ord}_d(q)$, each. Observing that $\Omega_q(h) = M_h \backslash \{0\}$ (and thus $\phi_q(h) = q^{\deg(h)} - 1$) if $h \in F[x]$ is monic and irreducible, from (4.2), (4.3) and (4.6) we thus obtain

$$\phi_q(x^{m\pi} - 1) = q^{(\pi-1)m} \cdot \prod_{d|m} (q^{\mathrm{ord}_d(q)} - 1)^{\varphi(d)/\mathrm{ord}_d(q)}. \tag{4.9}$$

In [Or] the q-polynomials have been used to determine the number of normal bases for E_n over F (i.e., the degree of Ψ_{x^n-1}) (see also [LiNi]). The exact number of normal bases was also determined in Hensel's classical paper [He].

5 Primitive normal bases

In Section 3 we have seen that the multiplicative and the additive structure of finite fields are quite similar. Primitive and normal elements are important because they yield representations for the multiplicative and the additive structure, respectively. In particular the arithmetic based on normal bases is important for applications in cryptography (we refer to Jungnickel [Ju] for an extensive treatment of the arithmetic of finite fields). ¿From an algorithmic point of view there is a fundamental difference between primitive and normal elements: suppose that E_n is given over F in terms of an irreducible polynomial, then there are several deterministic polyomial time algorithms known (in n and $\log(q)$) which determine a normal element for E_n/F (we here only mention the work of Poli [Po] whose algorithm seems to have the best known complexity); it is not known however whether there exists a deterministic polynomial time algorithm which produces a primitive element for E_n; in fact, all known *tests* for primitivity require the factorization of $q^n - 1$, which itself is a difficult problem.

Given a Galois field F (again with q elements) and the extension E_n (in $\bar{F}$), it is natural to ask, whether there exists a primitive w in E_n which is *simultaneously* normal over F, i.e.,

$$(\mathrm{Ord}_q(w), \mathrm{ord}(w)) = (x^n - 1, q^n - 1).$$

Completing previous work of Carlitz [Ca] and Davenport [Da], the final answer has only been achieved in 1987, when Lenstra and Schoof [LeSc] proved the *primitive normal basis theorem.*

Primitive Normal Basis Theorem. *For any extension E_n/F of finite fields there exists a primitive $w \in E_n$ which is normal over F.* □

In the present section we shall report on recent progress concerning the existence of primitive normal elements with additional properties. A monic irreducible

$$\iota = x^n + \iota_{n-1}x^{n-1} + ... + \iota_1 x + \iota_0 \in F[x]$$

is called primitive (resp. normal) if all its roots are primitive (resp. normal) (if w is a root of ι then $\sigma^i(w) = w^{q^i}$ where $0 \leq i \leq n-1$ are all the roots of ι; in particular all roots have the same additive order and the same multiplicative order). Since there are known no efficient methods which determine primitive normal polynomials (equivalently which determine primitive normal elements), one may ask whether certain coefficients of such a polynomial can be prescribed. Motivated by a conjecture of Morgan and Mullen [MoMu1], the existence of primitive normal elements with prescribed trace or/and prescribed norm was recently studied by Cohen and the author [CoHa1, CoHa2, Co2]. If $w \in E_n$ is a root of ι, then observe that

$$-\iota_{n-1} = T(w) := \sum_{i=0}^{n-1} w^{q^i} \quad \text{and} \quad (-1)^n \iota_0 = N(w) := \prod_{i=0}^{n-1} w^{q^i}, \tag{5.1}$$

where $T(w)$ denotes the (E_n, F)-trace of w and $N(w)$ the (E_n, F)-norm of w. The main results of [CoHa1, CoHa2, Co2] are summarized in the following (the letter **F** refers to *free*, which in [CoHa2] is used instead of *normal*).

Theorem PFT ([CoHa1], conjectured in [MoMu1]): *If E_n/F is an extension of Galois fields with $n \geq 2$ and if $a \in F$ is any nonzero element, then there exists a primitive $w_a \in E_n$ which is normal over F and satisfies $T(w_a) = a$. (The assumption on a is necessary as the trace of a normal element is always nonzero.)* □

Theorem PFN ([CoHa2]): *If E_n/F is an extension of Galois fields with $n \geq 2$ and if $b \in F$ is any primitive element, then there exists a primitive $w_b \in E_n$ which is* *normal over F and satisfies $N(w_b) = b$. (The assumption on b is necessary as the norm of a primitive element is always primitive.)* □

Theorem PFNT ([CoHa2, Co2]): *Let E_n/F be an extension of Galois fields with $n \geq 5$. Assume that $a \in F$ is nonzero and $b \in F$ is primitive. Then there exists a primitive $w_{a,b} \in E_n$ which is normal over F and satisfies the two conditions $T(w) = a$ and $N(w) = b$.* □

The existence of primitive elements with prescribed trace (not necessarily nonzero) was settled by Cohen [Co1] (see also Jungnickel and Vanstone [JuVa]). The existence of normal elements with prescribed norm (not necessarily primitive) is settled in [CoHa2]. For the precise statements we refer to the original papers. Concerning the degree $n = 3$ and $n = 4$ for which "problem **PFNT**" is still meaningful, we offer the following conjecture.

Conjecture 5.1 *Let F be a finite field, $a \in F$ nonzero and $b \in F$ primitive. Then there exist elements $\alpha, \beta, \gamma \in F$ such that the polynomials*

$$x^3 - ax^2 + \alpha x - b \text{ and } x^4 - ax^3 + \beta x^2 + \gamma x + b$$

are primitive and normal. □

The key method which is used to attack problems of the above kind is to derive formulae involving Gauss sums of the characteristic functions of the set of elements satisfying all properties one is interesting in. We shall demonstrate this by considering the generalization of the "**PFNT**-problem" studied in [Ha3].

Definition 5.2 If q and n are as above, then, for divisors $k, l \geq 1$ of n, the quadruple (q, k, l, n) is called *universal* if for every primitive $b \in E_l$ and every normal a in E_k/F there exists a primitive $w_{a,b}$ in E_n which is normal over F with (E_n, E_k)-trace equal to a and (E_n, E_l)-norm equal to b (again the assumptions on a and b are necessary). □

Problem 5.3 *Which quadruples (q, k, l, n) are universal?* □

In [Ha3], the motivation for studying this generalized version of the "**PFNT**-problem" is to prove an infinite version of the primitive normal basis theorem for primary closures of finite fields. In this context the following is true.

Theorem 5.4 *$(q, r^\alpha, r^\beta, r^\gamma)$ is universal for all prime powers $q > 1$, all primes $r \geq 7$, all $\alpha, \beta \geq 0$ and all $\gamma >$ max$\{\alpha, \beta\}$.* □

In the rest of this section we follow [Ha3] and demonstrate how to derive a sufficient criterion for a quadruple to be universal. Throughout, the (E_n, E_k)-trace is denoted by $T_{n,k}$ and the (E_n, E_l)-norm is denoted by $N_{n,l}$.

Consider first the multiplicative part. If D is a divisor of $q^n - 1$, then M_D in (5.2) is the characteristic function of all elements of E^* whose multiplicative order is divisible by $\bar{D}$, where $\bar{D}$ is defined to be the largest divisor of $q^n - 1$ whose square-free part is that of D (see [Ca, Da, LeSc, CoHa1]).

$$M_D(w) := \frac{\varphi(D)}{D} \sum_{d|D} \frac{\mu(d)}{\varphi(d)} \sum_{(\eta,d)} \eta(w), \qquad w \in E^*, \tag{5.2}$$

here the second sum runs over all $\varphi(d)$ multiplicative characters η of the character group $\hat{E^*}$ of E^* (isomorphic to E^*) whose order is equal to d.

For a divisor l of n, the characteristic function of the set of $w \in E_n^*$ having (E_n, E_l)-norm $b \in E_l^*$ is given by

$$N_b(w) := \frac{1}{q^l - 1} \sum_{\nu \in \hat{E}_l^*} \nu(N_{n,l}(w)b^{-1}), \qquad w \in E^*, \tag{5.3}$$

where the sum runs over all multiplicative characters of E_l.

We next investigate normality and prescribed trace. For a divisor k of n let $\hat{E_k}$ be the group of additive characters of E_k. The characteristic function T_a of all $w \in E_n$ with (E_n, E_k)-trace equal to a is as follows:

$$T_a(w) := \frac{1}{q^k} \sum_{\lambda \in \hat{E_k}} \lambda(T_{n,k}(w) - a), \qquad w \in E. \tag{5.4}$$

In order to cope with normality, we have to remark that, similar to the multiplicative case, the group $\hat{E_n}$ of additive characters is isomorphic to $(E_n, +)$ as $F[x]$-module as defined in Section 3 (see also [LeSc], [CoHa1], [Ha4]). For a monic divisor G of $x^n - 1$ let

$$A_G(w) := \frac{\phi_q(G)}{q^{\deg(G)}} \sum_{g|G} \frac{\mu_q(g)}{\phi_q(g)} \sum_{(\chi,g)} \chi(w), \tag{5.5}$$

where the first sum runs over all monic F-divisors of G and the symbol (χ, g) indicates that the second sum runs over all additive characters of E_n having q-order equal to G. Then A_G is the characteristic function of the set of $w \in E_n$ whose q-order is divisible by $\bar{G}$ where $\bar{G}$ is the largest monic divisor of $x^n - 1$ whose square-free part is equal to that of G.

The following result is taken from [Ha3].

Theorem 5.5 *Given a quadruple (q, k, l, n) as above, let P be the largest divisor of $q^n - 1$ which is relatively prime to $q^l - 1$ and let $t \in F[x]$ be the largest monic* *divisor of $x^n - 1$ which is relatively prime to $x^k - 1$. Then, with $a \in E_k$ being normal over F and $b \in E_l$ being primitive,*

$$\sum_{w \in E^*} M_P(w) A_t(w) N_b(w) T_a(w) \tag{5.6}$$

is the total number of elements in E_n which are primitive and normal over F with (E_n, E_k)-trace equal to a and (E_n, E_l)-trace equal to b.

Moreover, (q, k, l, n) is universal provided that

$$\frac{q^{n/2}}{q^k(q^l - 1)} > (2^\Omega - \frac{1}{q^k})(2^\omega - \frac{1}{q^l - 1}), \tag{5.7}$$

where ω denotes the number of distinct prime divisors of P and Ω denotes the number of distinct monic irreducible F-divisors of t. □

The criterion (5.7) is derived through analysis of absolute values of Gauss sums occuring in the term (5.6) (for a multiplicative character η and an additive character χ of E_n, the (complex valued) Gauss sum $G(\eta, \chi)$ is defined by $G(\eta, \chi) := \sum_{w \in E_n^*} \eta(w)\chi(w)$, see [LiNi, Chapter 5, Section 2]). We shall here demonstrate how (5.7) can be used to prove the following asymptotic result (see [Ha4] for a similar reasoning).

Theorem 5.6 *There are at most finitely many quadruples (q, k, l, n) with $n \geq 5$, $q \geq 257$ and $k, l \leq n/5$ which are not universal.*

Proof. For an integer $z \geq 1$ let $d(z)$ denote the number of positive divisors of z. Then $2^\omega \leq d(P) \leq d(q^n - 1)$. By [HaWr, Section 18.1, Satz 315], for any $\varepsilon > 0$ there exists a constant $c_\varepsilon > 0$ such that $2^\omega \leq c_\varepsilon q^{n\varepsilon}$. On the other hand $n - k$ is an upper bound of Ω. Thus, using (5.7), for (q, k, l, n) to be universal it is sufficient to have $2^{n-k} c_\varepsilon q^{n\varepsilon} < q^{n/2-k-l}$. Thus, with $\max\{k, l\} \leq n/5$, an easy calculation shows that for (q, k, l, n) to be universal, the condition $2^{4n/5} c_\varepsilon q^{-(1/10-\varepsilon)n} < 1$ is sufficient. Now, let $\varepsilon < 1/10$ and $\delta := 1/8 - 5\varepsilon/4$. Then $\delta > 0$ and (q, k, l, n) is universal provided that

$$c_\varepsilon (\frac{2}{q^\delta})^{4n/5} < 1. \tag{5.8}$$

The latter holds, for all $n \geq 5$, whenever q is large enough, say $q \geq q_\varepsilon$, where q_ε is a constant depending only on ε. Observe next that $\delta < 1/8$, whence for $q \geq 257 > 2^8$ one has $2/q^\delta < 1$ and therefore (5.8) is also satisfied whenever n is large enough. We conclude that for any q from the interval $[257, q_\varepsilon]$ there are only finitely many n such that (q, k, l, n) is not universal for divisors k, l of n which are less than $n/5$. This completes the proof of the theorem. □

We remark that the range of possible exceptions to universality can be made more precise when using more concrete upper bounds for ω (see the proof of the present

Theorem 4.4 given in [Ha3]). When $n \geq 7$ and $k = l = 1$ then (5.7) turns out to be a good criterion (see [CoHa2]). In order to solve the "**PFNT**-problem" for $n = 6$ and $n = 5$ (i.e., the universality of $(q, 1, 1, 5)$ and $(q, 1, 1, 6)$ for all q) Cohen [Cp2] has developed an efficient sieving technique as well as an improvement of (5.7) (for $k = l = 1$).

We also remark that it is not difficult to show (see [Ha3]) that the universality of (q, k, l, n) implies that of (q, k', l', n) if k' divides k and l' divides l. It is therefore important to know the universality for divisors of n as large as possible.

6 Cyclotomic polynomials and their additive q-analogues

In the present section we are once more concerned with the cyclotomic polynomials and their (additive) q-analogues Ψ_g which were introduced in Section 3. It is here our aim to present properties of these polynomials which are useful for their computation (see [Ha1, Section 10] for the cyclotomic polynomials). We use the same notation as in Section 3 and start with the cyclotomic polynomials.

1. If D is a divisor of N such that $\nu(N)$ divides D then $\Phi_N = \Phi_D(x^{N/D})$; in particular $\Phi_N = \Phi_{\nu(N)}(x^{N/\nu(N)})$;
2. if N and T are relatively prime and p does not divide T then $\Phi_N(x^T) = \prod_{D|T} \Phi_{ND}$;
3. if π is a power of p then $\Phi_N(x^\pi) = \Phi_N^\pi$.

Next, consider Ψ_g and recall that $\alpha_q(g)$ is the associated q-polynomial of g. In order to describe the analogous properties of the polynomials Ψ_g, we denote the compositions of polynomials by $*$ (e.g., see above, we have $\Phi_{ND} = \Phi_N * x^D$ when D and N have the same prime divisors).

1. If h is a divisor of g such that $\nu(g)$ divides h then $\Psi_g = \Psi_h * \alpha_q(g/h)$, in particular $\Psi_g = \Psi_{\nu(g)} * \alpha_q(g/\nu(g))$;
2. if g and h are relatively prime then $\Psi_g * \alpha_q(h) = \prod_{d|h} \Psi_{gd}$.

Observe that the first formula reflects (4.2) while there is a connection between the second formula and (4.3) (we do not go into further detail, here).

7 Cyclotomic modules and completeness

So far we have always studied $(\bar{F}, +)$ as a module with respect to the fixed ground field F (see (3.6)). In the present section we introduce a dynamical component by allowing a variation of the ground field. We shall be concerned with the *complete module structure* of $\bar{F}$, a theory which has been developed in [Ha1] and [Ha6].

Observe first that if E_k is any finite extension of F then $(\bar{F}, +)$ also carries the structure as an E_k-module with respect to the Frobenius automorphism σ^k over E_k, i.e., the scalar multiplication is given by

$$h \circ_k w := h(\sigma^k)(w), \;\; w \in \bar{F},\, h \in E_k[x]. \tag{7.1}$$

Now, analogously to Section 3, the *q^k-order of $w \in \bar{F}$* is defined to be the monic polynomial h of least degree in $E_k[x]$ such that $h \circ_k w = 0$.

Let us consider a finite F-module M_g ($g \in F[x]$ indivisible by x). There is a largest integer $\kappa = \kappa(g)$ such that g has the form $g = h(x^\kappa)$ for some monic $h \in F[x]$.

Definition 7.1 The parameter κ is called the *module character of M_g*. □

The latter definition is motivated by the following fact.

Proposition 7.2 *M_g is an E_d-module (i.e., a σ^d-invariant E_d-subspace of $\bar{F}$) if and only if d is a divisor of $\kappa(g)$.* □

Now, from Theorem 3.1, applied to any divisor d of κ, we know that M_g is a cyclic E_d-module (the generators of M_g as an E_d-module are exactly the elements of $\Omega_{q^d}(h(x^{\kappa/d}))$, i.e., those elements having q^d-order equal to $h(x^{\kappa/d})$). The following result says much more, namely that M_g is in fact *completely cyclic.*

Theorem 7.3 *Let M_g be a finite F-module of $\bar{F}$. Then there exists an element $v \in M_g$ such that v simultaneously generates M_g as E_d-module for all d dividing $\kappa(g)$. Such an element v is called a* complete generator for *M_g.* □

As in Section 3 it is important to emphasize the special case where $g = x^n - 1$ (where $n \geq 1$ is some integer). Recall that $E_n = M_{x^n-1}$. The module character of the latter is equal to n, and one therefore recovers the *complete normal basis theorem* which is due to Blessenohl and Johnsen [BlJo].

Complete Normal Basis Theorem. *For every extension E_n/F of finite fields there exists an element $w \in E_n$ such that w simultaneously is normal for E_n/E_d for all divisors d of n, i.e, for all intermediate fields of E_n/F.* □

An element of the latter kind is called *completely normal in E_n/F* (again the terminology is not consistent since sometimes the term *completely free* is used).

According to Section 5 we next define $\Omega_q^c(g)$ to be the set of all complete generators of M_g and let $\phi_q^c(g)$ denote the cardinality of that set. We shall discuss some properties of these sets and therefore restrict our attention to the class of *cyclotomic modules* (introduced in [Ha1, Ha6]) for which the properties of the cyclotomic polynomials given in Section 6 are important.

Definition 7.4 M_g is called a *cyclotomic module* if g is of the form $\Phi_k(x^t)$ where $k, t \geq 1$ are integers such that p does not divide k and (without loss of generality) k and t are relatively prime. □

Since $x^n - 1 = \Phi_1(x^n)$, each finite extension E_n of F is a cyclotomic module. Moreover, the module character corresponding to $\Phi_k(x^t)$ is equal to $kt/\nu(k)$.

The most important structural result for complete generators of cyclotomic modules is the following Complete Decomposition Theorem ([Ha1, Ha6]), which can be seen as a complete version of (5.4).

Complete Decomposition Theorem (CDT). *Consider a finite field F and the cyclotomic module corresponding to the polynomial $g = \Phi_k(x^t)$. Let t' be the largest divisor of t which is relatively prime to the characteristic p of F. Assume that r is a prime divisor of t' and denote by R the largest power of r dividing t. Then the following four assertions hold for the polynomials δ and ε defined by*

$$\delta := \Phi_k(x^{t/r}) \text{ and } \varepsilon := \Phi_{kR}(x^{t/R}). \tag{7.2}$$

- *$g = \delta \cdot \varepsilon$ and δ and ε are relatively prime,*
- *$M_g = M_\delta \oplus M_\varepsilon$,*
- *$\kappa(\delta) = \frac{\kappa(g)}{r} = \kappa(\varepsilon)$,*
- *$\Omega_q^c(g) \subseteq \Omega_q^c(\delta) \oplus \Omega_q^c(\varepsilon)$.*

Moreover, the following two assertions are equivalent

1. *$\Omega_q^c(g) = \Omega_q^c(\delta) \oplus \Omega_q^c(\varepsilon)$ (and therefore $\phi_q^c(g) = \phi_q^c(\delta) \cdot \phi_q^c(\varepsilon)$),*
2. *the order of q modulo $\nu(kt')$ is not divisible by R.* □

One of the main features of the Complete Decomposition Theorem (CDT) is that it can be applied iteratively yielding a product formula for $\phi_q^c(\Phi_k(x^t))$. We demonstrate this in an example.

Example 7.5 Let $n = 84$ and $F = \mathrm{GF}(q)$ where the characteristic p of F is different from 2, 3 and 7 (which are the prime divisors of 84). CDT can always be applied to $x^n - 1$ by choosing the largest prime divisor r of n which is different from p. Thus, taking $r = 7$, we obtain

$$\Omega_q^c(x^{84} - 1) = \Omega_q^c(x^{12} - 1) \oplus \Omega_q^c(\Phi_7(x^{12})).$$

For the subsequent applications we remark that 42 is the square-free part of 84 and that $\mathrm{ord}_{42}(q)$ is a divisor of 6, whence $\mathrm{ord}_{\nu(d)}(q)$ is not divisible by 7 or 4 for every divisor d of 84. Taking $r = 2$ applied to both summands above yields

$$\Omega_q^c(x^{84} - 1) = \Omega_q^c(x^6 - 1) \oplus \Omega_q^c(\Phi_4(x^3)) \oplus \Omega_q^c(\Phi_7(x^6)) \oplus \Omega_q^c(\Phi_{28}(x^3)).$$

Next, CDT can be applied to decompose $x^6 - 1$ into $x^2 - 1$ and $\Phi_3(x^2)$ $(r = 3)$, $x^2 - 1$ into $x - 1 = \Phi_1$ and Φ_2 $(r = 2)$, and $\Phi_4(x^3)$ into Φ_4 and Φ_{12} $(r = 3)$. Altogether we have a decomposition of $\Omega_q^c(x^{84} - 1)$ which is described by the following set of polynomials:

$$\{\Phi_1, \Phi_2, \Phi_3(x^2), \Phi_4, \Phi_{12}, \Phi_7(x^6), \Phi_{28}(x^3)\}.$$

In general, CDT cannot be applied to $\Phi_3(x^2)$, $\Phi_7(x^6)$ and $\Phi_{28}(x^3)$ but a specification of q can lead to further decompositions. For a general q we can summarize that $\phi_q^c(x^{84} - 1)$ is equal to

$$(q-1)^2 \cdot \phi_q^c(\Phi_3(x^2)) \cdot \phi_q^c(\Phi_4) \cdot \phi_q^c(\Phi_{12}) \cdot \phi_q^c(\Phi_7(x^6)) \cdot \phi_q^c(\Phi_{28}(x^3)). \ \square$$

In [Ha6] we have proved that a decomposition of a cyclotomic module as obtained in Example 7.5 is uniquely determined no matter in which order the primes r are chosen.

A further important feature of the CDT is that the module character of the summands corresponding to δ and ε is a proper divisor of the module character of the entire module (corresponding to g), i.e., with every decomposition the module character *decreases.* In the above example the highest module character in the achieved decomposition is equal to 6, while we have started with $\kappa(x^{84} - 1) = 84$. The phenomenon of decreasing the module character is important for constructions of completely normal elements, which is done in [Ha1, Chapter VI]. In this context we remark that the notion of regularity (see Section 4) also plays an important rôle for cyclotomic modules under the complete point of view and that a complete version of (4.8) is available (see also Section 8). It follows also from results in [Ha1] that a complete generator of any cyclotomic module can be constructed deterministically in polynomial time.

8 On the enumeration of complete normal bases

Via computer search, Morgan and Mullen [MoMu2] have determined the exact number of completely normal elements for the 56 pairs (q, n) where $q = 2, 3, 4, 5, 7, 8, 9$ and $n \leq 18, 12, 9, 8, 6, 5, 5$, respectively, and they have posed the problem to find formulae for the number of completely normal elements. We shall discuss this in the present section.

First of all, as outlined in Section 7, the CDT gives a product formula for the number of complete generators of cyclotomic modules (in particular completely normal elements, see Example 7.5). According to Definition 5.1, we define the cyclotomic module described by $\Phi_k(x^t)$ to be *regular* if (q, kt) is regular, i.e., if $\mathrm{ord}_{\nu(kt')}(q)$ is relatively prime to kt. In [Ha1, Chapter VI] we have applied the decomposition theory for studying regular cyclotomic modules and we were able to determine the exact value for $\phi_q^c(\Phi_k(x^t))$ in that case. Instead of reproducing the complicated formula, we offer the following conjecture which is valid for regular cyclotomic modules.

Conjecture 8.1 *Assume that p does not divide kt' and let π be a power of p. Then*

$$\phi_q^c(\Phi_k(x^{t'\pi})) \geq (q-1)^{\varphi(k)t'} \cdot q^{\varphi(k)t'(\pi-1)}. \tag{8.1}$$

Morever, equality holds if and only if $q-1$ is divisible by kt'. □

For general cyclotomic modules we have used a *complete version* of the product construction (4.8) in order to derive lower bounds for the number of complete generators (see [Ha1, Section 25]). However, in general, these bounds are rather weak compared to the bound in (8.1).

For the rest of this section we shall have a look at the smallest non-regular problem instance, as this already indicates the difficulty of the general problem of finding the number of completely normal elements.

We consider the extension E_{rs}/F where $F = \mathrm{GF}(q)$ with characteristic p and where r and s are primes different from p. If $r = s$ (a regular case) then by [Ha1, Section 15], every normal element of E_{r^2}/F is already completely normal. Let us therefore assume that $r < s$. An application of the Complete Decompositon Theorem gives

$$\phi_q^c(x^{rs}-1) = \phi_q(x-1) \cdot \phi_q(\Phi_r) \cdot \phi_q^c(\Phi_s(x^r)).$$

If r does not divide the order of q modulo s (a regular case), then

$$\phi_q^c(\Phi_s(x^r)) = \phi_q(\Phi_s) \cdot \phi_q(\Phi_{sr})$$

and therefore, again, every normal element of E_{sr}/F is completely normal.

Let us thus look at the non-regular case where r divides $\mathrm{ord}_s(q)$.

First, letting $f_1, ..., f_d$ be the irreducible F-divisors of Φ_s (where $d = (s-1)/\mathrm{ord}_s(q)$), we have (see [Ha1, Section 12])

$$\Omega_q^c(\Phi_s(x^r)) = \bigoplus_{i=1}^{d} \Omega_q^c(f_i(x^r)),$$

and we need to consider $\phi_q^c(f(x^s))$, where f is one of the f_i. Let $Q = q^r$. An element v is a complete generator of $M_{f(x^r)}$ over F if and only if $\mathrm{Ord}_q(v) = f(x^r)$ and $\mathrm{Ord}_Q(v) = f$. In the following, g denotes a monic F-divisor of $f(x^r)$ and h

denotes a monic E_r-divisor of f. For such an h let V_h be the kernel of $h(\sigma^r)$, in particular, $M_{f(x^r)} = V_f$.

One can show (see [Ha1, Section 14]) that for every pair (g, h), $M_g \cap V_h$ carries the structure of an E_l-vector space, where $l = \mathrm{ord}_s(q)$ is the degree of f (this is due to the fact that M_g and V_h are $F[x]$-modules with respect to the F-endomorphism σ^r). Now, for every pair (g, h) let $\epsilon(g, h)$ be the E_l-dimension of $M_g \cap V_h$. Then knowledge of the function ϵ enables one (via the inclusion-exclusion principle) to determine $\phi_q^c(f(x^r))$. In this context we offer the following problem.

Problem 8.2 *Define the function m by*

$$m(g,h) := max\ \{0, dim_{E_l}(M_g) + dim_{E_l}(V_h) - r\}. \tag{8.2}$$

Is it true (independent from the choice of f) that $\epsilon = m$? □

Up to now we were able to show that $m = \epsilon$ for $r = 2$, $r = 3$ or $r = 5$, only. But we are thereby able to determine formulae for the number of completely normal elements for most of the pairs (q, n) where $n \leq 100$ and where q is any prime power which is relatively prime to n. (This and the rest of this section will have to be worked out in [Ha7].) We shall give an example.

Example 8.3 Let $s = 7$, $r = 3$ and assume that q modulo 7 is equal to 2,3,4 or 5, whence $\mathrm{ord}_7(q)$ is divisible by 3.

If $q \equiv 2$ modulo 3 then

$$\phi_q^c(\Phi_7(x^3)) = (q^9 - 4q^6 + 5q^3 - 2)^2,$$

and therefore

$$\phi_q^c(x^{21} - 1) = (q - 1) \cdot (q^2 - 1) \cdot (q^9 - 4q^6 + 5q^3 - 2)^2.$$

If $q \equiv 1$ modulo 3 then

$$\phi_q^c(\Phi_7(x^3)) = (q^9 - 6q^6 + 15q^3 - 10)^2,$$

and

$$\phi_q^c(x^{21} - 1) = (q - 1)^3 \cdot (q^9 - 6q^6 + 15q^3 - 10)^2.$$

In both cases, Conjecture 8.1 is true. In the special case where $q = 2$ we obtain $\phi_2^c(x^{21} - 1) = 259308$ (see [Ha1, Section 14]). The total number of normal elements for $E_{21}/\mathrm{GF}(2)$ is 583443. □

The general problem seems to be very difficult, but we shall finally discuss an interesting connection to *MDS-codes.*

MDS-codes are important objects studied in Coding Theory (see [MWSl]) which are related to some fundamental objects in Finite Geometries as well (see

[HiTh]). MDS-codes are optimal in the sense that among all codes with the same length and the same minimum distance, they have the maximum number of codewords and therefore carry the highest information rate.

Let us return to the situation above. If h_j is an irreducible E_r-divisor of f, then V_{h_j} is a one-dimensional E_l-space. Hence, choosing a nonzero element of each of the E_r-submodules V_{h_j} (running over all irreducible E_r-divisors of f) we obtain an E_l-basis of $M_{f(x^r)}$. Let $M_{f(x^r)}$ be coordinatized with such a basis. Next, let g be a fixed monic F-divisor of $f(x^r)$. Then the fact that $\dim_{E_l}(M_g \cap V_h) = m(g,h)$ for all h (see Problem 8.2) is equivalent to the fact that M_g is an MDS-code with respect to the chosen coordinate system of $M_{f(x^r)}$. In other words, the minimum weight of M_g considered as block code of length r over E_l is equal to $r - \dim_{E_l}(M_g) + 1$.

We close this section with the following (down-to-earth) problem (compare with Example 7.5).

Problem 8.4 *Let q be a prime power such that $\mathrm{ord}_7(q) = 6$. Determine the number of complete generators for the cyclotomic modules corresponding to $\Phi_7(x^6)$ and $\Phi_{28}(x^3)$.* □

9 On primitive complete normal bases

In this final setion we turn to a further important problem in finite field theory.

Problem 9.1 *Let $F = \mathrm{GF}(q)$ and consider an extension E_n/F. Does there exist a primitive element in E_n which additionally is completely normal over F?* □

It is conjectured in Morgan and Mullen [MoMu2] (and widely believed) that such elements in fact do always exist (i.e., for all prime powers $q \geq 2$ and all $n \geq 1$). By means of a computer search, Morgan and Mullen have supported this conjecture by calculating for every pair (q,n), with $q \leq 97$ a prime and $q^n < 10^{50}$, a monic irreducible polynomial of degree n over $\mathrm{GF}(q)$ whose roots are primitive and completely normal for $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$. Besides an extensive table with 1061 polynomials they have also determined the exact number of primitive and completely normal elements for the 56 pairs (q,n), where $q = 2,3,4,5,7,8,9$ and $n \leq 18,12,9,8,6,5,5$, respectively.

In [Ha8] we were able to solve Problem 9.1 by proving a *primitive complete normal basis theorem* for a large class of extensions. The precise result is as follows.

Theorem 9.2 *Let E_n be the field extension of degree n over a finite field $F = \mathrm{GF}(q)$. Assume that (q,n) is regular (see Definition 4.1). Assume further that $q-1$ is divisible by 4 if q is odd and n is even. Then there exists a primitive element $w \in E_n$ which is completely normal over F.* □

For the proof of that result we have combined character sum methods (as in Section 5) together with the decomposition theory of cyclotomic modules (as outlined in Section 7). We shall finally give examples which demonstrate that the class of regular extensions is in fact quite large.

Example 9.3 A *Carmichael number* is an odd composite $N \in \mathbb{N}$ such that $r-1$ divides $N-1$ for every prime divisor r of N (see [Ko, page 128], there exist infinitely many Carmichael numbers). E.g., 561, 1105, 1729 and 2465 are Carmichael numbers. Now, if N is a Carmichael number, then (N^s, q) is regular for each prime power $q > 1$ and each integer $s \geq 1$, and Theorem 9.2 applies to this situation. □

Example 9.4 Let $q \geq 2$ be any prime power. We determine a set L of primes as follows: we start with $L = \{s\}$ where s is an odd prime and consider all primes r with $s+1 \leq r \leq B$ in increasing order; if s is not a divisor of $r-1$ for every s in the current set L, then r is added to L. Now, if n is any number all of whose prime divisors are from L (no matter in which multiplicity the primes occur in n), then (q, n) is regular and Theorem 9.2 applies to this situation. When taking $s = 7$ and $B = 1000$, we obtain the following list with 70 primes (the total number of primes r with $7 \leq r \leq 1000$ is equal to 165):

{ 7, 11, 13, 17, 19, 31, 41, 47, 49, 61, 73, 97, 101, 107, 109, 139, 151, 163, 167, 173, 179, 181, 193, 227, 233, 241, 251, 263, 269, 271, 277, 317, 349, 383, 401, 431, 433, 461, 479, 487, 499, 509, 523, 541, 563, 569, 577, 587, 601,
619, 641, 691, 719, 751, 769, 787, 797, 811, 823, 829, 839, 853, 887, 929,
983, 997 }.

For $s = 7$ and $B = 100000$ we obtain a list with 3181 primes the largest of which is 99907. The total number of primes in the interval $[7; 100000]$ is equal to 9585. □

References

[BlJo] *D. Blessenohl and K. Johnsen*, Eine Verschärfung des Satzes von der Normalbasis, J. Algebra **103** (1986), 141-159.

[Ca] *L. Carlitz*, Primitive roots in a finite field, Trans. Am. Math. Soc. **73** (1952), 373-382.

[Co1] *S. D. Cohen*, Primitive elements and polynomials with arbitrary trace, Discrete Math. **83** (1990), 1-7.

[Co2] *S. D. Cohen*, Gauss sums and a sieve for generators of Galois fields, Publ. Math. Debrecen **56** (2000), to appear.

[CoHa1] *S. D. Cohen and D. Hachenberger*, Primitive normal bases with prescribed trace, Applic. Alg. Engin. Comm. Comp. **9** (1999), 383-403.

[CoHa2] *S. D. Cohen and D. Hachenberger*, Primitivity, freeness, norm and trace, Discrete Math. (2000), to appear.

[Da] *H. Davenport*, Bases for finite fields, J. London Math. Soc. **43** (1968), 21-49.

[Ha1] *D. Hachenberger*, "Finite Fields: Normal Bases and Completely Free Elements", Kluwer Academic Publishers, Boston, 1997.

[Ha2] *D. Hachenberger*, On primitive and free roots in a finite field, Applic. Alg. Engin. Comm. Comp. **3** (1992), 139-150.

[Ha3] *D. Hachenberger*, Universal generators for primary closures of Galois fields, in: D. Jungnickel and H. Niederreiter (eds.), Proceedings of the Fifth International Conference on Finite Fields and Applications, Augsburg, August 1999, to appear.

[Ha4] *D. Hachenberger*, Primitive normal bases for towers of field extensions, Finite Fields and their Applications **5** (1999), 378-385.

[Ha5] *D. Hachenberger*, On the additive order of roots of unity and constructions of normal bases, in preparation.

[Ha6] *D. Hachenberger*, A decomposition theory for cyclotomic modules under the complete point of view, (1999), submitted.

[Ha7] *D. Hachenberger*, On the combinatorics of complete generators for cyclotomic modules, in preparation.

[Ha8] *D. Hachenberger*, Primitive complete normal bases for regular extensions, Glasgow Math. J. (2000), to appear.

[HaWr] *G. H. Hardy and E. M. Wright*, "Einführung in die Zahlentheorie", R. Oldenbourg, München, 1958.

[He] *K. Hensel*, Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor, J. reine angew. Math. **103** (1888), 230-237.

[HiTh] *J. H. W. Hirschfeld and J. A. Thas*, "General Galois Geometries", Clarendon Press, Oxford, 1991.

[Ju] *D. Jungnickel*, "Finite Fields. Structure and Arithmetic." Bibliographisches Institut, Mannheim, 1993.

[JuVa] *D. Jungnickel and S. A. Vanstone*, On primitive polynomials over finite fields, J. Algebra **124** (1989), 337-353.

[Ko] *N. Koblitz*, "A Course in Number Theory and Cryptography", Springer, Berlin, 1994 (2nd Edition).

[Le] H. W. Lenstra, Jr., Algorithms for finite fields, in "Number Theory and Cryptography", Ed.: J. H. Loxton, London Math. Soc. LNS **154**, 76-85, Cambridge University Prress, Cambridge.

[LeSc] *H. W. Lenstra, Jr. and R. J. Schoof*, Primitive normal bases for finite fields, Math. Comp. **48** (1987), 217-231.

[LiNi] *R. Lidl and H. Niederreiter*, "Finite Fields", Reading, Massachusetts, Addison-Wesley 1983.

[Lü] *H. Lüneburg*, On the early history of Galois fields, in: D. Jungnickel and H. Niederreiter (eds.), Proceedings of the Fifth International Conference on Finite Fields and Applications, Augsburg, August 1999, to appear.

[MWSl] *F. J. MacWilliams and N. J. A. Sloane*, The Theory of Error-Correcting Codes, Amsterdam, North-Holland, 1977.

[MoMu1] *I. H. Morgan and G. L. Mullen*, Primitive normal polynomials over finite fields, Math. Comp. **63** (1994), 759-765.

[MoMu2] *I. H. Morgan and G. L. Mullen*, Completely normal primitive basis generators of finite fields, Utilitas Math. **49** (1996), 21-43.

[Or] *O. Ore*, Contributions to the theory of finite fields, Trans. Am. Math. Soc. **36** (1934), 243-274.

[Pe] *S. Perlis*, Normal bases of cyclic fields of prime power degree, Duke Math. J. **9** (1942), 507-517.

[Po] *A. Poli*, A deterministic construction of normal bases with complexity $O(n^3 + n\log(n)\log(\log(n))\log(q))$, J. Symbolic Computation **19** (1995), 305-319.

[Ro] *G.-C. Rota*, On the foundations of Combinatorial Theory I: theory of Möbius functions, Zeitschrift f. Wahrsch.theorie und Verw. Gebiete **2** (1964), 340-368.

[Sche] *A. Scheerhorn*, Trace- and norm-compatible extensions of finite fields, Applic. Alg. Engin. Comm. Comp. **3** (1992), 435-447.

Characterizations of Some Distance-regular Graphs their Spectra

W, Haemers*, E. van Dam

Tilburg University
e-mail: Haemers@kub.nl

We deal with the question: When can one see from the spectrum of a graph whether it is distance-regular or not? We give some new cases for which this is true. As a consequence we find (among others) that the following distance-regular graphs are uniquely determined by their spectum: The collinearity graph of the generalized octagons of order $(2,1)$, $(3,1)$ and $(4,1)$, the Biggs-Smith graph and the coset graphs of the doubly truncated binary Golay code and the extended ternary Golay code.

Veronese Varieties over Fields with non-zero Characteristic: A Survey

Hans Havlicek

Abteilung für Lineare Geometrie
Technische Universität
Wiedner Hauptstraße 8–10, A-1040 Wien, Austria
e-mail: havlicek@geometrie.tuwien.ac.at

1 Introduction

Non-zero characteristic of the (commutative) ground field F heavily influences the geometric properties of Veronese varieties and, in particular, normal rational curves. Best known is probably the fact that, in case of characteristic two, all tangents of a conic are concurrent. This has lead to the concept of a *nucleus*. However, it seems that there are essentially distinct definitions. Some authors, like J.A. Thas [38], use this term to denote a point which extends a normal rational curve to an $(q+2)$-arc (F a finite field of even order q), others, like A. Herzer [23], use the same term for the intersection of all osculating hyperplanes of a Veronese variety. In order to overcome this difference of terminology we introduce the term (r,k)*-nucleus*. The two types of nuclei mentioned above are just particular examples fitting into this general concept.

Each nucleus is an *invariant subspace*, i.e. a subspace in the ambient space of a Veronese variety which is fixed (as a set of points) under the group of automorphic collineations of the variety. However, an invariant subspace needs not be a nucleus.

In the present survey we collect some recent results on nuclei of Veronese varieties and invariant subspaces of normal rational curves. We must assume, however, that the ground field is not "too small", since otherwise a Veronese variety is like dust: "few points" in some "high-dimensional" space.

Nuclei and invariant subspaces do not appear in classical textbooks on Veronese varieties ($F = \mathbb{R}, \mathbb{C}$), since for characteristic zero all invariant subspaces are trivial. If the ground field has characteristic $p > 0$, then geometric properties of invariant subspaces are closely related to *multinomial coefficients* that vanish modulo p and to the representations of certain integers in base p. In order to illustrate this connection some results on binomial and multinomial coefficients are gathered in Chapters 2 and 4.

2 Pascal's triangle modulo a prime p

2.1 A partition of zero entries

Throughout this section let p be a fixed prime. The representation of a non–negative integer $n \in \mathbb{N} := \{0, 1, 2, \ldots\}$ in base p has the form

$$n = \sum_{\sigma=0}^{\infty} n_\sigma p^\sigma =: \langle n_\sigma \rangle \tag{1}$$

with only finitely many digits $n_\sigma \in \{0, 1, \ldots, p-1\}$ different from 0.

Let $\langle n_\sigma \rangle$ and $\langle j_\sigma \rangle$ be the representations of non–negative integers n and j in base p. By a Theorem of Lucas [4, 364],

$$\binom{n}{j} \equiv \prod_{\sigma=0}^{\infty} \binom{n_\sigma}{j_\sigma} \pmod{p}. \tag{2}$$

Pascal's triangle modulo p will be denoted by Δ. The numbering of its rows starts with the index 0. Also, let Δ^i ($i \in \mathbb{N}$) be the subtriangle of Δ that is formed by the rows $0, 1, \ldots, p^i - 1$. From (2) each triangle Δ^{i+1} ($i \geq 0$) has the following form, with products taken modulo p:

$$\begin{array}{c}
\binom{0}{0}\Delta^i \\
\binom{1}{0}\Delta^i \quad \nabla^i \quad \binom{1}{1}\Delta^i \\
\binom{2}{0}\Delta^i \quad \nabla^i \quad \binom{2}{1}\Delta^i \quad \nabla^i \quad \binom{2}{2}\Delta^i \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\binom{p-1}{0}\Delta^i \quad \nabla^i \qquad\qquad\qquad \cdots \qquad\qquad\qquad \nabla^i \quad \binom{p-1}{p-1}\Delta^i
\end{array}$$

Here the ∇^i's are triangles with all entries equal to zero. Observe that the baseline of Δ^i has p^i entries, whereas the top line of ∇^i is formed by $p^i - 1$ zero entries. So ∇^0 is empty. The binomial coefficients on the left hand side of the Δ^i's are exactly the entries of Δ^1. None of them vanishes modulo p. If $i \geq 2$, then each subtriangle $\binom{n}{j}\Delta^i$ from above can be decomposed into subtriangles proportional to Δ^{i-1} and subtriangles ∇^{i-1}, and so on. Cf., among others, [24, 91–92], [33, Theorem 1], [44].

The zero entries of Pascal's triangle modulo p fall into (disjoint) maximal subtriangles ∇^i ($i \in \mathbb{N}^+$). We get a partition of all zero entries of Δ by gluing together all triangles ∇^i of same size to one class, say $\bar{i}$. A formal definition of this partition, which is the backbone of many further considerations, is as follows:

Definition 1 [11] A pair $(n, j) = (\langle n_\sigma \rangle, \langle j_\sigma \rangle)$ of non–negative integers with $j \leq n$, $\binom{n}{j} \equiv 0 \pmod{p}$, and $L := \max\{\sigma \in \mathbb{N} \mid j_\sigma > n_\sigma\}$, is in *class* $\bar{i}$, if

$$i = \min\{\sigma \mid \sigma > L,\ j_\sigma < n_\sigma\} \in \mathbb{N}^+.$$

2.2 Counting zero entries

The following is taken from [11]. Let $n = \langle n_\sigma \rangle \in \mathbb{N}$ and $i \in \mathbb{N}^+$. Then the number of entries in row n of Δ belonging to class $\overline{i}$ equals

$$\Phi(i,n) := \#\overline{i(n)} = \Big(p^i - 1 - \sum_{\mu=0}^{i-1} n_\mu p^\mu\Big) \cdot n_i \cdot \prod_{\sigma=i+1}^{\infty} (n_\sigma + 1). \tag{3}$$

The number of entries in row n of Δ belonging to classes $\overline{i}$, $\overline{(i+1)}$, ... is

$$\Sigma(i,n) := \sum_{\eta=i}^{\infty} \Phi(\eta, n) = n + 1 - \Big(1 + \sum_{\mu=0}^{i-1} n_\mu p^\mu\Big) \prod_{\sigma=i}^{\infty} (n_\sigma + 1). \tag{4}$$

For $i = 1$ this is due to N.J. Fine [7].

When exhibiting "vertical" properties of Δ the following *top line function* turns out useful: Given $b \in \mathbb{N}^+$ and $R \in \mathbb{N}$ then let

$$T(R,b) := \sum_{\sigma=R}^{\infty} b_\sigma p^\sigma. \tag{5}$$

This function has the following property: If $(n,j) \in \overline{i}$ and $b := n+1$ then $T(i,b)$ gives the "top line" of the triangle ∇^i containing the (n,j)-entry of Δ, i.e.

$$0 \equiv \binom{n}{j} \equiv \binom{n-1}{j} \equiv \ldots \equiv \binom{T(i,b)}{j} \not\equiv \binom{T(i,b)-1}{j} \pmod{p}. \tag{6}$$

We refer to [14], [31], [36] for further properties of Δ.

3 Normal Rational Curves

3.1 Definition of k-nuclei

Let $\{\mathbf{b}_0, \mathbf{b}_1\}$ be a basis of a 2-dimensional vector space $\mathbf{X}$ over a commutative field F (the parameter space) and let $\mathbf{Y}$ be an $(n+1)$-dimensional vector space over F with a basis $\{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_n\}$, where $n \geq 2$. The *Veronese mapping*

$$F(x_0\mathbf{b}_0 + x_1\mathbf{b}_1) \mapsto F\Big(\sum_{e=0}^{n} x_0^{n-e} x_1^e \mathbf{c}_e\Big) \ (x_i \in F). \tag{7}$$

maps the point set of the projective line $\mathcal{P}(\mathbf{X})$ into the point set of $\mathcal{P}(\mathbf{Y})$, i.e. the projective space on $\mathbf{Y}$. Its image is a *normal rational curve* $\mathcal{V}_1^n$ (sometimes abbreviated as NRC) with ambient space $\mathcal{P}(\mathbf{Y})$ [1], [2], [3], [5], [26, Chapter 21]. In terms of coordinates and an inhomogeneous parameter $x := x_1/x_0$ we obtain

$$\mathcal{V}_1^n := \{F(1, x, \dots, x^n) \mid x \in F \cup \{\infty\}\}. \tag{8}$$

Recall the *non-iterative derivation* due to H. Hasse, F.K. Schmidt, and O. Teichmüller [15], [27, 1.3]. The k-th derivative $D^{(k)} : F[X] \to F[X]$ is a linear mapping such that $D^{(k)}(X^r) = \binom{r}{k} X^{r-k}$ for $k \le r$ and $D^{(k)}(X^r) = 0$ otherwise $(r, k \in \mathbb{N})$.

If we fix one $u \in F$ then columns of the regular matrix

$$\begin{pmatrix} \binom{0}{0} & 0 & 0 & \dots & 0 \\ \binom{1}{0}u & \binom{1}{1} & 0 & \dots & 0 \\ \binom{2}{0}u^2 & \binom{2}{1}u & \binom{2}{2} & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ \binom{n}{0}u^n & \binom{n}{1}u^{n-1} & \binom{n}{2}u^{n-2} & \dots & \binom{n}{n} \end{pmatrix} \tag{9}$$

give, respectively, a point of the NRC (8) and its *derivative points*. The *k-osculating subspace* ($k \in \{-1, 0, \dots, n-1\}$) of $\mathcal{V}_1^n$ at the given point is the k-dimensional projective subspace spanned by the first $k+1$ columns of the matrix (9). The derivative points at $F\mathbf{c}_n$ $(u = \infty)$ are $F\mathbf{c}_{n-1}, F\mathbf{c}_{n-2} \dots, F\mathbf{c}_0$.

Formal derivation in $F[X]$ is in general not an adequate tool to describe osculating subspaces [35].

The (empty) (-1)-osculating subspace is introduced for formal reasons only. However, we refrain from calling the entire space an n-osculating subspace. As usual, a 1-osculating subspace is also called a *tangent*.

Definition 2 [11] The *k-nucleus* $\mathcal{N}^{(k)}\mathcal{V}_1^n$ ($k \in \{-1, 0, \dots, n-1\}$) of a normal rational curve $\mathcal{V}_1^n$ is the intersection of all its k-osculating subspaces.

Remark 1 Instead of a parametric representation one could also use a *generating map* [16], [19], *Segre varieties* [5], [32], [46], [47] or tools from multilinear algebra [12], [23] in order to define osculating subspaces.

If $\#F \ge n + 2$ or $n = 2$, then each automorphic collineation of the NRC (8) preserves osculating subspaces. Otherwise, there are automorphic collineations of the NRC that do not preserve all osculating subspaces, whence the concept of osculating subspaces depends on the parametric representation of the NRC rather than on the points of the NRC [17], [19, 2.4].

3.2 Number and dimensions of nuclei

The following theorem links nuclei of a NRC with Pascal's triangle:

Theorem 1 [11] *If $\#F \geq k+1$, then the k-nucleus $\mathcal{N}^{(k)}\mathcal{V}_1^n$ of the normal rational curve (8) equals the subspace spanned by those base points $F\mathbf{c}_j$, where $j \in \{0,1,\ldots,n\}$ is subject to*

$$\binom{k+1}{j} \equiv \binom{k+2}{j} \equiv \ldots \equiv \binom{n}{j} \equiv 0 \pmod{\operatorname{char} F}. \tag{10}$$

By Theorem 1, $\operatorname{char} F = 0$ implies that all nuclei of a NRC are empty. Thus we assume in the remaining part of this section that

$$\operatorname{char} F =: p > 0;\ n =: \langle n_\sigma \rangle,\ n+1 =: b =: \langle b_\sigma \rangle \text{ (in base } p). \tag{11}$$

The (projective) dimension of a k-nucleus is described in

Theorem 2 [11] *If $\#F \geq k+1$ and*

$$T(R,b) = \sum_{\mu=R}^{\infty} b_\mu p^\mu \leq k+1 < \sum_{\sigma=Q}^{\infty} b_\sigma p^\sigma = T(Q,b) \tag{12}$$

with at most one $b_\sigma \neq 0$ for $\sigma \in \{Q, Q+1, \ldots, R-1\}$, then the k-nucleus of $\mathcal{V}_1^n$ has dimension

$$n - \Big(1 + \sum_{\mu=0}^{R-1} n_\mu p^\mu\Big) \prod_{\sigma=R}^{\infty} (n_\sigma + 1) = \Sigma(R,n) - 1. \tag{13}$$

The condition on the digits b_σ guarantees that the top line function T does not assume a value that is properly between $T(R,b)$ and $T(Q,b)$.

If $k = n-1$, then (13) turns into Timmermann's formula [41, 4.15]

$$\dim \mathcal{N}^{(n-1)}\mathcal{V}_1^n = n - \prod_{\sigma=0}^{\infty} (n_\sigma + 1) = \Sigma(1,n) - 1; \tag{14}$$

cf. also [40].

Remark 2 If the ground field F does not meet the richness condition of Theorem 2, then (13) is a lower bound for the dimension of the k-nucleus, but it seems to be an open problem to explicitly determine the dimension of the k-nucleus in terms of k, n, and $\#F$. See also [18] and Example 3.

Next we state a formula for the number of distinct nuclei:

Theorem 3 [11] *If $\#F \geq n$, then there are as many distinct nuclei of $\mathcal{V}_1^n$ as non-zero digits in the representation of $b = n+1$ in base p.*

Example 1 Let $p = 2$ and $n = 50$: The representation of $50+1$ in base 2 is $\langle 110011 \rangle$; there are four non-zero digits. So there are four distinct nuclei, including one empty nucleus. From

$$\begin{gathered} T(0,51) = \langle 110011 \rangle = 51, \quad T(1,51) = \langle 110010 \rangle = 50, \\ T(2,51) = T(3,51) = T(4,51) = \langle 110000 \rangle = 48, \\ T(5,51) = \langle 100000 \rangle = 32, \quad T(6,51) = \langle 0 \rangle = 0, \end{gathered}$$

we obtain the following values:

k	$-1, 0, \ldots, 30$	$31, 32, \ldots, 46$	$47, 48$	49
$\dim \mathcal{N}^{(k)} \mathcal{V}_1^n$	-1	12	38	42

Remark 3 Let $\#F \geq n$. Then

$$n = 2p^i - 2 \geq 2 \tag{15}$$

is necessary and sufficient for the smallest non-empty nucleus to be a single point. In fact, this point is $F\mathbf{c}_{p^i-1}$. In particular, if F is a finite field of even order q, then this point together with $\mathcal{V}_1^n$ is a $(q+2)$-arc [38]. Cf. also [8], [37]. In general, however, the geometric meaning of this point seems to be unknown.

From Theorem 3 all nuclei are empty exactly if

$$n = \langle n_J, p-1, \ldots, p-1 \rangle = n_J p^J - 1 \geq 2 \tag{16}$$

with $1 \leq n_J < p$ and $J \in \mathbb{N}$. See also [23], [32].

Further properties of nuclei can be found in [10], [11].

3.3 Invariant subspaces

Each NRC $\mathcal{V}_1^n$ admits a group of collineations that is similar - via (7) - to $\mathrm{P\Gamma L}(2, F)$ acting on the projective line $\mathcal{P}(\mathbf{X})$. If $\#F \geq n+2$ or $n = 2$ then this group is the full collineation group of the curve [17].

Each nucleus is an *invariant subspace* i.e. it remains fixed (as a point set) under the full collineation group of the NRC. In many low-dimensional examples there are no invariant subspaces other than nuclei. Clearly, all invariant subspaces form a lattice with the operations of “join” and “meet”.

In order to find all invariant subspaces, we follow J. Gmainer [9]: Suppose that the dimension n is fixed. For $j \in \mathbb{N}$ let

$$\Omega(j) := \{m \in \mathbb{N} \mid 0 \leq m \leq n, \tbinom{m}{j} \not\equiv 0 \pmod{\operatorname{char} F}\}. \tag{17}$$

Given a subset $J \subset \{0, 1, \ldots, n\}$ then put

$$\Omega(J) := \bigcup_{j \in J} \Omega(j), \quad \Psi(J) := \bigcup_{j \in J} \{j, n-j\}. \tag{18}$$

Both Ω and Ψ are closure operators on $\{0, 1, \ldots, n\}$.

Now we are able to formulate the main theorem for invariant subspaces.

Theorem 4 [9] *Let $\#F \geq n+2$ or $n = 2$. A subspace $\mathcal{U}$ is invariant under the collineation group of the normal rational curve (8) if, and only if, $\mathcal{U}$ is spanned by base points $F\mathbf{c}_\lambda$ with $\lambda \in \Lambda \subset \{0, 1, \ldots, n\}$ such that $\Psi(\Lambda) \subset \Lambda$ and $\Omega(\Lambda) \subset \Lambda$.*

In case of $\operatorname{char} F = 0$ there are only trivial invariant subspaces. Thus we may restrict ourselves to the case

$$\operatorname{char} F = p > 0. \tag{19}$$

By Theorem 4 it suffices to find all Ψ-closed index sets $\Omega(J) \subset \{0, 1, \ldots, n\}$. To this end we proceed in four steps:

Firstly, let $\langle b_\sigma \rangle$ be the expansion of $b = n+1$ in base p. We define

$$V(i, b) := \sum_{\sigma=0}^{i-1} b_\sigma p^\sigma \text{ for all } i \in \mathbb{N}. \tag{20}$$

Secondly, we fix one number $i \in \mathbb{N}$. Suppose that I_α, where $\alpha \in \{1, 2, \ldots, L\}$, is a family of sets such that the following conditions on the sets I_α and the digits b_σ of b hold true:

1. Each non-empty set I_α has the form $I_\alpha = \{j \in \mathbb{N} \mid H_\alpha > j \geq h_\alpha\}$ with $i - 1 \geq H_\alpha > h_\alpha \geq 0$.
2. If $\alpha > \beta$ and $I_\alpha, I_\beta \neq \emptyset$, then $h_\alpha > H_\beta$.
3. $b_{H_\alpha} < p - 1$ and $b_{h_\alpha} > 0$ for each non-empty set I_α.

For empty subsets I_α no numbers H_α, h_α will be defined. Thus

$$V(i, b) = \langle \ldots, b_{H_\alpha}, \underbrace{b_{H_\alpha - 1}, \ldots, b_{h_\alpha}}_{I_\alpha \neq \emptyset}, \ldots \rangle \tag{21}$$

and blocks of digits belonging to different non-empty sets $I_\alpha \cup \{H_\alpha\}$ do not overlap. So we are in a position to define a number by simultaneously changing the digits of $V(i, b)$ for all non-empty sets I_α as follows:

$$V(I_1, \ldots, I_L; i, b) := \langle \ldots, b_{H_\alpha} + 1, \underbrace{0, \ldots, 0}_{I_\alpha \neq \emptyset}, \ldots \rangle \tag{22}$$

Thirdly, we assign to each $(I_1, I_2, \ldots, I_L, i, b)$, such that $V(I_1, I_2, \ldots, I_L; i, b)$ is defined, the set

$$\mathcal{T}(I_1 \times I_2 \times \cdots \times I_L) \tag{23}$$

of all $(T_1, T_2, \ldots, T_L)$ satisfying the following conditions:

1. If $T_\alpha \neq \emptyset$ then $T_\alpha \subset I_\alpha$ and $h_\alpha = \min T_\alpha$.
2. $V(T_1, T_2, \dots, T_L; i, b)$ is defined.

Finally, whenever $V(I_1, I_2, \dots, I_L; i, b)$ is defined, put

$$\Lambda(I_1, \dots, I_L; i, b) := \bigcup \Big(\Omega(V(T_1, \dots, T_L; i, b))\Big), \tag{24}$$

by taking the union over all $(T_1, T_2, \dots, T_L) \in \mathcal{T}(I_1 \times I_2 \times \dots \times I_L)$.

Let us say that an invariant subspace is *irreducible* if it is not spanned by the invariant subspaces properly contained in it. Then, with all the assumptions made so far, we obtain

Theorem 5 [9] *Let $\#F \geq n+2$ or $n = 2$. An invariant subspace $\mathcal{U}$ of the normal rational curve (8) is irreducible if, and only if, it can be written as*

$$\mathcal{U} := \operatorname{span}\{F\mathbf{c}_\lambda \mid \lambda \in \Lambda(I_1, \dots, I_L; i, b)\}. \tag{25}$$

As the lattice of invariant subspaces has only finitely many elements, each invariant subspace is a join of irreducible ones.

Example 2 Let $n = 31$, $p = 3$ and $\#F \geq 33$. From $b = 32 = \langle 1012 \rangle$ we get

$$\begin{array}{rclrcl} V(0,32) & = & \langle 0 \rangle, & V(1,32) & = & \langle 2 \rangle, \\ V(3,32) & = & \langle 012 \rangle, & V(\{0\};3,32) & = & \langle 020 \rangle, \\ V(\{1\};3,32) & = & \langle 102 \rangle, & V(\{0,1\};3,32) & = & \langle 100 \rangle, \\ V(4,32) & = & \langle 1012 \rangle. & & & \end{array}$$

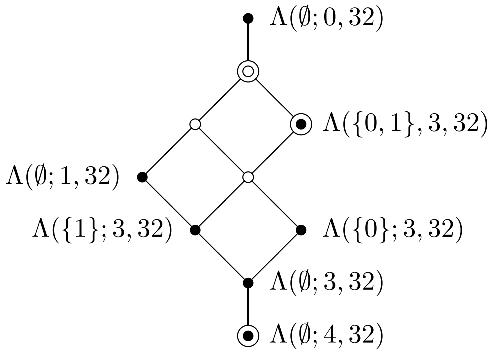
Note that, for example, $V(0,32) = V(\emptyset;0,32)$. Further $V(2,32) = V(3,32)$, $V(\{0\};2,32) = V(\{0\};3,32)$, and $V(I_1, I_2, \dots, I_L; 4, 32) \geq 32$. So

$$\begin{aligned} \Omega(\langle 0 \rangle) &= \{\langle 0 \rangle, \langle 1 \rangle, \dots, \langle 1011 \rangle\}, \\ \Omega(\langle 2 \rangle) &= \{\langle 2 \rangle, \langle 12 \rangle, \langle 22 \rangle, \langle 102 \rangle, \langle 112 \rangle, \langle 122 \rangle, \langle 202 \rangle, \langle 212 \rangle, \langle 222 \rangle, \langle 1002 \rangle\}, \\ \Omega(\langle 12 \rangle) &= \{\langle 12 \rangle, \langle 22 \rangle, \langle 112 \rangle, \langle 122 \rangle, \langle 212 \rangle, \langle 222 \rangle\}, \\ \Omega(\langle 20 \rangle) &= \{\langle 20 \rangle, \langle 21 \rangle, \langle 22 \rangle, \langle 120 \rangle, \langle 121 \rangle, \langle 122 \rangle, \langle 220 \rangle, \langle 221 \rangle, \langle 222 \rangle\}, \\ \Omega(\langle 102 \rangle) &= \{\langle 102 \rangle, \langle 112 \rangle, \langle 122 \rangle, \langle 202 \rangle, \langle 212 \rangle, \langle 222 \rangle\}, \\ \Omega(\langle 100 \rangle) &= \{\langle 100 \rangle, \langle 101 \rangle, \dots, \langle 222 \rangle\}, \\ \Omega(\langle 1012 \rangle) &= \emptyset, \end{aligned}$$

are the relevant index sets and

$$\begin{array}{rcl} \Lambda(\emptyset;0,32) & = & \Omega(\langle 0 \rangle), \\ \Lambda(\emptyset;1,32) & = & \Omega(\langle 2 \rangle), \\ \Lambda(\emptyset;3,32) & = & \Omega(\langle 12 \rangle), \\ \Lambda(\{0\};3,32) & = & \Omega(\langle 12 \rangle) \cup \Omega(\langle 20 \rangle) \\ \Lambda(\{1\};3,32) & = & \Omega(\langle 12 \rangle) \cup \Omega(\langle 102 \rangle) \\ \Lambda(\{0,1\};3,32) & = & \Omega(\langle 12 \rangle) \cup \Omega(\langle 20 \rangle) \cup \Omega(\langle 102 \rangle) \cup \Omega(\langle 100 \rangle) \\ \Lambda(\emptyset;4,32) & = & \emptyset. \end{array}$$

The Hasse diagram of the lattice of invariant subspaces is given in the figure. Filled circles represent irreducible subspaces and double circles mark nuclei.


$\Lambda(\emptyset; 0, 32)$
$\Lambda(\{0,1\}, 3, 32)$
$\Lambda(\emptyset; 1, 32)$
$\Lambda(\{1\}; 3, 32)$
$\Lambda(\{0\}; 3, 32)$
$\Lambda(\emptyset; 3, 32)$
$\Lambda(\emptyset; 4, 32)$

In many low-dimensional examples the invariant subspaces form a chain. In general, however, the following holds true:

Theorem 6 [9] *Let the positions of the non-zero digits of $b := n+1$ in base p be denoted by $N_1, N_2, \ldots, N_d$. Then the lattice of invariant subspaces is totally ordered if, and only if, one of the following cases occurs:*

1. $d \in \{1, 2\}$.
2. $d \geq 3$, $N_d - N_1 = d - 1$, *and* $N_2 = \ldots = N_{d-1} = p - 1$.

Thus all invariant subspaces can be found, provided that the ground field is sufficiently large. Also, in specific cases the structure of the lattice of invariant subspaces is known.

Remark 4 If we project a NRC from one of its invariant subspaces other than $\mathcal{P}(\mathbf{Y})$, then a rational curve is obtained; this curve admits a collineation group isomorphic to $\mathrm{P\Gamma L}(2, F)$. Via (7) and the projection, the group actions on the curve and the projective line $\mathcal{P}(\mathbf{X})$ are similar.

4 Pascal's simplex modulo a prime

Throughout this section let p be a fixed prime. Given $m, t \in \mathbb{N}$ then put

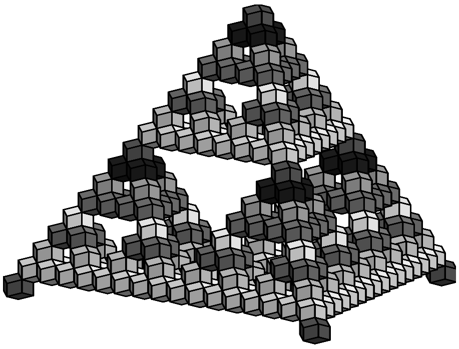
$$E_m^t := \{(e_0, e_1, \ldots, e_m) \in \mathbb{N}^{m+1} \mid e_0 + e_1 + \ldots + e_m = t\}. \tag{26}$$

The array of multinomial coefficients $\binom{t}{e_0, e_1, \ldots, e_m}$ with $(e_0, e_1, \ldots, e_m) \in E_m^t$ is frequently called *Pascal's simplex*.

The theorem of Lucas (2) can be generalized to multinomial coefficients as follows [4, 364]: If $t, e_0, e_1, \dots, e_m \in \mathbb{N}$ have representations $t = \sum_\sigma t_\sigma p^\sigma$ and $e_i = \sum_\sigma e_{i,\sigma} p^\sigma$ in base p then

$$\binom{t}{e_0, e_1, \dots, e_m} \equiv \prod_{\sigma \in \mathbb{N}} \binom{t_\sigma}{e_{0,\sigma}, e_{1,\sigma}, \dots, e_{m,\sigma}} \pmod{p}. \tag{27}$$

For trinomial coefficients ($m = 3$) it is possible to illustrate Pascal's simplex in the form of a pyramid:



The picture above shows a part of Pascal's pyramid modulo 2. It is based upon a tiling of the space by rhombic dodecahedra. If an entry of the pyramid vanishes, then the corresponding dodecahedron is omitted. Entries at the same "horizontal" level (t constant) are equally shaded. Cf. [25].

The following has been established independently by F.T. Howard [30, Theorem 3.1] and N.A. Volodin [42, Theorem 2]; see also [43]:

The number of $(m+1)$–tuples $(e_0, e_1, \dots, e_m) \in E_m^t$ such that the multinomial coefficient $\binom{t}{e_0, e_1, \dots, e_m}$ is divisible by the prime p equals

$$\binom{m+t}{t} - \prod_{\sigma \in \mathbb{N}} \binom{m + t_\sigma}{t_\sigma}. \tag{28}$$

5 Veronese varieties

5.1 Definition of (r, k)-nuclei

Let $\{\mathbf{b}_0, \mathbf{b}_1, \dots, \mathbf{b}_m\}$ be a basis of an $(m + 1)$-dimensional vector space $\mathbf{X}$ over F (the parameter space) and let $\mathbf{Y}$ be an $\binom{m+t}{t}$-dimensional vector space over F with a basis $\{\mathbf{c}_{e_0, e_1, \dots, e_m} \mid (e_0, e_1, \dots, e_m) \in E_m^t\}$; cf. (26). We shall always assume that $m \geq 1$ and $t \geq 2$ in order to avoid trivialities.

Generalizing (7), the *Veronese mapping* is given by

$$F\Big(\sum_{i=0}^{m} x_i\mathbf{b}_i\Big) \mapsto F\Big(\sum_{E_m^t} x_0^{e_0}x_1^{e_1}\dots x_m^{e_m}\mathbf{c}_{e_0,e_1,\dots,e_m}\Big) \ (x_i \in F). \tag{29}$$

Its image is a *Veronese variety* $\mathcal{V}_m^t$ with ambient space $\mathcal{P}(\mathbf{Y})$, i.e. the projective space on $\mathbf{Y}$. (By putting $m := 1$ and $n := t$ a NRC $\mathcal{V}_1^n$ is obtained.)

The Veronese image of each r-dimensional subspace of $\mathcal{P}(\mathbf{X})$ $(0 \le r < m)$ is a sub-Veronesean $\mathcal{V}_r^t$ of $\mathcal{V}_m^t$. (For $r = 0$ we get just one point, for $r = 1$ a normal rational curve, etc. Cf. also [6].) For each $k \in \{-1, 0, \dots, t-1\}$ there exists a *k-osculating subspace of $\mathcal{V}_m^t$ along $\mathcal{V}_r^t$*. We call it an *(r,k)-osculating subspace* of $\mathcal{V}_m^t$. Its dimension equals

$$\sum_{i=t-k}^{t} \binom{r+i}{i}\binom{m+t-r-i-1}{t-i} - 1; \tag{30}$$

cf. [23] and the papers cited in Remark 1. Now we adopt the following

Definition 3 The (r,k)-*nucleus* of a Veronese variety $\mathcal{V}_m^t$ is the intersection of all its (r,k)-osculating subspaces.

The k-nuclei of a normal rational curve are the $(0,k)$-nuclei according to the present definition.

Remark 5 A geometric characterization of quadratic Veronese mappings ($t = 2$) can be found in [22]. Combinatorial characterizations of the Veronese surface ($m = t = 2$) over a finite field are given in [29]. Applications of Veronese varieties over finite fields in coding theory and authentication systems can be found in [13], [20], [21], [28], [37], [39], [45]. Partial linear spaces derived from Veronese varieties are discussed in [34].

5.2 Intersection of osculating hyperplanes

From (30), each $(t-1, m-1)$-osculating subspace of a Veronese variety $\mathcal{V}_m^t$ is a hyperplane of $\mathcal{P}(\mathbf{Y})$ which is called an *osculating hyperplane* (or *contact hyperplane*) of the Veronese variety $\mathcal{V}_m^t$. Thus to each hyperplane of the parameter space there corresponds an osculating hyperplane of the Veronesean. In terms of dual bases this *dual Veronese mapping* is given by

$$F\Big(\sum_{i=0}^{m} a_i\mathbf{b}_i^*\Big) \mapsto F\Big(\sum_{E_m^t} \tbinom{t}{e_0,e_1,\dots,e_m} a_0^{e_0}a_1^{e_1}\dots a_m^{e_m}\mathbf{c}^*_{e_0,e_1\dots,e_m}\Big) \ (a_i \in F). \tag{31}$$

See also [5, pp. 160–163]. The intersection of all osculating hyperplanes of a $\mathcal{V}_m^t$ is its $(m-1, t-1)$-nucleus. Both A. Herzer [23] and H. Karzel [32] determined all Veronese varieties where this specific nucleus is empty.

Theorem 7 [12] *The $(m-1,t-1)$-nucleus of a Veronese variety $\mathcal{V}_m^t$ contains exactly those base points $F\mathbf{c}_{e_0,e_1,\ldots,e_m}$ satisfying*

$$\binom{t}{e_0,e_1,\ldots,e_m} \equiv 0 \pmod{\operatorname{char} F}. \tag{32}$$

If $\#F \geq t$, then this nucleus is spanned by those base points.

From this and (28) follows

Theorem 8 [12] *Let $\sum_{\sigma\in\mathbb{N}} t_\sigma p^\sigma$ be the representation of t in base $p = \operatorname{char} F > 0$. If $\#F \geq t$, then the $(m-1,t-1)$-nucleus of a Veronese variety $\mathcal{V}_m^t$ has dimension*

$$\binom{m+t}{t} - \prod_{\sigma\in\mathbb{N}} \binom{m+t_\sigma}{t_\sigma} - 1. \tag{33}$$

Example 3 Let $\operatorname{char} F = 2$.

The $(1,1)$-nucleus of the Veronese surface $\mathcal{V}_2^2$ is a plane; cf. [29, Chapter 25].

From Theorem 8 the $(1,2)$-nucleus of the Veronese surface $\mathcal{V}_2^3$ is a single point provided that $\#F \neq 2$. On the other hand, if $\#F = 2$ then, by solving a system of seven linear equations, the $(1,2)$-nucleus of $\mathcal{V}_2^3$ is easily seen to be three-dimensional. In either case $\mathcal{V}_2^3$ carries a family of twisted cubics that arise as Veronese images of the lines in the parameter plane. For $\#F \neq 2$ the 2-nucleus of a twisted cubic is empty, but for $\#F = 2$ this nucleus is a single point.

References

[1] E. Bertini. *Introduzione alla geometria proiettiva degli iperspazi.* E. Spoerri, Pisa, 1907.

[2] E. Bertini. *Einführung in die projektive Geometrie mehrdimensionaler Räume.* Seidel u. Sohn, Wien, 1924.

[3] H. Brauner. *Geometrie projektiver Räume II.* BI-Wissenschaftsverlag, Mannheim Wien Zürich, 1976.

[4] A.E. Brouwer and H.A. Wilbrink. Block designs. In F. Buekenhout, editor, *Handbook of incidence geometry*, chapter 8, pages 349–382. Elsevier, Amsterdam, 1995.

[5] W. Burau. *Mehrdimensionale projektive und höhere Geometrie.* Dt. Verlag d. Wissenschaften, Berlin, 1961.

[6] W. Burau. Über ausgezeichnete Aufspaltungen des Raumes einer Veroneseschen V_n^t und ihre Anwendung auf die Berechnung der Hilbertfunktion der rationalen Normregelmannigfaltigkeiten. *Veröff. Univ. Innsbruck*, 91:17–28, 1974.

[7] N.J. Fine. Binomial coefficients modulo a prime. *Am. Math. Mon.*, 54:589–592, 1947.

[8] D.G. Glynn. The non-classical 10-arc of PG(4, 9). *Discrete Math.*, 59:43–51, 1986.

[9] J. Gmainer. Pascal's triangle, normal rational curves, and their invariant subspaces. submitted.

[10] J. Gmainer. *Rationale Normkurven in Räumen mit positiver Charakteristik.* Thesis, Vienna University of Technology, 1999.

[11] J. Gmainer and H. Havlicek. Nuclei of normal rational curves. J. Geom., in print.

[12] J. Gmainer and H. Havlicek. A dimension formula for the nucleus of a Veronese variety. *Lin. Algebra Appl.*, 305:191–201, 2000.

[13] V.D. Goppa. *Geometry and codes.* Kluwer, Dordrecht Boston London, 1988.

[14] H. Harborth. Über die Teilbarkeit im Pascal-Dreieck. *Math.-phys. Semesterber.*, 22:13–21, 1975.

[15] H. Hasse. Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten. *J. Reine Angew. Math.*, 177:215–237, 1937.

[16] H. Havlicek. Normisomorphismen und Normkurven endlichdimensionaler projektiver Desargues-Räume. *Monatsh. Math.*, 95:203–218, 1983.

[17] H. Havlicek. Die automorphen Kollineationen nicht entarteter Normkurven. *Geom. Dedicata*, 16:85–91, 1984.

[18] H. Havlicek. Erzeugnisse projektiver Bündelisomorphismen. *Ber. Math.-Stat. Sekt. Forschungszent. Graz*, 215, 1984.

[19] H. Havlicek. Applications of results on generalized polynomial identities in desarguesian projective spaces. In R. Kaya, P. Plaumann, and K. Strambach, editors, *Rings and geometry*, pages 39–77. D. Reidel, Dordrecht, 1985.

[20] H. Havlicek. The Veronese surface in $\mathrm{PG}(5,3)$ and Witt's 5-$(12,6,1)$–design. *J. Comb. Theory, Ser. A*, 84(1):87–94, 1998.

[21] H. Havlicek. Giuseppe Veronese and Ernst Witt – neighbours in PG(5,3). *Aequationes Math.*, 58:85–92, 1999.

[22] H. Havlicek and C. Zanella. Quadratic embeddings. *Beitr. Algebra Geom.*, 38:289–298, 1997.

[23] A. Herzer. Die Schmieghyperebenen an die Veronese-Mannigfaltigkeit bei beliebiger Charakteristik. *J. Geom.*, 18:140–154, 1982.

[24] E. Hexel and H. Sachs. Counting residues modulo a prime in Pascal's triangle. *Indian J. Math.*, 20:91–105, 1978.

[25] P. Hilton and J. Pedersen. Relating geometry and algebra in the pascal triangle, hexagon, tetrahedron, and cuboctahedron Part 1: Binomial coefficients, extended binomial coefficients and preparation for further work. *College Mathematics Journal*, 30(3):170–186, 1999.

[26] J.W.P. Hirschfeld. *Finite projective spaces of three dimensions.* Oxford University Press, Oxford, 1985.

[27] J.W.P. Hirschfeld. *Projective geometries over finite fields.* Clarendon Press, Oxford, second edition, 1998.

[28] J.W.P. Hirschfeld and L. Storme. The packing problem in statistics, coding theory, and finite projective spaces. *J. Stat. Plann. Inference*, 72(1-2):355–380, 1998.

[29] J.W.P. Hirschfeld and J.A. Thas. *General Galois geometries.* Oxford University Press, Oxford, 1991.

[30] F.T. Howard. The number of multinomial coefficients divisible by a fixed power of a prime. *Pac. J. Math.*, 50:99–108, 1974.

[31] V.V. Karachik. p-latin matrices and Pascal's triangle modulo a prime. *Fibonacci Q.*, 34(4):362–372, 1996.

[32] H. Karzel. Über einen Fundamentalsatz der synthetischen algebraischen Geometrie von W. Burau und H. Timmermann. *J. Geom.*, 28:86–101, 1987.

[33] C.T. Long. Pascal's triangle modulo p. *Fibonacci Q.*, 19:458–463, 1981.

[34] N. Melone. Veronese spaces. *J. Geom.*, 20:169–180, 1983.

[35] R. Riesinger. Normkurven in endlichdimensionalen Desarguesräumen. *Geom. Dedicata*, 10:427–449, 1981.

[36] J.B. Roberts. On binomial coefficient residues. *Canadian J. Math.*, 9:363–370, 1957.

[37] L. Storme and J.A. Thas. k-arcs and dual k-arcs. *Discrete Math.*, 125, No.1–3:357–370, 1994.

[38] J.A. Thas. Normal rational curves and $(q+2)$–arcs in a Galois space $S_{q-2,q}$ $(q = 2^h)$. *Atti Accad. Naz. Lincei, VIII. Ser., Rend., Cl. Sci. Fis. Mat. Nat.*, 47:249–252, 1969.

[39] J.A. Thas. M.D.S. codes and arcs in projective spaces: A survey. *Le Matematiche*, 47(2):315–328, 1992.

[40] H. Timmermann. Descrizioni geometriche sintetiche di geometrie proiettive con caratteristica $p > 0$. *Ann. Mat. Pura Appl. IV. Ser.*, 114:121–139, 1977.

[41] H. Timmermann. *Zur Geometrie der Veronesemannigfaltigkeit bei endlicher Charakteristik*. Habilitationsschrift, Univ. Hamburg, 1978.

[42] N.A. Volodin. Distribution of polynomial coefficients congruent modulo p^N. *Math. Notes*, 45:195–199, 1989.

[43] N.A. Volodin. Number of multinomial coefficients not divisible by a prime. *Fibonacci Q.*, 32(5):402–406, 1994.

[44] S. Wolfram. Geometry of binomial coefficients. *Am. Math. Mon.*, 91:566–571, 1984.

[45] C. Zanella. Linear sections of the finite Veronese varieties and authentica-tion systems defined using geometry. *Des. Codes Cryptography*, 13(2):199–212, 1998.

[46] J. Zeuge. Eine geometrische Kennzeichnung der Mannigfaltigkeiten von Segre und Veronese und eine damit zusammenhängende ausgezeichnete Transformation zwischen gewissen projektiven Räumen. *Atti Accad. naz. Lincei, VIII. Ser., Rend., Cl. Sci. fis. Mat. natur.*, 53:531–540, 1972.

[47] J. Zeuge. Die Schmiegräume an die Veronesemannigfaltigkeit. *Mitt. Math. Ges. Hamburg*, 10(5):391–393, 1977.

On Embedded Products of Grassmannians

H. Havlicek

Abteilung für Lineare Geometrie - Technische Universität
Wiedner Hauptstraße 8–10, A-1040 Wien, Austria

C. Zanella*

Università di Padova, Italy
e-mail: zanella@math.unipd.it

It is known that the classical embeddings of geometries such as Grassmannians and products of two projective spaces are essentially unique [1,2]. In this talk we deal with the analogous question concerning products of Grassmannians, and give a partial answer to it.

References

[36] H. Havlicek: *Zur Theorie linearer Abbildungen I, II*, J. Geom. **16** (1981), 152–180.

[37] C. Zanella: *Universal properties of the Corrado Segre embedding*, Bull. Belg. Math. Soc. Simon Stevin **3** (1996), 65–79.

On the Steiner System S(24,8,5)

C. Hering

Math. Inst. der Universität
Auf der Morgenstelle 10 - D-72076 Tuebingen - Germany
e-mail: hering@uni-tuebingen.de

We present a new characterization of the Steiner System S(24,8,5).

Arcs and Curves over a Finite Field

J.W.P. Hirschfeld*

University of Sussex, UK
e-mail: jwph@sussex.ac.uk

G. Korchmáros

Università degli Studi della Basilicata, Potenza, Italy
e-mail: korchmaros@unibas.it

Given a plane algebraic curve $\mathcal{C}$ defined over a finite field $\mathbf{F}_q$, how many points does it have?

The short answer is that it depends what you mean. Here are four possible contenders:

(1) the number N_q of $\mathbf{F}_q$-rational points on a non-singular model of $\mathcal{C}$;
(2) the number M_q of points in the projective plane $PG(2, q)$ which lie on $\mathcal{C}$.
(3) the number $\hat{M}_q$ of points in $PG(2, q)$ which lie on $\mathcal{C}$ with each t-fold point counted with multiplicity t;
(4) the number B_q of branches of $\mathcal{C}$ centred at points of $PG(2, q)$.

These numbers can all be distinct.

The theorems of Hasse–Weil and Stöhr–Voloch give bounds on N_q. Applications to combinatorial problems in $PG(2, q)$ can require bounds on B_q. Upper and lower bounds on B_q will be discussed.

References

[38] J.W.P. Hirschfeld and G. Korchmáros: *On the number of solutions of an equation over a finite field*, Bull. London Math. Soc., to appear.

On Conic Blocking Sets

L. Holder, W. Cherowitzo*

Mathematics Department - University of Colorado at Denver - Denver, CO, USA
e-mail L. Holder: dlholder@math.cudenver.edu
e-mail W. Cherowitzo: wcherowi@carbon.cudenver.edu

A (lineal) conic blocking set is a set of lines in $PG(2,q)$ with the property that every conic of the plane intersects at least one line of the set. Such sets arise naturally in the study of flocks of general cones where they are used to distinguish the case of quadratic cones from the others. The study of these sets is in its infancy and we will report on our preliminary findings. We examine only the special case where the lines are concurrent. The results of computer searches in planes of order less than 100 provide data on the sizes of minimal conic blocking sets. A dualization of the problem and an application of some optimization techniques has provided an efficient algorithm for handling the combinatorial explosion inherent in these searches. We provide several constructions, in both odd and even characteristic, of irreducible conic blocking sets (those not containing a smaller conic blocking set). The proofs for these constructions heavily rely on the theory of flocks of quadratic cones. Finally, we report on the progress made in proving the conjectured bounds for the sizes of the minimal conic blocking sets of this type.

Skewaffine Spaces in the Language of Distance Spaces

H. Hotje

University of Hannover, Germany
e-mail: hotje@math.uni-hannover.de

In the past J. André generalized the affine spaces under different aspects to so called non commutative geometries. One of the most general definitions which was inspired by Pfalzgraf is that of skewaffine spaces. Many interesting results are found but this subject is not much familiar to the geometry community. Maybe the reason for this lies in the language of the axioms used.

Here we will give descriptions of such spaces in the language of distance spaces as proposed by W. Benz. Moreover we can find connections to other geometries like Ferrero geometries.

References

[39] J. André: *On non-commutative geometry*, Ann. Univ. Saraviensis. Ser. Math. **4**, 1993, 93-130.

[40] W. Benz: *Geometrische Transformationen*, Mannheim 1992.

[41] H. Hotje: *Einige Anmerkungen zu einer Konstruktion von Marchi/Zizioli*, Proc. 4. Congress of Geometry, (Thessaloniki, 1996), 192-197, Aristotle Univ. Thess. 1997.

Dual Polar Spaces and Fully Gated Graphs

C. Huybrechts*, P.J. Cameron

School of Mathematical Sciences - Queen Mary and Westfield College
London E1 4NS, UK
e-mail: C.huybrecths@qmw.ac.uk

Given two points x and y of a graph Γ, the *segment* $[x, y]$ is the union of all shortest paths joining x and y. A graph Γ is said to be *fully gated* if for every convex subset Y of Γ (i.e. a set containing the segment determined by any two of its points) and every point x of Γ, there exists a point p_x of Y (the "projection" of x on Y) with the property that p_x belongs to each segment $[x, y]$, where $y \in Y$. P. J. Cameron has observed a connection between dual polar spaces and fully gated graphs: the collinearity graph of every dual polar space is fully gated. This observation suggests the possibility to characterize dual polar spaces in terms of fully gated graphs. In this talk, I will discuss some developments in that direction.

On Subplanes of Free Planes

O. Iden

Matematisk Institutt - University of Bergen
J BRUN 12 N-5020 Bergen, Norway
e-mail: iden@mi.uib.no

For the families of free affine, projective, non-projective Moebius, Laguerre and Minkowski planes the ascending chain condition (Sandler 1964) is proved. The tool is a theorem that establishes a basis for subplanes of such planes based on the representation of these planes as posets.

On the Linear Labeling of Lattice Constellations from Algebraic Number Fields

J.C. Interlando

Dipartimento di Elettronica - Politecnico di Torino on leave from
Departamento de Matemática - Universidade Estadual Paulista (UNESP)
São José do Rio Preto, Brazil

M. Elia*

Dipartimento di Elettronica - Politecnico di Torino, Italy
e-mail: elia@polito.it

Conway and Sloane [2] describe several constructions of n-dimensional constellations, also known as multilevel codes. One way to construct them is to take finite subsets of an n-dimensional lattice Λ, which in turn is obtained from an algebraic number field $\mathbb{F} = \mathbb{Q}(\alpha)$ of degree n. The finite set consists of the representatives of the cosets of a prime ideal in $\mathfrak{o}_{\mathbb{F}}$, the maximal order of $\mathbb{F}$. The key to the construction of Λ is to use the canonical embedding σ of $\mathfrak{o}_{\mathbb{F}}$ into $\mathbb{R}^n$ [1]. In this contribution we define and determine the *linear labeling* of the elements of such a lattice $\Lambda = \sigma(\mathfrak{o}_{\mathbb{F}})$ by the elements of a Galois field $GF(q)$. For this, let $\{\omega_1, \ldots \omega_n\}$ be an integral basis for $\mathfrak{o}_{\mathbb{F}}$. A mapping $\ell : \Lambda \to GF(q)$ is called a linear labeling (of the points of Λ by $GF(q)$) if $\ell(\sigma(x_1\omega_1 + \ldots + x_n\omega_n)) = x_1\ell(\sigma(\omega_1)) + \ldots + x_{n-1}\ell(\sigma(\omega_n))$. It can be obtained as follows: Given a rational prime p, let $\overline{m}_{\alpha,\mathbb{Q}}(x)$ be the minimal polynomial of α (over $\mathbb{Q}$) with its coefficients reduced modulo p. Suppose further that $\overline{m}_{\alpha,\mathbb{Q}}(x) = \prod_{j=1}^{g} P_j(x)^{e_j}$, where the $P_j(x)$ are distinct irreducible polynomials of degree f_j over $GF(p)$. Then $p\mathfrak{o}_{\mathbb{F}} = \prod_{j=1}^{g} \mathfrak{p}_j^{e_j}$, where $\mathfrak{p}_j$ are distinct prime ideals in $\mathfrak{o}_{\mathbb{F}}$ given by $\mathfrak{p}_j = (p, P_j(\alpha))$, and $\mathrm{Norm}(\mathfrak{p}_j) = q_j = p^{f_j}$. It follows that $\mathfrak{o}_{\mathbb{F}}/\mathfrak{p}_j \cong GF(q_j)$. Denote this isomorphism by φ, and let $\mathbf{pr}$ be the natural mapping from $\mathfrak{o}_{\mathbb{F}}$ onto $\mathfrak{o}_{\mathbb{F}}/\mathfrak{p}_j$. It can be proven that $\ell = \varphi \circ \mathbf{pr} \circ \sigma^{-1}$ is a linear labeling of Λ by $GF(q_j)$. In fact, ℓ can be completely defined by setting $\ell(\sigma(\alpha)) = \overline{\alpha}$, where $\overline{\alpha}$ is a root of the polynomial $P_j(x)$ over $GF(p)$. Finally, by taking q_j elements of $\sigma(\mathfrak{o}_{\mathbb{F}})$ of minimal energy and distinct labels, a finite constellation of the highest density is determined, labeled by $GF(q_j)$. The linear labeling can be extended in a natural way to sublattices of $\mathfrak{o}_{\mathbb{F}}$, which are images of principal ideals of $\mathfrak{o}_{\mathbb{F}}$.

References

[42] Z. I. Borevich and I. R. Shafarevich: *Number Theory*, New York: Academic Press, 1966.

[43] J. H. Conway and N. J. A. Sloane: *Sphere Packings, Lattices and Groups*, New York: Springer-Verlag, 1988.

This work is supported by FAPESP under grant No. 99/02698-7.

Generalized Tensions and Potentials

A. Khelladi

USTHB Institut de Mathématiques - BP 32 El Alia 16111 - Algiers, Algeria
e-mail: `kader-khelladi@yahoo.fr`

The generalization which will be present is on the bidirected graphs, a natural extension of directed graphs. A *bidirection* τ of an undirected graph $G = (V, E)$ is a mapping τ from the set H of half edges of G into $\{-1, +1\}$ ($H = \{(e, v) \in E \times V | e \text{ is incident to } v\}$). Every bidirection gives rise to a *signature* of the edges

$$\sigma : E \longrightarrow \{-1, +1\} \text{ where } \sigma(e) = -\tau(e, u) \cdot \tau(e, v) \text{ if } e = uv \,.$$

A cycle of G is balanced if it contains an even number of negative edges snd G is balanced if every cycle of G is balanced.

If $G = (V, E, \tau)$ is a bidirected graph, let us recall that the $\mathbb{Z}$-module $\mathbb{Z}^V$ (resp. $\mathbb{Z}^E$) is the set of mappings from V (resp. E) into $\mathbb{Z}$. We recall also the classical mappings

$$\partial_\tau : \mathbb{Z}^E \longrightarrow \mathbb{Z}^V \quad \text{and} \quad : \mathbb{Z}^V \longrightarrow \mathbb{Z}^E$$

defined by

$$\partial_\tau(f)(v) = \sum_{e \in E} \tau(e, v) f(v) \quad \forall\, v \in V \,;$$
$$\delta_\tau(f)(e) = \sum_{v \in V} \tau(e, v) f(v) \quad \forall\, e \in E \,.$$

The $\mathbb{Z}$-modules $\mathrm{Ker}\,(\partial_\tau)$ and $\mathrm{Im}\,(\delta_\tau)$ are respectively the set of (generalized) flows and tensions in G and are the sets of mappings from E into $\mathbb{Z}$. The support of a tension $t : E \longrightarrow \mathbb{Z}$ is the set of edges of G where t is not zero. The minimal supports of tensions are the cocircuits of the matroid $\mathcal{M}(G)$ associated to the bidirected graph G.

We prove some results on the tensions whose supports are circuits as difference of 0-1 potentials on the vertices and we interpret them in terms of subgraphs of G, thus extending some results of W.T. Tutte. In particular we prove the following generalization of a result of A. Bouchet on isthmuses in bidirected graphs: "*Let $G = (V, E, \tau)$ be a connected bidirected graph and A a subset of V. If $\omega(A)$ is an elementary cocycle of the undirected graph of $G = (V, E)$ and if the induced subgraph G_A (or G–A) is balanced, then either $\omega(A)$ is a cocircuit of the matroid $\mathcal{M}(G)$ or a disjoint union of two such cocircuits*".

Circularity of Certain *F*-pairs

H. Kiechle

Mathematisches Seminar - Universität Hamburg
Bundesstr. 55 - D-20146 Hamburg, Germany
e-mail: `kiechle@math.uni-hamburg.de`

An *F-pair* (N, Φ) consists of two groups $(N, +)$ and Φ such that Φ acts as an automorphism group on N, and such that for every $\phi \in \Phi \setminus \{\mathbf{1}\}$, the map $\phi - \mathbf{1} : \mathbf{N} \to \mathbf{N}$ is bijective. We call (N, Φ) finite if N is finite. In this case the condition is equivalent to the condition that Φ acts fixed point free on N. A finite F-pairs gives rise to the 2-designs $(N, \mathbf{B})$ with the set $\mathbf{B} := \{\Phi a + b;\ a, b \in N,\ a \neq 0\}$. The F-pair and the design are called *circular* if $|B \cap B'| \leq 2$ for all $B, B' \in \mathbf{B}$. We'll present some new results on the circularity of F-pairs with non-abelian Φ.

Group–theoretic Ccharacterizations of Classical Ovoids

O.H. King*

University of Newcastle, UK
e-mail: O.H.King@newcastle.ac.uk

A. Cossidente

Università della Basilicata - Potenza, Italy

The only known ovoids of $PG(3,q)$ are the elliptic quadrics, which exist for all q, and the Suzuki-Tits ovoids, which exist for $q = 2^e$, $e \geq 3$ odd. It is well known that for odd q, the only ovoids are the elliptic quadrics. For even q, the ovoids have been classified only for q up to and including 32. We use Aschbacher's Theorem (together with two theorems of Flesner) to study ovoids admitting collineation groups with various properties, and in particular show that, for even q, an ovoid admitting a transitive collineation group must be an elliptic ovoid or a Suzuki-Tits ovoid.

Caps of the Hermitian Variety Arising from Maximal Curves

G. Korchmáros

Università degli Studi della Basilicata
e-mail: korchmaros@unibas.it

Let $\mathcal{H}(r,q^2)$ be the non–degenerate Hermitian variety in $\mathbf{PG}(r,q^2)$. A *cap* (or *partial ovoid*) of $\mathcal{H}(r,q^2)$ is a point–set K in $\mathcal{H}(r,q^2)$ such that K has at most one point in common with every maximal singular subspace of $\mathcal{H}(r,q^2)$. A cap K is a (k,n)-*cap* if K has size k and n is the maximum number of common point of K with a hyperplane of $\mathbf{PG}(r,q^2)$. We show that $\mathcal{H}(n,q^2)$ contains large (k,n)-caps with $n \le q+1$ arising from $\mathbf{GF}(q^2)$-maximal curves. Here a $\mathbf{GF}(q^2)$-maximal curve of genus g is a projective, geometrically irreducible, non-singular, algebraic curve defined over $\mathbf{GF}(q^2)$ such that the number of its $\mathbf{GF}(q^2)$-rational points attains the Hasse-Weil upper bound $1+q^2+2qg$.

A geometric description of Hermitian two-graphs and its applications

E. Kuijken

Fund for Scientific Research - Flanders (Belgium) (F.W.O.)
Universiteit Gent
Vakgroep Zuivere Wiskunde en Computeralgebra
Galglaan 2 - B-9000 Gent - Belgium
e-mail: `ekuijken@cage.rug.ac.be`

A two-graph (Ω, Δ) is a pair of a finite vertex set Ω and a block set Δ which is a subset of the set of 3-subsets of Ω, such that each 4-subset of Ω contains an even number of blocks. Let ρ be a Hermitian polarity in $\mathrm{PG}(2, q^2)$, q an odd prime power, with associated Hermitian form H and set of absolute points $\mathcal{U}$. The Hermitian two-graph is defined as follows: the point set is $\mathcal{U}$, and a triple $\{x, y, z\}$ is a block iff $H(x, y)H(y, z)H(z, x)$ is a square, respectively a non-square, if $q \equiv -1 \pmod 4$, respectively $q \equiv 1 \pmod 4$. We give a geometric construction for the Hermitian two-graph for certain values of q. In the case $q = 3^h$, $h \in \mathbb{N}$, we use the representation of $\mathcal{U}$ on the parabolic quadric $Q(6, q)$. If q is prime, a geometric description arises from the study of the automorphism group of the two-graph.

Constructing Graphs with Several Pseudosimilar Vertices or Edges

Josef Lauri

Department of Mathematics - University of Malta
e-mail: jlau@um.edu.mt

Some of the most interesting problems connected with pseudosimilarity in graphs concern the construction of graphs with large sets of pseudosimilar vertices or edges. This can be understood in two ways: Either the graph contains a large set of vertices or edges which are mutually pseudosimilar or else for every vertex (edge) in the graph there is another vertex (edge) to which it is pseudosimilar. We shall survey the methods used to construct such graphs and on the way we shall also discuss some related results and point out some unanswered questions.

1 Introduction

All graphs considered will be finite, simple and undirected, unless otherwise stated. The vertex-set and the edge-set of a graph G are denoted by $V(G)$ and $E(G)$, respectively. If v is a vertex in G, then $G - v$ denotes the subgraph of G obtained by removing v and all edges incident to v; if e is an edge of G then $G - e$ denotes the subgraph obtained by removing the edge e.

Two vertices u, v in a graph G are said to be *similar* if there is an automorphism of G which maps u into v. The vertices u, v are said to be *removal-similar* if the subgraphs $G - u$ and $G - v$ are isomorphic. If u and v are removal-similar but not similar, then they are called *pseudosimilar*. In this case we sometimes say that v is a *pseudosimilar mate* of u and vice-versa. If $S \subset V(G)$ such that any two vertices in S are pseudosimilar mates, then we say that the vertices of S are *mutually pseudosimilar* in G.

Pseudosimilar edges are similarly defined, as are the terms pseudosimilar mates for pairs of edges and mutually pseudosimilar for sets of edges.

The reason why pairs of pseudosimilar vertices arise is quite well understood in terms of a sort of truncation of cyclic symmetry. Thus, take a graph H with vertices u and v and an automorphism α of H such that $\alpha^t(u) = v$ for some

$t > 1$ and $\alpha^r(u) \neq v$ for $1 \leq r < t$. Then u and v are removal-similar in $G = H - \{\alpha(u), \ldots, \alpha^{t-1}(u)\}$; if moreover they also happen to be not similar, then we have a pair of pseudosimilar vertices. Godsil and Kocay [7] showed that, in fact, every pair of pseudosimilar vertices can be obtained this way.

Theorem 1 ([7]) *Let u and v be two pseudosimilar vertices in a graph G. Then G is an induced subgraph of some graph H such that H has an automorphism α with $\alpha(G - v) = G - u$ and $\alpha^t(u) = v$, and such that $V(H) - V(G) = \{x_1, \ldots, x_r\}$, where $x_i = \alpha^{t+i}(u)$ and $\alpha(x_r) = u$.*

Therefore the most interesting questions and constructions involve graphs with several pseudosimilar vertices or edges. The two situations we shall be investigating are the construction of graphs in which every vertex (edge) has a pseudosimilar mate and graphs with large sets of mutually pseudosimilar vertices (edges).

A general survey about pseudosimilarity can be found in [18]. Some work presented here has been carried out since the publication of that survey. Graph theoretic terms used but not defined in this paper are standard and can be found in any graph theory text such as [9].

2 Every vertex can have a pseudosimilar mate: The KSS construction.

The question of whether or not in a graph every vertex can have a pseudosimilar mate has been settled since 1981 [12]. The solution to this question turns out to be a simple corollary of the solution to another problem about symmetries of graphs, namely the construction of *graphical regular representations (GRR)* of groups of odd order. A graph G is said to be a GRR of a group Γ if $\mathrm{Aut}(G) \simeq \Gamma$ and $\mathrm{Aut}(G)$ acts regularly on $V(G)$, that is, it is transitive on $V(G)$ and the stabiliser of any $v \in V(G)$ is trivial. Except for a finite number of known groups, all finite, nonabelian groups which are not generalised dicyclic groups have GRRs. A number of authors contributed towards obtaining this result, but here we shall only be requiring GRRs for groups of odd order (it follows, see [2] for example, that such groups must be nonabelian).

Theorem 2 ([10]) *Except for one group of order 27, all nonabelian groups of odd order have GRRs.*

Using the existence of GRRs for groups of odd order enabled Kimble, Schwenk and Stockmeyer to construct graphs in which every vertex has a pseudosimilar mate.

Theorem 3 ([12]) *There are infinitely many graphs in which every vertex has a pseudosimilar mate.*

Proof Let Γ be a group of odd order and let H be a GRR of Γ. We note that, since the stabiliser of any vertex of H under the action $\mathrm{Aut}(H) \simeq \Gamma$ is the identity element of Γ, it follows that if r is any vertex of H, then $G = H - r$ has the identity automorphism group.

Now, let v be any vertex in G. There is an automorphism α of H mapping r to v. The vertices $\alpha^{-1}(r)$ and $v = \alpha(r)$ are distinct, because otherwise α would contain a cycle of length 2, which is impossible since Γ has odd order. Since α^{-1} maps $\{v, r\}$ onto $\{r, \alpha^{-1}(r)\}$, it follows that $G - v = H - r - v \simeq H - \alpha^{-1}(r) - r = G - \alpha^{-1}(r)$; that is, $v = \alpha(r)$ and $\alpha^{-1}(r)$ are removal-similar in G. But G has the identity automorphism group, therefore v and $\alpha^{-1}(r)$ are pseudosimilar. $\square$

We shall refer to this construction as the *KSS construction.* In [12], Kimble, Schwenk and Stockmeyer also gave some nice examples illustrating the use of the above theorem.

One question which the above result brings up is whether or not the KSS construction is the only one which gives graphs all of whose vertices have pseudosimilar mates.

Question 1 *Is there a characterisation analagous to Theorem 1 of graphs all of whose vertices have a pseudosimilar mate? If in a graph G all vertices have a pseudosimilar mate, is it always possible to extend G to a vertex-transitive graph by adding only one new vertex? In particular, are all such graphs obtainable via the KSS construction?*

3 Every edge can have a pseudosimilar mate: Adapting the KSS construction.

Finding graphs in which every edge has a pseudosimilar mate proved to be more elusive. First attempts [11, 18] only managed to show that there are families of graphs of order n such that, as n increases, the proportion of edges in the graph having a pseudosimilar mate tends to 1. However, in 1996, using graphs constructed by Alspach and Xu [1], Lauri and Scapellato [21] proved the following.

Theorem 4 ([21]) *There are infintely many graphs in which every edge has a pseudosimilar mate.*

The idea is to adapt the KSS construction as follows. Let H be a graph with an odd number of edges and whose automorphism group acts regularly on its edge-set. Then, as in Theorem 3, deleting from H any edge gives a graph all of whose edges have a pseudosimilar mate.

The problem is to find such graphs H. Families of graphs with these properties were, in fact, constructed in [1] and a special case of this family can be described as Cayley graphs in the following way. (We recall that, if Γ is a group and $S \subset \Gamma$ with $S^{-1} = S$, $1 \notin S$ and $\Gamma = \langle S \rangle$, then the *Cayley graph* $\mathrm{Cay}(\Gamma, S)$ is the graph with vertex-set equal to Γ and in which two vertices x, y are adjacent if and only if $y = xs$ for some $s \in S$.)

Let p be a prime number with $p \equiv 1 \mod 3$ and $p \equiv 1 \mod 5$. Let Γ_{3p} be the group defined by

$$\Gamma_{3p} = \langle b, c | b^3 = c^p = 1, c^b = b^{-1}cb = c^r \rangle$$

where r is such that $r^3 = 1 \mod 3$. Let t be such that $t^5 = 1 \mod p$, and let a be the automorphism of Γ_{3p} defined by $b^a = b$ and $c^a = c^t$. Let

$$T = \{c^a, c^{a^2}, c^{a^3}, c^{a^4}, c^{a^5} = c\}$$

and

$$S = bT \cup T^{-1}b^{-1} = bT \cup T^{-1}b^2.$$

Let H_{3p} be the Cayley graph $\mathrm{Cay}(\Gamma_{3p}, S)$.

Theorem 5 ([1]) *The automorphism group of the Cayley graph H_{3p} constructed above acts regularly on its edge-set.*

This Cayley graph has order $3p$ and degree 10, therefore it has an odd number, $15p$, of edges, as required. Also, by Dirichlet's Theorem on primes in an arithmetic progression (see [4], for example), there is an infinite number of primes in the arithmetic progression $\{1 + 15k : k = 0, 1, 2, \dots\}$ and therefore an infinite number of Cayley graphs H_{3p} can be constructed as above. This therefore proves Theorem 4.

The smallest value of p for which the above construction works is $p = 31$ giving a Cayley graph with 465 edges and therefore a graph with 464 edges, all of them paired by pseudosimilarity.

In the above construction, the Cayley graphs H_{3p} are all $\frac{1}{2}$-transitive, that is, the automorphism group is transitive on the vertices and the edges, but not on the directed arcs. Since what we need is a graph whose automorphism group acts regularly on its edges, one question which arises following the previous construction is whether or not it is possible to obtain a graph which is not vertex-transitive but whose automorphism group has the required action on the edge-set—such a graph would, of course, have to be bipartite. A graph of this type was constructed in [19] and we shall now briefly describe it.

We first give a few general definitions and results. The motivating idea behind these is the well-known characterisation, due to Sabidussi [23], of vertex-transitive graphs in terms of coset graphs.

Let Γ be a group and $\mathcal{H}, \mathcal{K}$ two subgroups of Γ. Let S be a subset of Γ. Define the graph $\mathrm{Cos}(\Gamma, \mathcal{H}, \mathcal{K}, S)$ as follows: Its vertices are the left cosets of $\mathcal{H}$ and of $\mathcal{K}$; two cosets $x\mathcal{H}$ and $y\mathcal{H}$ are adjacent if and only if $y^{-1}x \in \mathcal{K}S\mathcal{H}$. If, moreover, $S \subseteq \mathcal{K}\mathcal{H}$, that is, $\mathcal{K}S\mathcal{H} = \mathcal{K}\mathcal{H}$, then we denote $\mathrm{Cos}(\Gamma, \mathcal{H}, \mathcal{K}, S)$ simply by $\mathrm{Cos}(\Gamma, \mathcal{H}, \mathcal{K})$.

If $\mathcal{H} \cap \mathcal{K} = \{1\}$, then any two cosets $x\mathcal{H}$, $y\mathcal{K}$ are either disjoint or have exactly one element in common. In this case, $x\mathcal{H}$ and $y\mathcal{K}$ are adjacent in $\mathrm{Cos}(\Gamma, \mathcal{H}, \mathcal{K})$ if and only if they are not disjoint, that is, all edges of $\mathrm{Cos}(\Gamma, \mathcal{H}, \mathcal{K})$ are of the form $\{t\mathcal{H}, t\mathcal{K}\}$, where t is the element common to both cosets. Another useful way to look at adjacencies in $\mathrm{Cos}(\Gamma, \mathcal{H}, \mathcal{K})$ when $\mathcal{H} \cap \mathcal{K}$ is trivial is as follows: The coset $x\mathcal{H}$ is adjacent to all the cosets $xh\mathcal{K}$, for all $h \in \mathcal{H}$ (all these cosets are distinct); similarly, the coset $y\mathcal{K}$ is adjacent to all the cosets $yk\mathcal{H}$ for all $k \in \mathcal{K}$. Clearly, the degrees of the cosets $x\mathcal{H}$ and $y\mathcal{K}$ as vertices in $\mathrm{Cos}(\Gamma, \mathcal{H}, \mathcal{K})$ are $|\mathcal{H}|$ and $|\mathcal{K}|$, respectively.

The following two results are not difficult to prove.

Theorem 6 *Let G be a graph whose vertex-set is partitioned into two orbits V_1, V_2 under the action of the automorphism group Γ. Let $\mathcal{H}$ be the stabiliser of the vertex $u \in V_1$ and $\mathcal{K}$ the stabiliser of the vertex $v \in V_2$. Let S be the set of all those permutations $\alpha \in \Gamma$ such that $\alpha(u)$ is adjacent to v. Then G is isomorphic to Cos$(\Gamma, \mathcal{H}, \mathcal{K}, S)$. Moreover, if G is edge-transitive then $S \subseteq \mathcal{K}\mathcal{H}$, that is, G is isomorphic to Cos$(\Gamma, \mathcal{H}, \mathcal{K})$.*

Theorem 7 *Let $G =$ Cos$(\Gamma, \mathcal{H}, \mathcal{K})$. For $t \in \Gamma$, let λ_t denote the action of left translation by t on the left cosets of $\mathcal{H}$ and $\mathcal{K}$. Then λ_t is an automorphism of G; this action is transitive on the edges of G. Suppose ϕ is an automorphism of Γ which fixes setwise both $\mathcal{H}$ and $\mathcal{K}$. Let $\hat{\phi}$ denote the induced action on the cosets of $\mathcal{H}$ and $\mathcal{K}$. Then $\hat{\phi}$ is an automorphism of the graph G.*

From these two theorems it is clear that to obtain a graph whose automorphism group acts regularly on the edges but non-transitively on the vertices we need to find a coset graph $\mathrm{Cos}(\Gamma, \mathcal{H}, \mathcal{K})$ such that no automorphism of the group fixes $\mathcal{H}$ and $\mathcal{K}$. Of course we also require the graph to be connected, therefore $\mathcal{H} \cup \mathcal{K}$ must generate all of Γ. We can now describe the graph constructed in [19].

Let Ξ be the group of order $3 \cdot 5 \cdot 31$ defined as follows

$$\Xi = \langle a, w, c | a^5 = w^3 = c^{31} = 1, wa = awc, ca = ac^2, cw = wc^{25} \rangle.$$

Now let $\mathcal{H}$ be the cyclic subgroup generated by a and let $\mathcal{K}$ be the cyclic subgroup generated by w. Let $H = \mathrm{Cos}(\Gamma, \mathcal{H}, \mathcal{K})$. This graph is edge-transitive but not vertex-transitive since the cosets of $\mathcal{H}$ have degree 5 whereas the cosets of $\mathcal{K}$ have degree 3. Moreover, it is not difficult to check that no nontrivial automorphism of the group Γ fixes $\mathcal{H} \cup \mathcal{K}$, therefore there is reason to hope that, in fact, the full automorphism group of H is Ξ, that is, the automorphism group of H acts regularly on the edges. For this it is required to show that the stabiliser of any edge is trivial.

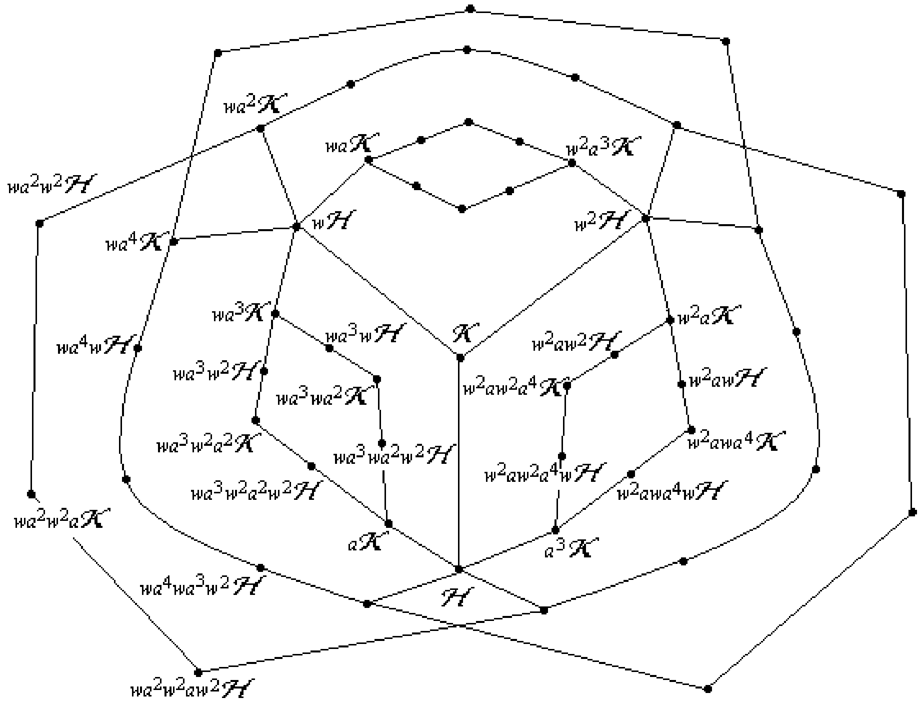


Figure 1: All the 8-cycles passing through the edges incident to $\mathcal{K}$

It turns out that the girth of H is 8 and that there are exactly eight cycles of length 8 containing any edge. A detailed consideration of these possible cycles leads to Figure 1, which shows all the 8-cycles passing through any of the three edges incident to $\mathcal{K}$ (and also the names of some of the vertices). By a more detailed consideration of the configuration shown in Figure 1 and using the fact that H is edge-transitive it is shown in [19] that if an automorphism of H fixes the edge $\{\mathcal{H}, \mathcal{K}\}$ then it must be trivial, as required.

The graph H in this last construction has 248 vertices and 465 edges, and therefore this again gives a graph with 464 edges all of which are paired by pseudosimilarity. The following question therefore naturally arises.

Question 2 *Are there graphs with less than 464 edges in which every edge has a* *pseudosimilar mate?*

Also, the non-vertex-transitive graph whose automorphism group acts regularly on its edges, and which was used in the previous construction, could very well be the first such graph in an infinite family, analogous to $H_{3p}, p = 31$, for Theorem 5. Therefore one can ask,

Question 3 *Find an infinite family of graphs which are not vertex-transitive but whose automorphism groups act regularly on the respective edge-sets.*

Finally, one can ask for pseudosimilar edges a question analogous to Question 1 of the previous section.

Question 4 *Is there a characterisation, analogous to Theorem 1, of graphs all of whose vertices have a pseudosimilar mate? Are all such graphs obtainable via the KSS construction adapted for edges?*

4 Cayley line-graphs

Whereas the problem of constructing graphs in which every vertex has a pseudosimilar mate turned out to be an easy application of the existence of GRRs for finite groups of odd order, the analogous problem for pseudosimilar edges was more difficult because there it was not sufficient to know that a group had a GRR; the GRR had to have some particular structure—not any GRR of the group would do.

The situation is perhaps best understood in terms of line-graphs, for now, since we are looking for a graph H whose automorphism group acts regularly on its edge-set, the line graph $L(H)$ is a GRR of its automorphism group (which is isomorphic to $\mathrm{Aut}(H)$). Therefore $L(H)$ is a Cayley graph of $\mathrm{Aut}(H)$ (see [2], for example). Hence we are now looking for particular Cayley graphs, namely those which are line-graphs.

It is therefore natural to ask, in this context, what form the set S must take for the Cayley graph $\mathrm{Cay}(\Gamma, S)$ to be a line graph. The answer is given by the next theorem.

Theorem 8 *Let Γ be a finite group and let $S \subseteq \Gamma$ with $S^{-1} = S$, $1 \notin S$ and $\Gamma = \langle S \rangle$. Let $S^* = S \cup \{1\}$. Then $G = Cay(\Gamma, S)$ is a line-graph if and only if $S^* = S_1 \cup S_2$ such that:*

1. *$S_1 \cap S_2 = \{1\}$,* **and**

2. **either** *both S_1 and S_2 are subgroups of Γ,*

3. **or else** $S_1 = \mathcal{H} \cup \mathcal{H}a$ *and* $S_2 = a^{-1}\mathcal{H}a \cup a^{-1}\mathcal{H}$*, for some* $\mathcal{H} \leq \Gamma$ *and* $a \in \Gamma$ *with* $\mathcal{H} \cap a^{-1}\mathcal{H}a = \{1\}$*.*

Proof We first recall the characterisation of line-graphs in terms of the Krausz decomposition of its edge-set (see [9]), namely, that a 2-connected graph (as is our Cayley graph G since it is vertex-transitive) is a line-graph if and only if its edges can be partitioned so that the edges in each part induce a complete graph and every vertex is incident to edges from exactly two parts of the partition. In the case of G (again since it is vertex-transitive) it is a line-graph if and only if the neighbours of one of its vertices v_0 together with v_0 induce two complete graphs which intersect only in v_0. We can take v_0 to be the vertex 1, whose set of neighbours is S. Therefore G is a line-graph if and only if $S^* = S_1 \cup S_2$ such that

(i) $S_1 \cap S_2 = \{1\}$, and

(ii) if $s_1, s_2 \in S^*$ then $s_1^{-1}s_2 \in S^*$ if and only if both s_1 and s_2 are in S_1 or S_2.

If Condition 1 and one of Conditions 2 or 3 of the theorem hold, then so do Conditions (i) and (ii), that is, G is a line-graph. Therefore, for the converse, suppose G is a line-graph, that is, Conditions (i) and (ii) hold. In the sequel, for $x, y \in S^*$ we shall use the notation $x \sim y$ to denote that x and y are both in S_1 or in S_2.

We now make two observations:

Observation 1.

Suppose S_i ($i = 1$ or 2) contains two subgroups $\mathcal{A}, \mathcal{B}$ of Γ. Then S_i also contains the subgroup $\mathcal{C} = \langle \mathcal{A} \cup \mathcal{B} \rangle$ generated by $\mathcal{A} \cup \mathcal{B}$. For, by (ii) and since each of $\mathcal{A}, \mathcal{B}$ contains the inverse of each of its elements, we have that for all $a \in \mathcal{A}$ and $b \in \mathcal{B}$, the elements $ab = (a^{-1})^{-1}b$ and $ba = (b^{-1})^{-1}a$ are both in S^*. Moreover, since $a^{-1}(ab)$ and $b^{-1}(ba)$ are in S^* and $a, b \in S_i$, then, by (ii), ab and ba are also in S_i. Therefore, if an element like $w = a_1b_2a_3 \dots a_{n-1}b_n$ is a product of elements $a_i \in \mathcal{A}, b_j \in \mathcal{B}$, we can show that $w \in S_i$ by induction on n: since a_1^{-1} and $b_2a_3 \dots a_{n-1}b_n$ are both in S_i then $w = (a_1^{-1})^{-1}b_2a_3 \dots a_{n-1}b_n$ is in S^*; also, since $a_1 \in S_i$ and $a_1^{-1}w$ is in S^*, then w is also in S_i, by (ii).

Therefore S_i contains a subgroup of Γ which is maximal in the sense that it contains every subgroup of Γ found in S_i. We denote this maximal subgroup by $\mathcal{H}_i$.

Observation 2.

Each S_i is the union of right cosets of $\mathcal{H}_i$. For, let $g \in S_i$. Then, for any $h \in \mathcal{H}_i$, $h^{-1}g \in S^*$, that is, $\mathcal{H}_i^{-1}g = \mathcal{H}_ig \subset S^*$. But, for any $h_1 \in H_i$ and $h_2g \in H_ig$, we have that $h_1^{-1}h_2g \in S^*$. Therefore h_2g must be in S_i, that is, $\mathcal{H}_ig \in S_i$. However, $g \in \mathcal{H}_ig$, that is, any element of S_i is in some right coset of $\mathcal{H}_i$.

We now claim that any two elements of S_i not contained in $\mathcal{H}_i$ must be in the same right coset of $\mathcal{H}_i$.

Consider, without loss of generality, S_1. Let $x, y \in S_1, x \neq y$ and let $x^{-1}y = z \in S^*$. From the relation $xz = y$ and $yz^{-1} = x$ it follows that $x^{-1} \sim z$ and $y^{-1} \sim z^{-1}$. There are now four cases to consider. (Note that below we use the fact that if both a and a^{-1} are in S_i then so is $\langle a \rangle$.)

Case I: $z \in S_1$.

Case I.1: $z^{-1} \in S_1$.

Therefore $x^{-1}, y^{-1} \in S_1$, and so, $\langle x \rangle$ and $\langle y \rangle$ are in S_1. Therefore all pairs of elements $x, y \in S_1$ such that $x^{-1}y = z \in S_1$ with z^{-1} also in S_1 must be in $\mathcal{H}_1$.

Case I.2: $z^{-1} \in S_2$.

Therefore $\langle x \rangle \subset S_1$ and so $x \in \mathcal{H}_1$. Moreover, $y^{-1} \notin S_1$, therefore $y \notin \mathcal{H}_1$, that is, y is in a nontrivial coset $\mathcal{H}_1 y$ of H_1 contained in S_1.

Case II: $z \in S_2$.

Case II.1: $z^{-1} \in S_1$.

Therefore $y, y^{-1} \in S_1$, that is, $\langle y \rangle \subset S_1$. Again, $y \in \mathcal{H}_1$ and x is in a nontrivial right coset $\mathcal{H}_1 x$ contained in S_1.

Case II.2: $z^{-1} \in S_2$.

Therefore $x^{-1}, y^{-1} \in S_2$. Consider $xy^{-1} = (x^{-1})^{-1}y^{-1} \in S$. But $x^{-1} \cdot xy^{-1} = y^{-1}$§. Therefore $x \sim xy^{-1}$, that is, $xy^{-1} \in S_1$. Similarly, yx^{-1} S_1. Therefore S_1 contains $\langle xy^{-1} \rangle \leq \mathcal{H}_1$. Therefore x, y are in non-trivial cosets of $\mathcal{H}_1$ (nontrivial since $x^{-1}, y^{-1} \notin S_2$). But $\mathcal{H}_1 y$ contains $xy^{-1} \cdot y = x$, that is, x and y are in the same nontrivial right coset of $\mathcal{H}_1$.

This proves our claim, and hence we can say that $S_1 = \mathcal{H}_1$ or $S_1 = \mathcal{H}_1 \cup \mathcal{H}_1 a$ and similarly $S_2 = \mathcal{H}_2$ or $S_2 = \mathcal{H}_2 \cup \mathcal{H}_2 b$. If $S_1 = \mathcal{H}_1$ and $S_2 = \mathcal{H}_2$ then we are done. So, suppose $S_1 = \mathcal{H}_1 \cup \mathcal{H}_1 a$ with $a \notin \mathcal{H}_1$. Therefore $a^{-1} \notin S_1$, otherwise $\langle a \rangle \subset S_1$ and a would therefore be in $\mathcal{H}_1$.

Hence $a^{-1} \in S_2$, and since $a^{-1} \notin \mathcal{H}_2$ then $a^{-1} \in \mathcal{H}_2 b$, which is therefore $H_2 a^{-1}$. That is, $S_2 = \mathcal{H}_2 \cup \mathcal{H}_2 a^{-1}$.

Now, for all $g \in \mathcal{H}_1 a$, g^{-1} is in S_2 but not in $\mathcal{H}_2$ (since $g \notin S_2$). Therefore $g^{-1} \in \mathcal{H}_2 a^{-1}$, so that $(\mathcal{H}_1 a)^{-1} \subseteq \mathcal{H}_2 a^{-1}$. Similarly, $(\mathcal{H}_2 a^{-1})^{-1} \subseteq \mathcal{H}_1 a$. Therefore $(\mathcal{H}_1 a)^{-1} = a^{-1}\mathcal{H}_1 = \mathcal{H}_2 a^{-1}$, hence $H_2 = a^{-1}\mathcal{H}_1 a$. Therefore $S_1 = \mathcal{H}_1 \cup \mathcal{H}_1 a$ and $S_2 = a^{-1}\mathcal{H}_1 a \cup a^{-1}\mathcal{H}_1$, as required. □

(The line-graph of the Cayley graph H_{3p} for $p = 5$ considered in the previous section is, in fact, the Cayley graph $\mathrm{Cay}(\Xi, S)$ (where Ξ is the group considered later in the same section) with $S^* = \mathcal{H} \cup \mathcal{H}w \cup w^{-1}\mathcal{H}w \cup w^{-1}\mathcal{H}$, where $\mathcal{H} = \langle a \rangle$.)

The problem of finding a graph whose automorphism group acts regularly on its edges can therefore be regarded as a problem of finding a Cayley graph $\mathrm{Cay}(\Gamma, S)$ which is a GRR and such that S has the special form described in the previous theorem. From this theorem, the simplest way to guarantee that $\mathrm{Cay}(\Gamma, S)$ is a line-graph is to let $S = \mathcal{H} \cup \mathcal{K} - \{1\}$ where $\mathcal{H}, \mathcal{K}$ are subgroups of Γ with trivial intersection. (In this case, if $\mathrm{Cay}(\Gamma, S)$ is the line-graph $L(H)$ of H then H is the graph $\mathrm{Cos}(\Gamma, \mathcal{H}, \mathcal{K})$ as defined in the previous section.)

Now, for the Cayley graph to be a GRR it is necessary that no automorphism of Γ fixes S. This necessary condition is not, in general, sufficient. The following result of Godsil [6], however, affirms that for a wide class of p-groups this simple condition is also sufficient to guarantee that the Cayley graph is a GRR.

Theorem 9 ([6]) *Let Γ be a finite p-group which admits no homomorphism onto the wreath product of $\mathbb{Z}_p$ by $\mathbb{Z}_p$. Let $S \subset \Gamma$, $S = S^{-1}$ and $\Gamma = \langle S \rangle$ such that no nontrivial automorphism of Γ fixes S. Then the Cayley graph Cay(Γ, S) is a GRR of Γ.*

Godsil's theorem and the above discussion have led Lauri and Scapellato [21] to pose the following question:

Question 5 *Does there exist a p-group Γ (p an odd prime) having two subgroups $\mathcal{H}, \mathcal{K}$ with the following properties: (i) $\mathcal{H} \cap \mathcal{K} = \{1\}$, (ii) $\Gamma = \langle \mathcal{H} \cup \mathcal{K} \rangle$, and (iii) no nontrivial automorphism of Γ fixes $\mathcal{H} \cup \mathcal{K}$ setwise?*

If Γ is not a p-group then finding such subgroups is possible. For example, if Ξ is again the group defined in the previous section, then it is routine to check that the subgroups $\mathcal{H} = \langle a \rangle$ and $\mathcal{K} = \langle w \rangle$ have the required properties.

We were, however, been unable to find even any nilpotent group which has two such subgraphs—nilpotent groups might therefore be the right class of group to look at if one is trying to show that the answer to the above question is negative.

5 Sheehan's fixing subgraphs

The idea of fixing subgraphs was introduced by John Sheehan in [25, 26, 27]. Since then it has turned out that fixing subgraphs are important in many areas of graph theory—an excellent survey of this development is given by [24]. We shall here point briefly to the connection between fixing subgraphs and pseudosimilarity, focusing in particular on a consequence of Theorem 4.

A spanning subgraph U of a graph G is termed a *fixing subgraph* of G if G contains exactly $|\mathrm{Aut}(G)|/|\mathrm{Aut}(G) \cap \mathrm{Aut}(U)|$ subgraphs isomorphic to U (the graph G must contain at least this number). If, in addition, $\mathrm{Aut}(U) \leq \mathrm{Aut}(G)$ then U is called a *strong fixing subgraph* of G. Let $F(G)$ ($F^*(G)$) be the set of fixing (strong fixing) subgraphs of G.

The connection with pseudosimilarity is that if an edge e has a pseudosimilar mate then the spanning subgraph $G - e$ cannot be in $F^*(G)$. As a direct corollary of Theorem 4 Sheehan proves,

Theorem 10 ([24]) *There are infinitely many graphs G such that*

(i) $G - e \notin F^*(G)$ *for all* $e \in E(G)$, *and*

(ii) $|F^*(G)| = 1$.

6 Large sets of mutually pseudosimilar vertices or edges

With the settling of the question of the existence of graphs in which every edge has a pseudosimilar mate, the most interesting and difficult problem in pseudosimilarity would now seem to be the following.

Question 6 *In a graph G of order n, what is the largest possible size k of a set of mutually pseudosimilar vertices? Alternatively, given k, what is the smallest graph which contains k mutually pseudosimilar vertices? What is the answer for the analogous questions on mutually pseudosimilar edges?*

This seems to be a very difficult question. We shall here review some constructions which attempt to pack as many as possible mutually pseudosimilar vertices (or edges) in a graph of order n. It is clear that not all of $V(G)$ can be mutually pseudosimilar, for such a graph G would be regular and an isomorphism from $G - u$ to $G - v$ could therefore be extended to an automorphism of G mapping u into v. With slightly more work one can also show that k must be less than $n - 1$. Also, this question has been resolved for trees (in [5] it is shown that $k < 3$ for any tree), for $k = 2$ ([7]; G must have order at least 6) and, it seems, for $k = 3$ (in [13] a graph on 17 vertices with three mutually pseudosimilar vertices is constructed, and this seems to be the smallest possible graph for $k = 3$).

The difficulty of Question 6 and these partial results suggest two questions.

Question 7 *Are there other interesting classes $\mathcal{C}$ of graphs such that, for any graph G in $\mathcal{C}$, the number of mutually pseudosimilar vertices in G must be less than some constant?*

Question 8 *Verify that a graph with $k = 3$ mutually pseusosimilar vertices must have order at least 17. What would be the analogous result for $k = 4$?*

But now we shall be considering sequences of graphs for which k, the number of mutually pseudosimilar vertices, increases without bound.

The simplest way [12] obtain such a sequence is to start with the transitive tournament T_k on k vertices (that is, the tournament with vertex-set $\{1, 2, \ldots, n\}$ in which i dominates j if and only if $i < j$). Clearly the vertices of T_k are all mutually pseudosimilar, but the tournament has to be transformed into an undirected graph while preserving the pseudosimilarity of its vertices. This process is illustrated for T_4 in Figure 2.

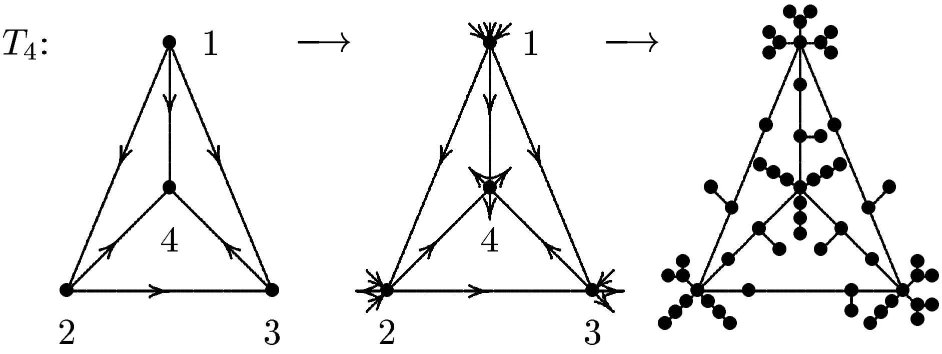


Figure 2: Transforming T_4 into a graph with 4 mutually pseudosimilar vertices

This construction gives a sequence of graphs G_k having k mutually pseudosimilar vertices and order $O(k^2)$.

Another general construction for creating a sequence of graphs with large sets of mutually pseudosimilar vertices runs as follows:

> Let G' be a graph containing r endvertices, all of which are mutually pseudosimilar. Let G be the graph obtained from G' by removing all its endvertices, and let R be the set of neighbours of the endvertices of G'—since no two endvertices are similar, no two can share a common neighbour, therefore $|R| = r$. Let X be the set of all those vertices of G which are in the same orbit as some vertex in R under the action of Aut(G). We now construct a sequence of graphs G_t, $t = 1, 2, \ldots$, containing r^t mutually pseudosimilar endvertices. Let $G_1 = G'$ and let H_1 be G_1 less one of its endvertices. Having constructed G_t, let H_t be G_t less one of its *pseudosimilar* endvertices. Then, G_{t+1} is obtained by attaching a copy of G_t to each vertex in R and a copy of H_t to each of the other vertices in $X - R$. (By attaching a copy of G_t (or H_t) to a vertex v of G we mean joining v to every vertex of G_t (or H_t) which is *not* an endvertex.)
>
> Each graph G_t so obtained has r^t mutually pseudosimilar endvertices and $O(|X|^t)$ vertices. Therefore if $k = r^t$ is the number of pseudosimilar endvertices, then the total number of vertices in G_t is $O(k^{\log |X| / \log |R|})$.

(Since the pseudosimilar vertices resulting from this construction are endvertices, that is, vertices of degree 1, the edges incident to these endvertices are also mutually pseudosimilar.)

The crucial step in the above construction is finding the starting graph G', that is, one with endvertices all of which are mutually pseudosimilar. We shall describe different methods which have been employed in order to do this.

Krishnamoorthy and Parthasarathy [16] started with the tournament on three vertices forming a directed cycle. If an endvertex is attached to two vertices of the tournament and the arcs are transformed into edges using "gadgets" as in the proof of Frucht's Theorem, then the two endvertices are pseudosimilar and the resulting graph $G' = G_1$ can be used as the base graph in the above construction. The graph G_2 obtained in this sequence, containing $2^2 = 4$ mutually pseudosimilar vertices, is shown in Figure 3. Starting with this base graph therefore gives a sequence of graphs G_t with $k = 2^t$ mutually pseudosimilar endvertices and order $O(k^{\log 3/\log 2})$.

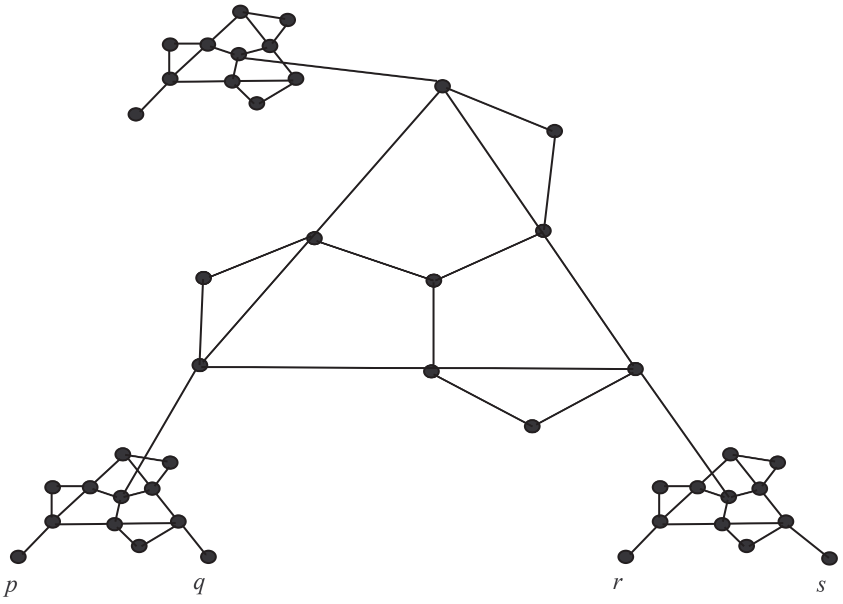


Figure 3: The graph G_2 with 2^2 mutually pseudosimilar vertices p, q, r, s

In [20] a different starting graph was used by exploiting the arc homogeneous property of the quadratic residue tournaments. Thus, consider $QT(7)$, the quadratic residue tournament on seven vertices (that is, the tournament with vertex-set $\{1, 2, \ldots, 7\}$ such that (i, j) is an arc if and only if $j - i$ is a nonzero square modulo 7). The vertices $1, 2, 3$ form a transitive subtournament of $QT(7)$ so that if an endvertex is joined to each of $1, 2, 3$ and the arcs of the tournament are transformed into edges by means of appropriate gadgets, then we get the graph $G' = G_1$ with three endvertices all of which are pseudosimilar. The above construction then yields a sequence of graphs G_t with $k = 3^t$ mutually pseudosimilar endvertices and order $O(k^{\log 7/\log 3})$, which is better than the construction of Kimble, Schwenk and Stockmeyer using transitive tournaments, but not as good as the construction of Krishnamoorthy and Parathasarthy.

The problem of finding a base graph G' as the starting graph of the above construction can be described in terms of permutation groups. Suppose Γ is a group of permutations acting on some set X such that, for some $R \subset X$, the following two conditions hold: (i) the setwise stabiliser $\Gamma_{\{R\}}$ of R is the identity and, (ii) for any two $(|R|-1)$-subsets A, B of R, there is a permutation α in Γ such that $\alpha(A) = B$. Then, by a result of Bouwer [3], one can construct a graph G with minimum degree at least 2 and $X \subseteq V(G)$ and whose automorphism group is isomorphic to Γ and such that X is invariant under the action of $\mathrm{Aut}(G)$ and also $\mathrm{Aut}(G)$ has the same action as Γ on X. Therefore if we attach one endvertex to each vertex of $R \subset V(G)$ we obtain the starting graph G' all of whose endvertices are mutually pseudosimilar. Hence such starting graphs can be constructed if permutation groups satisfying conditions (i) and (ii) are found.

In [17] such a permutation group with $|X| = 8$ and $|R| = 4$ was constructed. Let Γ be the group of affine transformations on the field $GF(8)$. This group is not 3-transitive but it is 3-homogeneous [22] (that is, any two 3-sets are similar under the action of Γ). Therefore all we need is a 4-set R such that $\Gamma_{\{R\}}$ is trivial. If we represent $GF(8)$ as $\mathbb{Z}_2[x]/p(x)$, where $p(x)$ is the primitive, irreducible (over $\mathbb{Z}_2$) polynomial $x^3 + x + 1$, and if we let $R = \{0, 1, x, x^2\}$, then one can easily check that the only permutation in Γ which fixes R setwise is the identity.

This then gives a starting graph G' with 4 endvertices all mutually pseudosimilar, and therefore a sequence of graphs G_t with $k = 4^t$ mutually pseudosimilar endvertices and order $O(k^{3/2})$. Till now, this sequence seems to be the one which gives the best "packing" of mutually pseudosimilar vertices.

In [17] there is also described a construction which produces, for all r, a graph containing r endvertices *all* of which are mutually pseudosimilar. However, this construction requires that $|X| = O(|R|^{2|R|})$ and it therefore does not solve the problem of obtaining as dense a packing of mutually pseudosimilar vertices as possible.

In [17] it is also shown that a permutation group satisfying Conditions (i) and (ii) above must have $|X| \geq 2|R|-1$. Therefore the above construction can, at best, produce a sequence of graphs G_t with $k = r^t$ mutually pseudosimilar endvertices and order $O(k^{\log(2r-1)/\log r})$.

The above constructions suggest the following questions, the first two of which are restricted versions of Question 6. In view of the preceding comments, a positive answer to Question 9 would require a totally different construction from the one we have been discussing. The constructions used in [8, 13] employ Cayley graphs and exploit the equivalence of the action of a permutation group Γ on a set X with its action on the set of cosets of a stabiliser. In [15], Kocay, Niesink and Zarnke systematically search for groups Γ with a subgroup $\mathcal{K}$ such that the action of Γ on the cosets of $\mathcal{K}$ can be used to construct graphs with $4 \geq k \geq 2$ pseudosimilar vertices. Perhaps these methods need to be investigated and extended further in order to tackle this problem.

Question 9 *Is it possible to construct a sequence of graphs $\langle G_k \rangle$ such that G_k has k mutually pseudosimilar vertices and order $O(k)$?*

Question 10 *Given k, what is the smallest graph which contains k endvertices* **all** *of which are mutually pseudosimilar?*

The next question asks whether there are tournaments which extend the arc homogeneous property of the quadratic residue tournaments to a type of local homogeneity with respect to one of its subtournaments. Such tournaments could be used (as the tournament $QT(7)$ was used above) in order to obtain the base graph G' for the above construction.

Question 11 *Can one construct, for any $k \geq 4$, a tournament A_k with the following property: A_k contains, as a subtournament, a transitive tournament T_k on k vertices such that, for any two subtournaments T_{k-1} and T'_{k-1} of T_k on $k-1$ vertices, there is an automorphism α of A_k such that $\alpha(T_{k-1}) = T'_{k-1}$.*

Finally, one can ask questions analogous to Question 1, namely whether there is a characterisation similar to Theorem 1 of graphs with $k > 2$ mutually pseudosimilar vertices. In [14] a theorem analogous to Theorem 1 was proved, but there the graph H could be infinite. In [8] this problem was partially solved for $k = 3$ with the extra assumption that there are no edges between a certain set of vertices containing the pseudosimilar ones. One can therefore ask the following.

Question 12 *Suppose a graph G has $k > 2$ mutually pseudosimilar vertices $u_1, u_2, \ldots, u_k$. Is G the induced subgraph of a finite graph H in which $u_1, \ldots, u_k$ are similar and which has $k-1$ automorphisms $\alpha_1, \ldots, \alpha_{k-1}$ such that $\alpha_i(G - u_1) = G - u_{i+1}$ and such that the vertices in $V(H) - V(G)$ are in the same orbit as $u_1, \ldots, u_k$ under the action of $Aut(H)$?*

References

[1] B. Alspach and M.-Y. Xu. $\frac{1}{2}$-arc-transitive graphs of order 3p. *J. Algebraic Combin.*, 3:347–355, 1994.

[2] N.L. Biggs. *Algebraic Graph Theory.* Cambridge University Press, second edition edition, 1994.

[3] I.Z. Bouwer. Section graphs for finite permutation groups. *J. Combin. Theory*, 6:378–386, 1969.

[4] H. Cohn. *Advanced Number Theory.* Dover, New York, 1990.

[5] M.M. Klawe D.G. Kirkpatrick and D.G. Corneil. On pseudosimilarity in trees. *J. Combin. Theory Ser. B*, 34:323–339, 1983.

[6] C.D. Godsil. On the full automorphism group of a graph. *Combinatorica*, 1:243–256, 1981.

[7] C.D. Godsil and W.L. Kocay. Constructing graphs with pairs of pseudosimilar vertices. *J. Combin. Theory Ser. B*, 35:146–155, 1982.

[8] C.D. Godsil and W.L. Kocay. Graphs with three mutually pseudosimilar vertices. *J. Combin. Theory Ser. B*, 35:240–246, 1983.

[9] F. Harary. *Graph Theory.* Addison-Wesley, Reading, Mass., 1969.

[10] W. Imrich. Graphical regular representations of groups of odd order. In A. Hajnal and V.T. Sós, editors, *Combinatorics*, volume 18 of *Colloq. Math. Soc. J. Bolyai*, pages 611–622. North-Holland, 1978.

[11] R.J. Kimble. Existence of graphs where almost every edge is pseudosimilar. In G. Chartrand et al., editor, *Theory and Applications of Graphs*, Proc. 4th International Conf., Theory and Applications of Graphs, Western Michigan University, Kalamazoo, pages 431–436. Wiley, 1981.

[12] R.J. Kimble, A.J. Schwenk, and P.K. Stockmeyer. Pseudosimilar vertices in a graph. *J. Graph Theory*, 5:171–181, 1981.

[13] W.L. Kocay. A small graph with three mutually pseudosimilar vertices. *Ars Combinatoria*, 14:99–103, 1982.

[14] W.L. Kocay. Graphs, groups and pseudosimilar vertices. *J. Austral. Math. Soc. Ser. A*, 37:181–189, 1984.

[15] W.L. Kocay, P. Niesink, and C.R. Zarnke. On coset diagrams for pseudosimilar vertices. *Utilitas Math.*, 46:65–80, 1994.

[16] V. Krishnamoorthy and K.R. Parthasarathy. Cospectral graphs and digraphs with given automorphism group. *J. Combin. Theory Ser. B*, 19:204–213, 1975.

[17] J. Lauri. Endvertex-deleted subgraphs. *Ars Combinatoria*, 36:171–182, 1993.

[18] J. Lauri. Pseudosimilarity in graphs—a survey. *Ars Combinatoria*, 46:77–95, 1997.

[19] J. Lauri. Cayley graphs, pseudosimilar edges, and line-graphs. *J. Combin. Math. and Combin. Comput.*, to appear.

[20] J. Lauri and M.C. Marino. On pseudosimilarity in graphs. In A. Barlotti et al., editor, *Combinatorics '88*, volume 2 of *Proc. International Conf. on Incidence Geometries and Combinatorial Structures, Ravello, Italy, 1988*, pages 169–179, 1991.

[21] J. Lauri and R. Scapellato. A note on graphs all of whose edges are pseudosimilar. *Graph Theory Notes of New York*, XXI:11–13, 1996.

[22] D. Livingstone and A. Wagner. Transitivity of finite permutation groups on unordered sets. *Math. Zeitsch.*, 90:393–403, 1965.

[23] G. Sabidussi. Vertex transitive graphs. *Monat. Math.*, 68:426–438, 1964.

[24] J. Sheehan. Minimum multiplicities of subgraphs. *Preprint*.

[25] J. Sheehan. Fixing subgraphs. *J. Combin. Theory*, 12:226–224, 1972.

[26] J. Sheehan. Fixing subgraphs and ulam's conjecture. *J. Combin. Theory*, 14:125–131, 1973.

[27] J. Sheehan. Smoothly embeddable subgraphs. *J. London Math. Soc.*, 9(2):212–218, 1974.

Invariants of *m*-dimensional Linear Subspaces of a Binary [*n*, *k*]-code

J.G. Maks*, J. Simonis

University of Delft, The Netherlands
e-mail: j.g.maks@twi.tudelft.nl

Let $\mathcal{C}$ be a binary $[n, k]$-code, and let $\mathcal{D}$ be an m-dimensional subspace of $\mathcal{C}$. A well-known invariant of $\mathcal{D}$ is the size of the support of $\mathcal{D}$. Another invariant, perhaps not as widely known, is the Hamming weight of the image of $\mathcal{D}$ under the Plücker mapping

$$Span\{u_1, ..., u_m\} \mapsto [u_1 \wedge ... \wedge u_m].$$

In this talk we describe the full list of invariants of $\mathcal{D}$ under the action of the group

$$S_n \times GL(m).$$

In particular the case $m = 2$ is discussed in great detail. We also explore the relations between the multiweight distribution of the code $\mathcal{C}_m$ of all m-dimensional linear subspaces of $\mathcal{C}$ and the multiweight distribution of the appropriately defined dual code $\mathcal{C}_m^{\perp}$.

On the Acrhomatic Number of $P(\alpha, K_n)$ and $P(\alpha, K_{1,n})$

M.F. Mammana

Dipartimento di Matematica - Università di Catania
e-mail: flavia@dmi.unict.it

Let $G = (V, S)$ be a graph. A k-coloring of G is a mapping c of the vertex set V onto a set of k-colors C such that any two adjacent vertices have different colors.

The smallest number n such that there is a n-coloring of G is called the *chromatic number* of G and is denoted by $\chi(G)$.

A *complete k-coloring* of a graph G is a k-coloring c such that for any distinct colors i and j there are two adjacent vertices in G colored with i and j.

The largest number n such that there is a complete n-coloring is called the *achromatic number* of G and is denoted by $\psi(G)$ [1].

Let G be a graph of order n and α be a permutation on the set $\{1, 2, \dots, n\}$. The permutation graph $P(\alpha, G)$ of the graph G is the graph that consists of two disjoint, identically labeled copies of G, G_1 and G_2, with n more edges $x_{i,\alpha(i)}$ that join the vertex v_i in G_1 with the vertex $v_{\alpha(i)} in G_2$.

Some results concerning the achromatic number of $P(\alpha, P_n)$ and $P(\alpha, C_n)$ have been proved by F. Milazzo and V. Vacirca [2]. In this talk we give some results concerning the achromatic number of $P(\alpha, K_n)$ and $P(\alpha, K_{1,n})$.

References

[44] F. Harary, S. Hedetniemi: *The achromatic number of a graph*, J. Combin. Theory **8** (1970).

[45] F. Milazzo, V. Vacirca: *On the achromatic number of* $G \times K_m$, Ars Combinatoria 24-B (1987).

Using a Progressive Withdrawal Algorithm to Study Superconnectivity in ℓ^1-Digraphs

X. Marcote*, I. Pelayo, C. Balbuena, J. Fabrega

Universitat Politecnica de Catalunya (UPC), Spain
e-mail: `francisco.javier.marcote@upc.es`

A maximally connected digraph is said to be superconnected if every minimum disconnecting set F of vertices is trivial, i.e., it consists of the vertices adjacent to or from a given vertex not belonging to F. This work is devoted to presenting a sufficient condition - in terms of the parameter ℓ^1 - on the diameter, in order to guarantee that the digraph is superconnected, giving also a lower bound for the superconnectivity parameter (κ_1) when nontrivial disconnecting sets exist. This result has been carried out with the help of a 'progressive withdrawal algorithm', that establishes how far away a vertex can be to or from a given set of vertices. An analogous result is presented in terms of arcs, assuring arc-superconnectivity and giving a lower bound for the parameter λ_1.

AMS classification: 05C40, 05C20

Decomposing Sets of Triples into Small Planes

R. Mathon

Toronto, Canada

A.P. Street*

University of Queensland, Australia
e-mail: aps@maths.uq.edu.au

In this talk we consider decompositions of the set of all triples chosen from a v-set into copies of the Fano plane on 7 points or copies of the affine plane on 9 points.

Generalized Balanced Weighing and Difference Matrices

V.C. Mavron

University of Wales - Aberystwyth, UK
e-mail: vcm@aber.ac.uk

BGW matrices are constructed over new groups, some non-abelian. The matrices do not have new parameters but some of their base designs are new. A construction of Colbourn and Kreher for difference matrices is generalized.

Mixed Partitions and 3-Spreads of $PG(7,q)$

K.E. Mellinger

University of Delaware - Newark, USA
e-mail: kmelling@math.udel.edu

By a classical result of Bruck and Bose, the study of translation planes is equivalent to the study of spreads; that is, a set of $q^n + 1$ mutually disjoint $(n-1)$-spaces which together form a partition of $PG(2n-1,q)$. The case when $n = 2$ has been studied in detail, but less is known about the higher dimensional cases. In *General Galois Geometries*, by Hirschfeld and Thas, a method of constructing $(2m+1)$-spreads of $PG(4m+3,q)$ is described. The construction starts with a partition of $PG(2m+1,q^2)$ into α Baer spaces (isomorphic copies of $PG(2m+1,q)$), and β m-spaces (isomorphic copies of $PG(m,q^2)$). This so called *mixed partition* can then be used to create a spread of $PG(4m+3,q)$. It is also pointed out that such a partition is known to exist for $\alpha = 0$. The author investigates the possibilities when $m = 1$ and $\alpha \neq 0$. Two infinite families of such mixed partitions are discovered and their associated spreads are examined.

Sequences from Groups

F. Merola

Dipartimento di Matematica - Università di Roma "La Sapienza" - Roma, Italy
e-mail: merola@mat.uniroma1.it

I will talk about some properties of the orbit-counting sequence of an oligomorphic permutation group. Oligomorphic groups are a class of permutation groups acting on an infinite set with links to combinatorial enumeration.

Upper and Lower Chromatic Number for Steiner Systems

L. Milazzo

Department of Mathematics - University of Catania
Viale A. Doria, 6 - 95125 Catania, Italy
e-mail: milazzo@dipmat.unict.it

The last results about upper chromatic number and the first ones about lower chromatic number in Steiner systems.

Scattered Subsets

E. Munarini, N. Zagaglia Salvi*

Politecnico di Milano - milano, Italy
e-mail: norzag@mate.polimi.it

An h-scattered subset of a linearly ordered set L is a subset S with the property that for each two elements x, y of S there are at least h elements not in S between x and y. An h-scattered subset of a cycle is defined in a similar way. We study some combinatorial properties of the species of scattered subsets in the case of linearly orderd sets and in the case of cycles. The cardinalities of the families of such subsets turn out to be a generalization of the Fibonacci numbers and of the Lucas numbers.

A Class of Imprimitive Permutation Groups

S. Musumeci
Università di Palermo - Palermo, Italy
e-mail: musumeci@dipmat.math.unipa.it

We try to classify permutation groups endowed with a system of imprimitivity Ξ subject to the following conditions, where N denotes the normal subgroup leaving every component in Ξ fixed:

(1) The group G/N, induced on Ξ, is finite;
(2) Let Δ be a block in Ξ, the group $G_\Delta/G_{[\Delta]}$ acts 2-transitively on Δ;
(3) The induced action of N on a block $\Delta \in \Xi$ is regular, which means that N acts transitively on Δ and, if $g \in N$ leaves a point $X \in \Delta$ fixed, then g leaves every point in Δ fixed (in symbols $N_X = N_{[\Delta]}$);
(4) Let $\Delta_1, \ldots, \Delta_m$ be distinct blocks in Ξ and, for $i = 1, \ldots, m$, let $X_i, Y_i \in \Delta_i$. Then, there is just one element $g \in N$ such that $g(X_i) = Y_i$ for all $i = 1, \ldots, m$.

On the Orientation Associated with a 3-Face-coloring of a Triangulation

A. Nakamoto, K. Ota, M. Watanabe*

Department of Computer Science and Mathematics
Kurashiki University of Science and the Arts
watanabe@soft.kusa.ac.jp

We consider an orientation associated with a 3-face-coloring of a triangulation, defined as the following: If most frequently used colors are red and blue in a 3-face-coloring for it, the edges of each red triangle are given the clockwise orientation, the edges of each blue triangle the anticlockwise orientation, and the other edges arbitrary orientations. We give upper and lower bounds of the number of triangles with the cyclic orientation in oriented triangulations. We also discuss long cycles in oriented Eulerian triangulations, including results related to these topics.

On 2-reducible Paths in k-edge-connected Graphs

H. Okamura

Department of Applied Mathematics - Konan University
Kobe 658-8501, Japan
e-mail: okamura@center.konan-u.ac.jp

Let $G = (V(G), E(G))$ be a k-edge-connected graph. We call a path (or cycle) P (not necessarily simple) of G 2-reducible if $G - E(P)$ is $(k-2)$-edge-connected. If k is even, for each two edges f and g, there is a 2-reducible cycle containing f and g. However for odd k, we can construct k-edge-connected graphs G having two vertices s and t of distance three such that any cycle containing s and t is not 2-reducible. We disscuss about 2-reducible paths in G.

Superconnected Digraphs and Graphs with Small Conditional Diameters

I. Pelayo*, C. Balbuena, J. Fàbrega, X. Marcote

Universitat Politecnica de Catalunya (UPC). Spain.
e-mail: `ignacio.m.pelayo@upc.es`

The conditional diameter D_ν of a (di)graph G measures how far apart can be a pair of subdigraphs G_1 and G_2 with $\delta^+(G_1) \geq \nu$ and $\delta^-(G_2) \geq \nu$. Thus, D_0 is the standard diameter and $D_0 \geq D_1 \geq \ldots \geq D_\delta$. We prove that if $D_\nu \leq 2\ell - 3$, where ℓ is a parameter which can be thought of as a generalization of the girth of a graph, then G is maximally connected, superconnected or has a good superconnectivity, only depending on the value of ν. To guarantee the same properties in the edge case it is enough that $D_\nu \leq 2\ell - 2$. The results for (undirected) graphs are obtained as a corollary of those for digraphs.

Pappus' Theorem for Ring-Geometries

T. Pfeiffer

ERC Frankona
Zelterstrasse 6; D-55545 Bad Kreuznach, Germany
e-mail: Thorsten.Pfeiffer@ercgroup.com

A famous result due to David Hilbert states for a projective plane over a division ring K the equivalence of Pappus' theorem and the commutativity of K. We extend this result to the projective plane over an arbitrary ring.

Partial K-loops of Exponent 2 and Factorizations of Graphs with Trapezium Condition

S. Pianta

Università Cattolica - Brescia, Italy
e-mail: geomet@dmf.bs.unicatt.it

Let P be a non empty set, $0 \in P$ a fixed point, $P' \subseteq P \setminus \{0\}$ and ${}^o : P' \to \text{Sym } P \cap J$ (where $J := \{\sigma \in \text{Sym } P | \sigma^2 = id \neq \sigma\}$) a map.
We call $(P, P', {}^o; 0)$ a **semiregular invariant reflection structure** if:

(B1') i) $\forall x \in P' : x^o(0) = x$

ii) $\forall y \in P \setminus \{0\} \ \exists n \geq 1$ and $\exists a_1, a_2, ..., a_n \in P' : \ a_1^o a_2^o ... a_n^o(0) = y\,;$

(B2) $\forall x, y \in P' \quad x^o y^o x^o \in (P')^o\,.$

By introducing a partial operation $+ : P' \times P \to P; (a, b) \to a + b := a^o(b)$ one obtains a **partial K-loop of exponent 2** i.e.

$$\forall a, b \in P', \ \forall x \in P : a + a = 0 \text{ and } (a + (b + a)) + x = a + (b + (a + x))\,.$$

Now for all $\{a, b\} \in \binom{P}{2}$ such that there is a $c \in P'$ with $c^o(a) = b$ we write $(a, b) := c$ and we associate to $(P, P', {}^o; 0)$ a graph with parallelism $(P, \mathcal{E}, \|)$ where

$$\mathcal{E} := \{\{a, b\} \in \tbinom{P}{2} | (a, b)\text{exists}\}$$

is the set of edges and $\{a, b\} \parallel \{c, d\} :\Leftrightarrow (a, b) = (c, d)$.
Then the set of all parallelism classes is a factorization of the graph $(P, \mathcal{E})$. In addition this graph satisfies the following **trapezium condition**:

(T) $\forall \{a, b\}, \{b, c\}, \{a', b'\}, \{b', c'\}, \{c, d\}, \{c', d'\} \in \mathcal{E}$ with $b \neq c$ and
$\{a, b\} \parallel \{a', b'\} \parallel \{c, d\} \parallel \{c', d'\}$ and $\{b, c\} \parallel \{b', c'\}$ then
$\{a, d\}, \{a', d'\} \in \mathcal{E}$ and $\{a, d\} \parallel \{a', d'\}\,.$

There is a one-to-one correspondence between these three types of partial structures. We discuss how one can complete them in order to obtain new examples of proper K-loops.

What is a Binary String?

F. Piper
London, UK
e-mail: f.piper@rhbnc.ac.uk

Clearly a simple answer to the question is that it is a string of 0s and 1s. However, that is neither interesting nor helpful. In this talk which is intended primarily for research students, we look at some of the ways in which mathematicians and communications engineers view binary strings, and take a very high level look at some of the fascinating and productive interaction between these various viewpoints. We will be particularly interested in cryptographic applications. Our basic assumption, since this is a paper presented at a combinatorics conference, is that the reader will be familiar with the mathematical concepts but may not be conversant with cryptography.
We also take this opportunity to resurrect an old, unresolved research problem that provides us with an opportunity to illustrate the potential interplay between the various interpretations. From a cryptographic viewpoint the problem is not particularly important, but it has remained unresolved for more than twenty years, and it would be interesting to know the answer.

1 Introduction

The digital age is with us and we now have both digital TV and digital telephones. So communications is 'all about' transmitting binary strings.

To communications engineers a bit string is likely to represent encoded data, i.e. a string of codewords. Clearly the identity of the data will depend on the encoding scheme used, and the coding scheme may be carefully chosen to achieve a specific objective eg error correction or detection. To quote from [4]: "Although it has origins in an engineering problem, the subject has developed by using more and more sophisticated mathematics." In fact coding theory provides an excellent example of a topic where communications engineers and combinatorists have worked in harmony for years. To many pure mathematicians certain block codes are merely vector spaces with certain (distance related) properties. They have exploited these properties to provide 'useful' codes without worrying about, or maybe not even being aware of, the practical applications.

Many excellent papers and books have been written to illustrate the rich interplay between error correcting codes and, for example, projective geometries over $GF(2)$. (See [4],[5] and [6]).

When data is coded for secrecy, an encryption algorithm is used to produce 'unintelligible' ciphertext. The encryption process involves the selection of one (of a large number) encryption keys that determines the transformation. Of necessity the transformation must be reversible, and the receiver has the appropriate decryption key that selects the inverse transformation. In most practical applications, the secrecy of the data relies on the secrecy of the deciphering key. Systems where the enciphering key is known publicly are called **public key systems**.

If we regard our data as a bit-string then the encryption process may act as a permutation on substrings, or blocks, of a fixed size $s > 1$, in which case it is called a **block cipher**, or it may encrypt the data bit by bit, which we will call a **stream cipher**.

Most public key systems are block ciphers and interpret a block as the binary representation of an integer, and the encryption process is a (modular) number theoretic transformation, using modular exponentiation. The underlying mathematical theory is straightforward, and the security tends to rely on the high computational complexity of specific, well-studied problems such as the factorisation of large integers.

Probably the simplest and most well known illustration of this is the celebrated RSA system. For this system two large primes, p and q say, are generated and their product n is computed. This value n is part of the public key. The second part of the public key is an integer e chosen so that $(e, (p-1)(q-1)) = 1$. In order to encrypt a binary message, the message is divided into blocks that are regarded as the binary representations of integers bounded above by $n-1$. A message block m is then encrypted to c where $c = m^e \bmod n$. The secret decryption key consists of n and the integer d which satisfies $ed = 1 \bmod (p-1)(q-1)$ and decryption is given by $m = c^d \bmod n$.

The fact that the algorithm 'works', i.e. that the original message is obtained after encryption and decryption, is an immediate consequence of Fermat's Little Theorem. For RSA to be secure it must be computationally impossible to deduce the secret key, which really means d, from the public values n and e. The calculation of d from the equation $ed = 1 \bmod (p-1)(q-1)$ is straightforward application of Euclid's Algorithm. Thus any serious attacker would be able to solve such an equation and RSA can only be secure if the attacker does not know which equation they have to solve i.e. only if they cannot factor n.

In this brief discussion of coding and cryptography we have already illustrated two different ways in which binary strings are 'interpreted' before specific communications problems are solved.

We now take the mathematician's viewpoint and list some of the more obvious interpretations of a binary string. Not surprisingly, although the terminology may be different, some of the interpretations are essentially the same. Interpretations of a binary string of length n include:

1. the binary representation of an integer from 0 to 2^n.
2. a vector in $V_n(2)$.
3. the coefficients of a binary polynomial of degree at most $n-1$.
4. an element of $GF(2^n)$.
5. an indicator sequence for a subset of an ordered set.
6. the generating cycle of an infinite periodic binary sequence.
7. the leading row of an incidence matrix of a cyclic 1-design.
8. the feedback coefficients for an n-stage LFSR.
9. the coefficients of a binary linear recurrences relation $s_{t+p} = \sum_{i=0}^{p-1} c_t s_{t+i}$ where each $c_i \in \{0,1\}$ and addition is modulo 2.

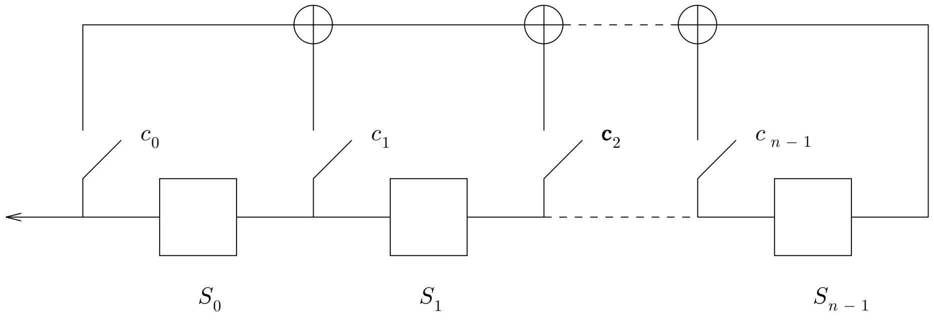
Clearly (1) to (4) need no explanation. One of the most common examples of an indicator sequence is where the set is the integers 0 to $n-1$ and the binary sequence identifies a λ-difference set. (Recall: $\{a_1, \cdots, a_k\}$ **is a λ-difference set modulo** n if the differences $(a_i - a_j) \bmod n$ (with $i \neq j$) assume each of the values 1 to $n-1$ exactly λ times. Thus, for example, $\{0,1,3\}$ is a 1-difference set mod 7 with indicator set 1101000.) An infinite binary sequence (s_t) is said to be **periodic** with period p if $s_t + p = s_t$ for all t, and the string $s_0, s_1, \cdots, s_{p-1}$ is called a generating cycle. Clearly any n-bit string is the generating cycle of an infinite binary sequence with period n. We will be interested in the use of sequences for encryption. Given an n-bit string then we can construct an $n \times n$ binary matrix A by letting the ith row of A, $i = 0$ to $n-1$, be that string rotated through i positions. Clearly this matrix is symmetric and each row and column has the same number of 1s. If this number is k then A is the incidence matrix of a $1-(n,k,k)$ incidence structure, which will be a design unless the string itself is the concatenation of two or more equal cycles.

Note. If we consider the string 1101000 then, regarded as an indicator sequence, we get the 1-difference set $\{0,1,3\}$ of integers mod 7. It is easy to see that if we take the integers $0,1,2,3,4,5,6$ as points and the translates of $\{0,1,3\}$ i.e. $\{1,2,4\}$, $\{2,3,5\}$ etc as the blocks then we have a $2-(7,3,1)$ design i.e. the projective plane of order 2. Similarly if we consider the matrix

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

then A is an incidence matrix for the same design. These examples merely show that, not surprisingly, it is often easy to travel from one interpretation to the other. Nevertheless the knowledge and expertise required of the various interpretations is often different and there can be rich interplay between different approaches. (As an example of the type of result that arises, many people have studied ways of generating difference sets and been able to characterise the geometric properties of the resultant designs. See, for example [1].) The Multiplier Theorem, which shows that the existence of an arithmetic property of a difference set implies the existence of an automorphism of the corresponding design, is just one example of a relevant result.

Representation (8) is very familiar to engineers and is similar to (9). A diagrammatic definition of an n-stage (binary) Linear Feedback Shift Register (LFSR) is given below. Each switch may be either open or closed. If the ith switch is open we put $c_i = 0$ while if it is closed $c_i = 1$.



Initially, at time $t = 0$, the stages $S_0, S_1, \cdots, S_{n-1}$ are filled with an initialisation binary vector $s_0, s_1, \cdots, s_{n-1}$. At each increase in the time t, the content $S_0(t)$ is output as the tth entry of a binary sequence (s_t). For $i = 0$ to $n-2$, $S_i(t+1) = S_i(t)$ while $S_{n-1}(t+1) = \sum_{i=0}^{n-1} c_i S_i(t)$, where addition is modulo 2. (Thus an LFSR is an electronics device that produces a binary sequence satisfying a linear recurrence relation. Two excellent references are [2] and [3].)

We make 3 observations:

(a) If the state vector, i.e. the contents of the stages, is ever all zeros then it can never change and the output sequence will be all zeros.

(b) The output sequence will depend on the initialisation vector.

(c) If $c_0 = 1$ then the sequence is always periodic with period at most $2^n - 1$.

LFSRs are commonly used as components of special types of encryption devices.

NOTE: The 3-stage LFSR with $c_0 = 1$ $c_1 = 0$ $c_2 = 1$ i.e. represented by the sequence 101 produces the sequence 1110100 when 111 is the initialisation vector. Thus different binary strings can represent identical 'objects' depending on the viewpoint of the user.

To the cryptographer an n-bit string might also represent a cryptographic key. If the data has been encrypted then it is likely to yield meaningless patterns if decoded before being decrypted. Indeed, in loose terms, the object of encryption is to transform (often highly) formatted data into bit-strings that appear to be randomly generated. Two standard references are [7] and [8].

2 Basic Cryptography

If we denote the message space, cryptogram space and key message space by M, C and K respectively then a block cipher can be defined as a function $f : M \times K \to C$. There have, not surprisingly, been many attempts to classify block ciphers in terms of the properties of f. (Clearly, in order that decipherment is possible, for any fixed key k the function f must be reversible.)

Definition 1 *A block cipher is* **linear** *if M and C are vector spaces over $GF(2)$ and, for each $k \in K$, the corresponding F is a linear transformation $M \to C$.*

For any linear cipher the all zero message is encrypted as all zeros. Thus we frequently exclude the all zero vectors from both M and C. In [12] the authors concentrate on the situation where $|M| = |C| = |K|$ and each cryptogram can be the encryption of any message, which, since the sets are finite, implies that for any $m \in M$ and $c \in C$, there is a unique $k \in M$ with $f(m, k) = c$. For reasons explained in the paper such ciphers are called $NEKMRP$ ciphers. When we do this in the case of a binary linear cipher, we obtain a cipher with $|M| = |C| = |K| = 2^n - 1$ and with the property that, for any pair of keys k_1, k_2 $f(m, k_1) \neq f(m, k_2)$ for any $m \in M$. If we regard these keys as determining $n \times n$ binary matrices, so that key k_i determines matrix A_i, then for a $NEKMRP$ linear cipher may be regarded as a set of $2^n - 1$ binary $n \times n$ matrices such that $A_i A_j^{-1}$ fixes no vector of $GF(2)^n \backslash \{0\}$ for all i, j with $i \neq j$. The authors of [12] then went on to define $NEKMRP$ bilinear ciphers which were characterised as being linear ciphers with the extra property that the set of all the enciphering matrices $\{A_i\}$, together with all non-zero $n \times n$ matrix, forms a vector space under matrix addition. A third family of ciphers, which they called multiplication ciphers, was also defined. The precise definitions are not relevant here. The important observation is that two of the world's leading cryptographers were attempting to characterise certain classes of block ciphers. They then went on to ask a number of natural questions such as "Does there exist a linear cipher which is not bilinear?". Their paper was written in 1988 but the answers to all their questions had been provided more than twenty years earlier by pure mathematicians with interests in translation planes and spreads (see [13], [14]).

Definition 2 *If V is a vector space of dimension $2n$ over F (with $|F| = q$) then a spread of V is a set of $q^n + 1$ n-dimensional subspaces $W_1, W_2, \cdots, W_{q^n+1}$ of V such that $W_i \cap W_j = \{0\}$ for $i \neq j$.*

In order to understand the relationship of spreads to linear block ciphers we need to represent them in terms of linear transformations. However, this is straightforward. If W is a vector space of dimension n over F and if $V = W \oplus W$ then, given $q^n - 1$ linear transformations T_i, $i = 3, \cdots, q^n + 1$ of W, we define subspaces $W_1, W_2, \cdots W_{q^n+1}$ of V as follows:

$$\begin{aligned} W_1 &= \{(x,0) : x \in W\} \\ W_2 &= \{(0,y) : y \in W\} \end{aligned}$$

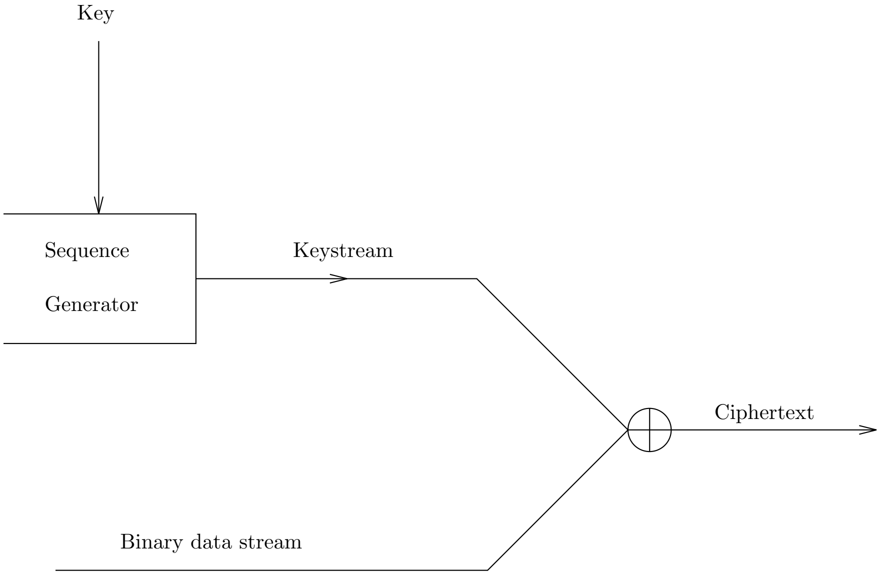
For $i = 3, \ldots, q^n + 1$,

$$W_i = \{(x, xT_i) : x \in W \text{ and } T_i \text{ is a non-singular linear transformation of W}\}.$$

It is easy to see that $W_1, W_2, \ldots, W_{q^n+1}$ forms a spread if, and only if, for all $i \neq j$, $T_i T_j^{-1}$ does not fix any non-zero vector of W. For $q = 2$ this is identical to the condition that a set of linear transformations define a $NEKMRP$ linear cipher and establishes a correspondence between translation planes (a popular research topic for combinatorialists in the 1960s and 1970s) with certain classes of block cipher. The 'extra properties' introduced in [12] in the context of block ciphers have geometric equivalents for translation planes. In particular bilinear ciphers correspond to semi-field planes and, since there are translation planes which are not semi-field planes, the question which we quoted for [12] was answered long before it was posed. A similar remark applies to the other questions and conjectures of [12]. This is an example where two interpretations of vector spaces, one as 'representing' translation planes and the other as 'representing' block ciphers, have led to the posing of identical questions but using terminology which made them unrecognisable to research workers in the other 'camps'.

For symmetric, (i.e. non-public key), systems there is no uniformity in the way bit-strings are interpreted. For instance, blocks of size s are frequently combined using vector addition modulo 2, but the use of addition mod 2^s is also common. Non-linearity is often introduced by the use of look-up tables and, in general, these encryption algorithms do not have neat mathematical formulations. They tend to use simple substitutions and transformations iteratively, and are assessed by statistical, as opposed to mathematical, analysis. For more details see [7] or [8].

For steam ciphers the situation is different. The encryption process operates on a single bit. However, clearly, there is not much you can do to a bit; you either leave it alone or complement it. If the process is to be secure then the attacker should have no way of predicting which bits are changed and which ones have been left unaltered. Diagrammatically a stream cipher is:



If this keystream were replaced by a truly random binary sequence, and each keystream bit were used only once then we would have the provably unbreakable Vernam Cipher. However, in most practical systems this is not the case and, for stream ciphers, we require our generation to be as indistinguishable from truly random generation as possible. We call such generation **pseudo-random**.

It is, of course, very difficult to give a precise mathematical definition of pseudo-randomness. Indeed the concept of 'good', changes with the application. However, in an attempt to quantify some criteria for assessing a given binary sequence's suitability for use as a pseudo-random sequence, Golomb proposed a set of randomness postulates for a binary sequence with (long) period p. Sequences satisfying Golomb's postulates are known as PN-sequences, where PN stands for Pseudo Noise.

3 PN-Sequences

Before we can introduce PN-sequences we need a few definitions.

Definition 3 *If (s_t) is a binary sequence then a* **run** *of length n is a subsequence of n consecutive identical entries which is neither preceded nor followed by the same element.*

So, for example, 0011101 starts with a run of 2 zeros followed by a run of 3 ones. It does not contain a run of 2 ones.

Definition 4 *A run of zeros is called a* **gap** *and a run of ones is usually called a* **block***. However, in order to avoid confusion with the blocks of our designs, in this paper we will refer to a run of ones as a* **1-run***.*

If (s_t) has period p then, for any a satisfying $0 \leq a < p$, let (s_{t+a}) be the translate of (s_t) with shift a and let $A(a)$ be the number of positions in which the generating cycles of (s_t) and (s_{t+a}) have the same entry.

Definition 5 *If (s_t) has period p then the* **autocorrelation function** *$C(a)$ is defined by $\frac{C(a)=(2A(a)-p)}{p}$. This is often written as $\frac{(A(a)-D(a))}{p}$, where $D(a)$ is the number of positions in which the generating cycles of (s_t) and (s_{t+a}) disagree.*

Clearly $C(0) = 1$. If $a \neq 0$ then the autocorrelation is said to be **out-of-phase**. It is perhaps worth noting that this type of autocorrelation, called the **periodic autocorrelation**, is particularly relevant in cryptography. However, for synchronisation applications the **aperiodic autocorrelation** is more appropriate. Here only the first $p-a$ terms of (s_t) and (s_{t+a}) are compared.

We can now state Golomb's postulates.

G1 If p is even then a cycle contains $\frac{p}{2}$ zeros. If $p$is odd then a cycle contains either $\left[\frac{p}{2}\right]$, or $\left[\frac{p}{2}\right]+1$ zeros.

G2 In a cycle of length p, 1/2 of the runs have length 1, 1/4 of the runs have length 2 and, in general, for each i for which there are at least 2^{i+1} runs, 2^{-i} of the runs have length i. Moreover, for each of these values of i there are equally many gaps and 1-runs.

G3 The out-of-phase autocorrelation is constant.

There are a number of observations that we should make about Golomb's postulates:

(a) One would expect any (long) sequence obtained by tossing a fair coin to 'almost' satisfy them.

(b) They are probably too precise. As we shall see, the set of sequences satisfying them is probably very limited. Nevertheless we would expect any pseudo-random sequence to have characteristics very similar to them.

4 Geometrical Consequences of Golomb's Postulates

Definition If (s_t) is a binary sequence with period p then we define $\underline{A}(s_t)$ to be the $p \times p$ matrix whose ith row is $(s_i, s_{i+1}, \ldots, s_{i+p-1})$ $i = 0 \ldots p-1$ and $\underline{D}(s_t)$ to be the incidence structure with $\underline{A}(s_t)$ as incidence matrix.

For $i = 0, 1, 2, \ldots, p-1$, let s_i be the $(i+1)$th row of $\underline{A}(s_t)$ (regarded as a binary vector) and let x_i be the block of $\underline{D}(s_t)$ determined by s_i. Thus, for each i, s_i is the generating cycle for (s_{t+i}).

Definition If x and y are binary vectors of the same length then:

(b) the **weight** of x, denoted by $w(x)$, is the number of positions in which x has a 1;

(b) the **Hamming distance** between x and y, denoted by $d(x, y)$, is the number of positions in which x and y have different entries.

NOTE that Golomb's postulate $G1$ merely says that, for $i = 0, 1, 2, \ldots, p-1$ $w_{(}s_i) = \frac{p}{2}$ if p is even and $w(s_i) = \left[\frac{p}{2}\right]$ or $\left[\frac{p}{2}\right] + 1$ if p is odd.

Thus Golomb's randomness postulate $G1$ merely determines the number of points on each block of $\underline{D}(s_t)$.

Postulate $G3$ says that the out-of-phase autocorrelation (that is, $C(a)$ with $a \neq 0$) is a constant. This is equivalent to saying that $A(a)$ and $D(a)$ are constants. From the definition, $D(a)$ is the number of positions in which $\underline{s}_0$ and $\underline{s}_a$ disagree which, clearly, is also the number of positions in which s_i and s_{i+a} disagree, $i = 0, 1, \ldots, p-1$. Thus for any i and a, $D(a) = w(\underline{s}_i + \underline{s}_{i+a})$ and so, if $C(a)$ is constant for all $a \neq 0$ then, for all i, j with $i \neq j$, $w(\underline{s}_i + \underline{s}_j)$ is a constant.

If x_i is the block of $\underline{D}(s_t)$ represented by $\underline{s}_i$ then $w(\underline{s}_i + \underline{s}_i) = |x_i \cup x_j \setminus (x_i \cap x_j)|$. So, if we let $\lambda_{ij} = |x_i \cap xj_{|}$, then $w(\underline{s}_i + \underline{s}_j) = 2(k - \lambda_{ij})$, where k is the number of points on a block. Hence if we put $w(\underline{s}_i + \underline{s}_j) = \mu$, where μ is constant, then $\lambda_{ij} = (2k - \mu)/2$ that is, λ_{ij} is independent of i and j. This means that if (s_t) satisfies $G3$ then $\underline{D}(s_t)$ is the dual of a 2-design which, since it is symmetric, implies that it is a 2-design.

Thus G3 implies that D(st) is a symmetric 2-design with a cyclic Singer group.

If $\underline{D}(s_t)$ is a $2 - (p, k, \lambda)$ design then, since it has a cyclic Singer group, the positions of the 1s in the generating cycle of (s_t) must determine a λ-difference set modulo p. As an illustration suppose (s_t) is the sequence of period 7 with generating cycle 0111010. Straightforward verification shows $k = 4$ and $C(a) =$

$-\frac{1}{7}$, $a \neq 0$. It is then easy to check that $\underline{D}(s_t)$ is a symmetric $2-(7,4,2)$ design and that the set $(1,2,3,5)$, which is determined by the positions of the 1s in the generating cycle, is a 2-difference set modulo 7. If (s_t) satisfies $G1$ and $G3$ then $\underline{D}(s_t)$ is a symmetric $2-(p,k,\lambda)$ design with $p = 2k-1$, $2k$ or $2k+1$. However, for a symmetric 2-design we cannot have $p = 2k$. Thus p must be either $2k-1$, or $2k+1$. From the relation $(p-1)\lambda = k(k-1)$ it is easy to compute λ, and we then have that $\underline{D}(s_t)$ is either a $2-(4\lambda+3, 2\lambda+1, \lambda)$ design or $2-(4\lambda-1, 2\lambda, \lambda)$ design. For general properties of designs see [10].

So postulates G1 and G3 together imply that D(st) is either a cyclic Hadamard 2-design or the complement of a cyclic Hadamard 2-design.

Clearly if $\underline{D}(s_t)$ is a Hadamard design then is the complement of a Hadamard design. Furthermore, if (s_t) satisfies $G1$ and $G3$ then $\underline{D}(s_t)$ is a Hadamard design if a cycle contains $1/2(p+1)$ zeros and $1/2(p-1)$ ones. It is worth noting here that if $\underline{D}$ is a Hadamard 2-design (or its complement) with a cyclic Singer group, then $\underline{D}$ determines a difference set which, in the way described earlier, gives a periodic sequence satisfying $G1$ and $G3$.

The implications of $G2$ are not as obvious as those of $G1$ and $G3$.

However, some detailed counting gives the following:

Theorem If (s_t) is a $PN-$sequence then $\underline{D}(s_t)$ is either a cyclic Hadamard design with parameters or the complement of one.

It is perhaps worth noting here that the converse of this result is obviously not true. In other words if $\underline{D}(s_t)$ is a cyclic Hadamard design with parameters $2-(2^{i+2}-1, 2^{i+1}-1, 2^i-1)$ or the complement of one, then (s_t) need not be a PN-sequence.

It was widely conjectured that if (s_t) is a PN-sequence then $\underline{D}(s_t)$ is isomorphic to the design of points and hyperplanes of a finite-dimensional projective space over $GF(2)$, or its complement. However, in 1981 U. Cheng discovered a PN-sequence (c_t) with period 127 that (up to complementation) is the only counter-example to that conjecture. Although the sequence (c_t) was not 'known' before Cheng's work, $\underline{D}(c_t)$, which is a Hadamard $2-(127,63,31)$ design with a cyclic Singer group, was known. In fact in [1] Baumert lists all such designs. To obtain the sequence (c_t) from [1] we take the difference set with the appropriate parameters labelled (e). From this set we construct the sequence (d_t), where $d_t = 1$ in the positions indicated by the difference set. The sequence (c_t) is then defined by $c_t = d_{39t}$ where $39t$ is reduced modulo 127. Thus the existence of a PN-sequence of period 127 is not at all obvious from Baumert's list. In fact Baumert exhibits four non-isomorphic cyclic Hadamard designs on 127 points which do not give PN-sequences. Cheng has shown, by computer search, that (up to complementation) (c_t) is the only counter example with $p \leq 255$.

We have already noted that LFSR produces periodic sequences with period $p \leq 2^n - 1$. In fact, for any n it is possible to choose the feedback coefficients so that, provided the initial state vector is not zero, the period if equal to $2^n - 1$.

(This is not quite so easy and we refer the interested reader to [2].)

Definition 6 *A sequence of period $2^n - 1$ which is generated on an n-stage shift register with linear feedback is called an m-sequence.*

Historically, m-sequences and PN-sequences have been confused and many people assumed they were the same up to complementation). However, the sequence (c_t) of Cheng provides an example of a PN-sequence that is not an m-sequence. Any m-sequence is a PN-sequence and, furthermore, if (s_t) is an m-sequence then $\underline{D}(s_t)$ is the complement of a design formed by the points and hyperplanes of projective space over $GF(2)$. (There are many proofs of this. One of the easiest involves showing that the matrix $A(s_t)$ has the correct rank.)

There are now a number of obvious interesting problems. One is to find all PN-sequences. Another is to find a characterisation of m-sequences by adding a suitable extra postulate to those of Golomb. One approach to both these problems may be via the Hadamard designs introduced here.

5 Conclusion

Some of the fascinating interplay between pure mathematics has been illustrated under the general theme of the study of binary sequences. This is most certainly not a new observation as is evidenced by the success of the Journal of Designs, Codes and Cryptography. Anyone interested in reading about some of the more recent advances should consult [11].

References

[1] L.D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics 182, Spring-Verlag, Berlin-New York 1971; MR 44 97

[2] S.W. Golomb, *Shift Register Sequences (revised edition)* Aegean Park Press, California 1982

[3] E.S. Selmer, *Linear Recurrence Relations Over Finite Fields*, Dept of Maths, Univ of Bergen 1966

[4] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes*, North Holland 1988

[5] R. Hill, *A First Course in Coding Theory*, Clarendon Press 1986

[6] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press 1979

[7] B. Schneier, *Applied Cryptography*, John Wiley & Sons 1996

[8] A. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press 1996

[9] U. Cheng, *Properties of Sequences*, PhD thesis, University of S California 1981

[10] Th. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Mannheim 1985

[11] *Difference Sets, Sequences and Their Correlation Properties* (Ed: A Pott et al, Nato Science Series 1998

[12] J.L. Massey, U. Maurer and M. Wang. *Non-expanding key-minimal, robustly perfect linear and bilinear ciphers*, Proc. of Eurocrypt 87 pp 237-245.

[13] H. Lunesburg, *Translation Planes*, Springer-Verlag, N York 1980

[14] D.R. Hughes and F.C. Piper, *Projective Planes*, Graduate Texts in Mathematics Vol 6, Springer-Verlag, New York 1972

On Buekenhout-Metz Unitals

O. Polverino

Seconda Università di Napoli (Caserta), Italy
e-mail: `polverin@matna2.dma.unina.it`

In the linear representation of the Desarguesian plane $PG(2, q^2)$ in $PG(5, q)$, the classical unital (the Hermitian curve) is represented by an elliptic quadric ruled by lines of a normal spread. We prove that a Buekenhout-Metz unital $\mathcal{U}$ in $PG(2, q^2)$, arising from an elliptic quadric, is represented in $PG(5, q)$, mainly, by an algebraic hypersurface of degree four. Moreover, such a hypersurface is reducible if and only if $\mathcal{U}$ is classical.

On the Geometry of Power Mappings in Finite Fields

A. Pott

Fakultät für Mathematik - Otto-von-Guericke-Universität
Postfach 4120 - 39016 Magdeburg Germany
email: alexander.pott@mathematik.uni-magdeburg.de

Let $\mathbb{F}_{q^n}$ denote the finite field with q^n elements where q is a power of the prime p. The field can be also viewed as a vector space $\mathbb{F}_q^n$ together with a cyclic group of $q^n - 1$ bijective linear mappings.

The simplest mappings $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ on finite fields are power mappings x^d. If d is a power of p then x^d is simply a linear mapping. It is interesting to see that certain powers of d give rise to "maximum nonlinear" functions.

We begin with the binary case $q = 2$. A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ gives rise to 2^n *boolean* functions $\mathbb{F}_{2^n} \to \mathbb{F}_2$:

$$f_\gamma := \mathrm{trace}_{2^n/2}(\gamma \cdot f(x))$$

where "trace" denotes the usual trace function $\sum_{i=0}^{n-1} x^{2^i}$ and $\gamma \in \mathbb{F}_{2^n}$. Note that f_γ is linear if f is linear. In order to measure the nonlinearity of f we define the nonlinearity of boolean functions $g : \mathbb{F}_{2^n} \to \mathbb{F}_2$: A linear function g ($\neq 0$) has the property that its kernel is a hyperplane, hence

$$\#\{x : g(x) = 0 \text{ and } \langle x, z\rangle = 0\} \in \{2^{n-1}, 2^{n-2}\}.$$

or

$$g^{(z)} := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{g(x) + \langle x, z\rangle} = 0.$$

Therefore, the linearity of an arbitrary boolean function g can be measured by

$$\max_{z \in \mathbb{F}_{2^n}} |g^{(z)}|$$

and a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is maximum nonlinear if

$$\max_{\gamma \in \mathbb{F}_{2^n}^*} \max_{z \in \mathbb{F}_{2^n}} |f_\gamma^{(z)}|$$

is as large as possible. The first part of my talk will be the following:

Survey bounds on the nonlinearity of power mappings and discuss several examples.

Computing the nonlinearity is usually a problem of calculating the number of solutions of an equation in $\mathbb{F}_{2^n}$; sometimes this equation is a quadratic form.

Another concept of nonlinearity is the so called (A)PN property of a function ((almost) perfect nonlinear). A function $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is almost perfect nonlinear if

$$f(x + a) - f(x) = b$$

has at most two solutions in x (given $a \neq 0$ and b). The function is called perfect if the number of solutions is precisely 1. It is well known that perfect functions give rise to projective planes of Lenz-Barlotti type II. Unfortunately, not many perfect linear functions are known, in particular, they cannot exist in characteristic 2. On the other hand, functions f where (*) has only few solutions can be used in differential cryptanalysis. Therefore, in the second part I will

Survey the known series of (almost) perfect nonlinear power functions.

In the binary case, both concepts of nonlinearity are linked:

Discuss the connection between APN functions and maximum nonlinear functions.

Finally, maximum nonlinear functions give rise to sequences with low (cross)correlations. These have several applications, in particular in mobile communications (code division multiple access systems):

Describe the application of power mappings in CDMA systems.

Baer Cone Intersections

H. Pralle

Mathematisches Institut der Justus-Liebig-Universität Giessen
Arndtstr. 2 - D-35392 - Giessen, Germany
e-mail: `harm.pralle@math.uni-giessen.de`

In a projective space $\mathcal{P} = \mathrm{PG}(d, q^2)$, $d \geq 2$, let V be a subspace of $\mathcal{P}$ of codimension at least two and C a complement of V in $\mathcal{P}$. A *Baer cone* is the set of subspaces of $\mathcal{P}$ that contain V and intersect C in subspaces of a given Baer subspace $\mathcal{B}$ of C. The 3-dimensional projective space is the lowest dimensional with non trivial intersection configurations of two Baer cones. We describe the intersection configurations of two Baer cones in $\mathrm{PG}(3, q^2)$.

Extending the Thas-Walker Construction

R. Riesinger

University of Wien, Austria
e-mail: havlicek@geometrie.tuwien.ac.at

Definition. *Let $\mathcal{S}$ be a spread of a Pappian projective* 3*-space* $\Pi = (\mathcal{P}, \mathcal{L})$ *and let* Σ *be a collection of proper or improper reguli contained in* $\mathcal{S}$*; by an improper regulus we mean a set* $\{x\}$ *with* $x \in \mathcal{L}$*. We call* Σ *a regulization of* $\mathcal{S}$*, if the following hold: (RZ1) Each line of* $\mathcal{S}$ *belongs either to exactly one regulus of* Σ *or to all reguli of* Σ*. (RZ2) There are at most two improper reguli in* Σ*.*

By $\mathcal{R}^c$ we denote the complementary regulus of a proper regulus $\mathcal{R}$, moreover, $\{x\}^c := \{x\}$. For the Thas-Walker construction the Klein mapping λ of $\mathcal{L}$ onto the Klein quadric H_5 plays a crucial role; $\lambda(\mathcal{R})$ is an irreducible (=*proper*) conic and $\lambda(\{x\})$ or a point (=*improper conic*). We classify the regulizations via the line set $\cup(\mathcal{R}^c|\mathcal{R} \in \Sigma) =: \mathcal{S}^c_\Sigma$ and consider the set $\{\lambda(\mathcal{R}^c)|\mathcal{R} \in \Sigma\} =: \mathcal{F}_\Sigma$ of conics; $\dim(\mathrm{span}(\lambda(\mathcal{S}^c_\Sigma))) =: v_\Sigma$. 1. ($v_\Sigma = 3$) If $\mathcal{S}^c_\Sigma$ is a non-degenerate linear congruence (=net) of lines (i.e. Σ is a *net generating* regulization, *hyperbolic* or *parabolic* or *elliptic* according to the type of $\mathcal{S}^c_\Sigma$), then $\mathcal{F}_\Sigma$ is a flock of $\lambda(\mathcal{S}^c_\Sigma) \subset H_5$. quadric or a quadratic The converse of the this statement is the Thas-Walker construction. 2. ($v_\Sigma = 4$) <3. ($v_\Sigma = 5$)> If $\mathcal{S}^c_\Sigma$ belongs to a single <no> linear complex of lines, then Σ is called a *unisymplecticly <asymplecticly> complemented* regulization. Properties of $\mathcal{F}_\Sigma$ are used to define the concept "flockoid of a Lie quadric" <"flocklet of the Klein quadric">. First <second> extension of the Thas-Walker construction: If $\mathcal{D}$ is a flockoid of a Lie quadric $L_4 \subset H_5$ <flocklet of H_5>, then $\cup((\lambda^{-1}(k))^c|k \in \mathcal{D})$ is a spread of Π admitting the regulization $\{(\lambda^{-1}(k))^c|k \in \mathcal{D}\}$ which is either unisymplecticly complemented or elliptic <either asymplecticly or unisymplecticly complemented or elliptic>.

References

[46] R. Riesinger.: *Extending the Thas-Walker construction*, Bull. Belg. Math. Soc., Simon Stevin, **6**, (1999), 237-247.

[47] R. Riesinger.: *The second extension of the Thas-Walker construction*, to appear on Beiträge Algebra Geom.

Complete Unital-derived Arcs in the Hall Planes

G. Rinaldi

Dipartimento di Matematica - Università di Modena e Reggio Emilia
Via Campi 213/B - 41100 Modena, Italy
e-mail: rinaldi@unimo.it

A well known theorem of B. Segre states that a complete arc of $PG(2,n)$ (n an even prime power) which is not an hyperoval, contains at most $n-\sqrt{n}+1$ points. This theorem is sharp for $n=q^2$. In fact, in $PG(2,q^2)$, with either q odd or even, a class of $(q^2-q+1)-$arcs were constructed in [1] and many authors proved their completeness, (see [2], [3],[4]). The arcs constructed by Kestenband are referred to as unital-derived arcs because they are the common intersection of $q+1$ hermitian unitals of $PG(2,q^2)$. Under certain circumstances, the set of points of a hermitian unital of $PG(2,q^2)$ constitutes the set of points of a unital in the Hall plane of the same order, $H(q^2)$, [5],[6]. Applying these results, a suitable choice of complete unital-derived arcs of $PG(2,q^2)$ allows to construct a class of complete arcs with q^2-q+1 points in the Hall plane $H(q^2)$. These arcs are still the intersection of $q+1$ unitals of $H(q^2)$. When it is $q^2=9$, the same construction gives rise also to a class of complete q^2-q+2-arcs of $H(9)$.

References

[48] B.C. Kestenband: *Unitals intersections in finite projective planes*, Geom. Ded. **11** (1981), 107-117.

[49] B.C. Kestenband: *A family of complete arcs in finite projective planes*, Colloq. Math. **57**, (1989), 56-67.

[50] J.C. Fisher, J.W.Hirschfeld, J.A.Thas: *Complete arcs in planes of square order*, Ann. Discrete Math. **30** (1986), 246-250.

[51] E. Boros, T.Szönyi: *On the sharpness of a theorem of B.Segre*, Combinatorica **6**, (3), (1986), 261-268.

[52] S. Barwick: *Unitals in the Hall Planes*, J. Geom. **58** (1997), no.1-2, 26-42.

[53] G. Rinaldi: *Hyperbolic Unitals in the Hall Planes*, J. Geom. **54** (1995),148-154.

Specialized Colourings of Steiner systems $S(2,4,v)$

Alexander Rosa*, S. Milici, V. Voloshin

McMaster University - Ontario, Canada
e-mail: rosa@mcmail.cis.mcmaster.ca

We consider colourings of Steiner systems $S(2,4,v)$ in which blocks have prescribed colour patterns, as a refinement of the classical weak colourings. We study the question of the existence of a colouring of given type in which exactly k colours are used, as well as the question of the existence of uncolourable systems. We also examine the related question of the existence of $S(2,4,v)$ with maximal arcs.

Hopf Algebras and the Penrose Polynomial

I. Sarmiento

Department of Mathematics and Computer Science
Free University of Berlin - Arnimallee 3, D-14195 Berlin, Germany
e-mail: sarmient@math.fu-berlin.de

Let λ be a positive integer and let G be a plane graph. Let $P(G, \lambda)$ be the Penrose polynomial of G. We will present an interpretation of $P(G, -\lambda)$ in terms of colourings of G. In order to prove our main theorem we construct a Hopf algebra $\mathcal{A}$ of graphs and an homomorphism of Hopf algebras P from $\mathcal{A}$ onto a Hopf algebra of polynomials in one indeterminate. If G is a plane graph, then $P(G)$ coincides with the Penrose polynomial of G.

Expectation Values for Codes over Rings

S.E. Schmidt

M.I.T., USA

e-mail: schmidt@math.mit.edu

For any finite ring R we construct a real-valued function w on R with $w(0) = 0$ such that the expectation value of w restricted to R_x (with repect to the uniform distribution) is 1 for all non-zero elements x of R. For our main result we additively extend w to a real-valued function on powers of R; then a large class of rings allows the following surprising statement.

THEOREM. *For any linear code C over a finite Frobenius ring, the expectation value of w restricted to C is given by the reduced length of C.*

Finally, we derive some remarkable applications which underline the importance of Frobenius rings for future coding theory.

Maximally Valued Division Algebras

E. Schörner

University of München, Germany

e-mail: schoerne@rz.mathematik.uni-muenchen.de

By a well–known result of Kaplansky, a valued field (K, v, Γ) is maximal if and only if any pseudoconvergent sequence has a pseudolimit in K; moreover, under the "Hypothesis A", (K, v, Γ) is isomorphic to a Hahn field of formal power series with a factor system. The equivalence of maximality and pseudocompleteness can also be shown for valued abelian groups and certain classes of valued modules as well as for ultrametric spaces with totally ordered value set; it is still an open question for valued skewfields. In this talk we will present the positive result for valued division algebras in the sense of Zelinsky having the same characteristic as its residue division algebra.

On Divisible Designs with Dual Translation Group

R.-H. Schulz*, S. Giese

Mathematisches Institut - Freie Universität Berlin - Berlin, Germany
e-mail: schulz@math.fu-berlin.de

We characterize divisible designs D which admit an elementary abelian full dual translation group, that means an elementary abelian automorphism group T of D fulfilling the following conditions.

(i) T fixes all point–classes of D.
(ii) T operates transitively on every point class of D.
(iii) $T_p \neq T_Q$ for all points P, Q of different point classes of D.

Line-transitive Point-imprimitive Linear Spaces

M. Sebille

Département de Mathématiques - Campus Plaine C.P. 216 - Université Libre de Bruxelles
Boulevard du Triomphe - B - 1050 Bruxelles, Belgium
e-mail: `msebille@cso.ulb.ac.be`

A **linear space** $S(2,k,v)$ is a pair $(X,\mathcal{B})$, where X is a set of v elements called **points** and $\mathcal{B}$ is a collection of k-subsets of X (called **lines**) such that every 2-subset of X is contained in one line (we also assume that $2 < k < v$).

In 1989, A. Delandtsheer and J. Doyen proved that if G is a line-transitive point-imprimitive automorphism group of a linear space $S(2,k,v)$, then v is bounded by a function $f(k) = (\binom{k}{2} - 1)^2$ depending only on the size of the lines. In 1992, P. Cameron and C. Praeger proved that if G is a line-transitive point-imprimitive automorphism group of an $S(2,k,f(k))$, then $k \in \{4,5,8\}$ and, the same year, W. Nickel, A. Niemeyer, C. O'Keefe, C. Praeger and T. Penttila proved that under the same hypotheses, $k = 8$ and there exist, up to isomorphism, exactly 446 such linear spaces.

The purpose of this talk is to give a new bound $B(k,i)$ for the number of points of a line-transitive point-imprimitive linear spaces depending not only on the size of the lines but also on the number i of unordered pairs of points contained in a given line and incident with only one imprimitivity class. We investigate the cases $i = 2$ and $i = 3$, and we construct an infinite family of $S(2,k,B(k,i))$.

This work is supported by the Belgian F.R.I.A. (Fonds pour la formation à la Recherche dans l'Industrie et dans l'Agriculture).

Partial Spreads in *PG*(4,2): Sym(6) Aspects

R. Shaw

Dept. of Mathematics - University of Hull
Hull HU6 7RX, UK
e-mail: `r.shaw@maths.hull.ac.uk`

Recently, see `http://www.hull.ac.uk/maths/research/2000/`, it has been proved that there exist 64 equivalence classes of partial spreads in $PG(4,2)$. In this paper we make use of aspects of the group isomorphisms $Sp(4,2)$ $Sym(6)$ and $O(5,2)$ $Sym(6)$ to give descriptions of roughly half of these classes. In particular we describe how to distinguish simply between the three classes of maximal partial spreads of size 7 by using $Sp(4,2)$ considerations. Similarly for those two classes of maximal partial spreads of size 9 which are of regulus type IΔ.

Multilinear Representability of Matroids

J. Simonis

Eindhoven University of Technology, The Netherlands
e-mail: j.simonis@twi.tudelft.nl

Linear representability of matroids is an old and well-researched subject. Recently, a more fundamental notion of matroid representability has emerged: almost-affine representability or representability by partitions.

There are several almost-affinely representable matroids that are not linearly representable. Some examples, notably the non-Pappus matroid and the exceptional 10_3-configuration, will be presented. Also the relation with quasigroups and the remarkable fact that all known examples happen to be multilinearly representable will be discussed.

Complete Arcs Arising from Conics

A. Sonnino
Università della Basilicata - Potenza, Italy
e-mail: sonnino@unibas.it

By a result going back to B. Segre and L. Lombardo Radice, the maximum number of points shared by an irreducible conic $\mathcal{C}$ and a k-arc K in $\mathrm{PG}(2,q)$ is $\frac{1}{2}(q+3)$ for q, and $\frac{1}{2}(q+2)$ for q even. If the maximum is attained, then K only contains a few points outside $\mathcal{C}$. This was showed in two long papers by G. Pellegrino who mostly used synthetic arguments related to certain axial correspondences. The aim of this talk is to present a different approach based on polynomials and linear collineations. A new proof will be given for the following result due originally to G. Korchmáros:

Let K be a complete k-arc in $PG(2,q)$, q odd, containing $\frac{1}{2}(q+3)$ points from an irreducible conic $\mathcal{C}$ of $PG(2,q)$. If $\frac{1}{2}(q+1)$ is a prime, then K contains at most four points outside $\mathcal{C}$. If $q^2 \equiv 1 \pmod{16}$, then this number can be at most two.

Caps in *PG*(5,3) and *PG*(6,3)

L. Storme*, J. Barát, Y. Edel, R. Hill, C. Jones, I. Landjev

University of Gent - Dept. of Pure Maths and Computer Algebra
Krijgslaan 281 - 9000 Gent, Belgium
e-mail: `ls@cage.rug.ac.be`

A *k-cap* in $PG(N,q)$ is a set of k points, no three of which are collinear. A k-cap is called *complete* when it is not contained in a larger cap.

The maximal size of a cap in $PG(5,3)$ is 56 and there is a unique example found by R. Hill. This 56-cap in $PG(5,3)$ can be used to construct a 112-cap in $PG(6,3)$, which is the largest known cap in $PG(6,3)$. Until two years ago, the best known upper bound on the size of a cap in $PG(6,3)$ was 164.

In [R. Hill, I. Landjev, C. Jones, L. Storme and J. Barát, *On complete caps in the projective geometries over* $\mathbf{F}_3$. Proceedings of the *Second Pythagorean Conference*, (Samos, Greece, May 30-June 5, 1999), J. Geom., to appear], a first study to improve the upper bound on the size of a cap in $PG(6,3)$, and to find the size of the second largest complete caps in $PG(5,3)$, was made.

Since 1999, a new approach involving computer searches has been used. The searches show that the size of the second largest complete caps in $PG(5,3)$ is equal to 48, and this latter result improves the upper bound on the size of caps in $PG(6,3)$ to 147.

Covers and Caps of the Klein Quadric $Q^+(5,q)$

P. Sziklai*, J. Eisfeld, L. Storme, A. Blokhuis

University of Budapest, Hungary
e-mail: sziklai@cs.elte.hu

A t-cover of a quadric Q is a set $\mathcal{C}$ of t-dimensional subspaces contained in Q such that every point of Q belongs to at least one element of $\mathcal{C}$. Here 1- and 2-covers of the Klein quadric $Q^+(5,q)$ are considered. For $t = 2$, a 2-cover contains at least $q^2 + q$ planes, and the extremal configuration can be described explicitly. As (via Plücker coordinates) there is a well-known bijection between the points of the Klein quadric and the *lines* of $PG(3,q)$, it gives a description of sets $\mathcal{C}$ containing points and lines, blocking all lines of $PG(3,q)$. Note that if $\mathcal{C}$ contains points only (or, dually, planes) of $PG(3,q)$, then the lower bound is $q^2 + q + 1$.

For $t = 1$, a 1-cover of $Q^+(5,q)$ has at least $q^3 + 2q + 1$ lines; some examples of this size will be presented as well.

As three points of the Klein quadric are collinear if and only if the corresponding three lines are concurrent *and* coplanar in $PG(3,q)$, a cap (i.e. a set of points, no three of which being collinear) contained in $Q^+(5,q)$ corresponds to a set $\mathcal{L}$ of lines in $PG(3,q)$ such that no three of which are concurrent and coplanar at the same time. It is easy to prove that $|\mathcal{L}| \leq (q+1)(q^2+1)$ if q is odd and $|\mathcal{L}| \leq (q+2)(q^2+1)$ if q is even. In the first case this bound is sharp.

On the other hand, it can be proved, that a complete cap (i.e. which is not contained in a larger cap) of the Klein quadric has size $\geq q^{3/2}$. A better bound will be presented as well.

On Blocking Sets in Higher Dimension

T. Szőnyi, Zs. Weiner*

Eotvos University - Budapest, Hungary
e-mail: weiner@cs.elte.hu

A *k-blocking set* in $PG(n,q)$ is a set of points such that it intersects every $(n-k)$-dimensional subspace. It is *non-trivial* if no k-dimensional subspace is contained in it; it is *minimal* when no proper subset of it is a k-blocking set. 1-blocking sets for $n=2$ will be called *planar*. We call a k-blocking set in $PG(n,q)$ *small*, if its size is less than $\frac{3}{2}(q^{(n-k)}+1)$.

For planar minimal blocking sets their size can only lie in certain (relatively short) intervals, each of which correspond to a value e, for some $1 \leq e \leq h/2$. When $p^e \neq 4, 8$, each line intersects the minimal blocking set in 1 modulo p^e points.

We generalize the above result for k-blocking sets, furthermore we also present some corollaries.

On *m*-ary Balanced Codes

L.G. Tallini

Dipartimento Di. Tec. - Politecnico di Milano,
20133 Milano, Italy
e-mail: luca.tallini@polimi.it

A m-ary balanced code with r check digits and k information digits is a code over the alphabet $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ of length $n = k + r$ and cardinality m^k such that each codeword is balanced; that is, the real sum of its components (or weight) is equal to $\lfloor (m-1)n/2 \rfloor$. This paper contains new efficient methods to design m-ary balanced codes which improve the constructions found in the literature, for all alphabet size $m \geq 2$. To design such codes, the information words which are close to be balanced are encoded using single maps obtained by a new generalization of Knuth's complementation method to the m-ary alphabet that we introduce in this paper. Whereas, the remaining information words are compressed via suitable m-ary uniquely decodable variable length codes and then balanced using the saved space. For any $m \geq 2$, a family of m-ary balanced codes can be obtained whose number of redundant digits is

$$r = \log_m k - \frac{1}{2} \log_m s(k) + O(1),$$

where $s = s(k)$ is any function of k such that $1 \leq s(k) \leq k$. Such family of codes can be implemented with $O(mk \log_m k + mks)$ m-ary digit operations and $O(k + ms^3)$ memory elements to store m-ary digits.

On Groups Whose Inner Automorphism Nearring is a Ring

M.J. Thomsen

Universität der Bundeswehr - Hamburg, Germany
e-mail: momme.thomsen@unibw-hamburg.de

Familiar algebraic structures are endomorphism rings, i.e. subrings of the full endomorphism ring $(\operatorname{End} G, +, \circ)$ determined by a given abelian group G. The structure of a given group G is reflected in the structure of its associated endomorphism rings and vice versa.

Endomorphism rings are subrings of the nearring $(\mathrm{M}(G), +, \circ)$ consisting of all mappings from G to G which are defined for every group G. $(\mathrm{M}(G), +, \circ)$ is called the full transformation nearring on G. Transformation nearrings on G, i.e. subnearrings of $(\mathrm{M}(G), +, \circ)$ are very general in the sense that every nearring can be embedded into a full transformation nearring on a suitable group G.

In the talk we concentrate on the so-called inner automorphism nearring $(\mathrm{I}(G),\ +,\ \circ)$ which is the subnearring of $(\mathrm{M}(G),\ +,\ \circ)$ generated by the group $(\mathrm{Inn}\ G,\ \circ)$ of all inner automorphisms of G.

We characterize in several ways those groups for which $(\mathrm{I}(G),\ +,\ \circ)$ is a ring and also those groups for which $(\mathrm{I}(G),\ +,\ \circ)$ is even a commutative ring. We explain how these properties are related to the property "G is of nilpotency class 2" and "G is of nilpotency class 3" and "G has elements of order 3".

A Mass Formula for Steiner Triple Systems $STS(2^{n-1})$ of 2-rank $2^n - n$

V.D. Tonchev

Michigan Technological University - Houghton, Michigan 49931, USA
http://www.math.mtu.edu/∼tonchev

A formula is found for the total number of distinct Steiner triple systems on $2^n - 1$ points whose 2-rank is one higher than the possible minimum $2^n - n - 1$. The formula can be used for deriving bounds on the number of pairwise nonisomorphic systems for large n, and for the classification of all nonisomorphic systems of small orders. It is proved that the number of nonisomorphic Steiner triple systems on $2^n - 1$ points of 2-rank $2^n - n$ grows exponentially.

Simultaneous Reduction of a Pair of Symmetric Bilinear Forms to Canonical Form

M.A. Vaccaro

Dipartimento di Matematica ed Applicazioni - Università di Palermo
Via Archirafi, 34, I-90123 Palermo
e-mail: vaccaro@dipmat.math.unipa.it

We try to classify pairs of symmetric bilinear forms on a finitely generated vector space over a field K of characteristic $\neq 2$. We give a complete classification in the case where the algebraic closure of K is a quadratic extension of K.

Classical Varieties and Codes

R. Vincenti

Università di Perugia - Perugia, Italy
e-mail: alice@unipg.it

It is well known that every projective variety, read as a projective multiset, can represent an algebraic code. In this paper we study from this point of view the Schubert varieties and the cubic surfaces V of $PG(4,q)$. It has been shown by many authors that a Grassmannian variety $G = G(m,d)$ of $PG(N-1,q)$ is a code of length equal to the number of rational points of G, of dimension N, and of minimum distance $q((m-d)d)$. The Schubert varieties are special varieties of G, who can represent a basis for the subvarieties of G of same dimension. A cubic surface V of $PG(4,q)$ can be built by means of a birational mapping between a line and a conic not lying in the same plane.

Infinite Permutation Groups with Nice Transitivity Properties

H. Wefelscheid

Universität-Gesamthochschule-Duisburg
e-mail: `wefelscheid@mat.uni-duisburg.de`

The transitivity properties, we have in mind are related with the names of Frobenius, Zassenhaus und Suzuki.

Beginning with doubly transitive Frobenius and with triply transitive Zassenhaus groups (e.e. sharply 2-transitive, resp. sharply 3-transitive permutation groups) we compare those properties which might be valid in the infinite case as well as in the finite case and examine properties which are only possible in the infinite case.

The literature about infinite Frobenius and infinite Zassenhaus groups is only small and the research can be devided into to lines: whether the theorem of Frobenius is valid or not. We concentrate our interest into the latter, more general case, present some (nontrivial) examples, and exhibit the connection to K-Loops.

Relations between Certain Classes of Incidence Loops, Codes and Chain Structures

E. Zizioli

Università Cattolica - Brescia, Italy
e-mail: geomet@dmf.bs.unicatt.it

The loops $(L, +)$ which are derived from non euclidean geometries ([1]) enjoy the following properties:

C1. For each $a \in L^* := L \setminus \{0\}$, the centralizer $Z(a) := \{x \in L \,|\, x + a = a + x\}$ is a subgroup of $(L, +)$.

C2. The set $\mathcal{F} := \{Z(a) \,|\, a \in L^*\}$ is an incidence fibration in the sense of [2] (hence $\mathcal{F}^* := \{X^* |\, X \in \mathcal{F}\}$ is a partition of L^*).

The task now arises of studying classes of abstract loops $(L, +)$ satisfying C1 and C2. Here I shall focus my attention to the subclass characterized by

C3. For each $a \in L^*, |Z(a)| = 2$.

These loops can be related via chain structures to a certain class of MDS codes.

References

[54] H.Karzel: *Recent developements on absolute geometries and algebraization by K-loops*, Discr.Math.**208/209** (1999), 387-409.

[55] E.Zizioli: *Fibered incidence loops and kinematic loops*, J.Geom. **30** (1987),144-156.