

Algebraic Geometry Codes

Basic Notions

Michael Tsfasman

Serge Vlăduț

Dmitry Nogin

PONCELET LABORATORY (CNRS AND INDEPENDENT UNIVERSITY OF MOSCOW); INSTITUT DE MATHÉMATIQUES DE LUMINY; INSTITUTE FOR INFORMATION TRANSMISSION PROBLEMS

E-mail address: `tsfasman@iml.univ-mrs.fr`

INSTITUT DE MATHÉMATIQUES DE LUMINY; INSTITUTE FOR INFORMATION TRANSMISSION PROBLEMS

E-mail address: `vladut@iml.univ-mrs.fr`

INSTITUTE FOR INFORMATION TRANSMISSION PROBLEMS

E-mail address: `nogin@iitp.ru`

2000 *Mathematics Subject Classification*. Primary 14H, 94B, 14G15, 11R58;
Secondary 11T23, 11T71

Our research while working on this book was supported by the French National Scientific Research Center (CNRS), in particular by the Institut de Mathématique de Luminy and the French–Russian Poncelet laboratory, by the Institute for Information Transmission Problems, and by the Independent University of Moscow. It was also supported in part by the Russian Foundation for Basic Research, projects 99-01-01204, 02-01-01041, and 02-01-22005, and by the program Jumelage en Mathématique.

Contents

Preface	ix
Advice to the Reader	xvii
Chapter 1. Codes	1
1.1. Codes and Their Parameters	1
1.1.1. Definition of a Code	1
1.1.2. $[n, k, d]_q$ Systems	3
1.1.3. Spectra and Duality	7
1.1.4. Bounds	15
1.1.5. Bounds for Higher Weights	21
1.1.6. Duality for Generalized Spectra	29
1.2. Examples and Constructions	33
1.2.1. Codes of Genus Zero	33
1.2.2. Some Code Families	36
1.2.3. Some Constructions	44
1.3. Asymptotic Problems	49
1.3.1. Main Asymptotic Problem	49
1.3.2. Asymptotic Bounds	51
1.3.3. Asymptotic Bounds for Higher Weights	57
1.3.4. Polynomiality	60
1.3.5. Other Asymptotics	64
Historical and Bibliographic Notes	67
Chapter 2. Curves	71
2.1. Algebraic Curves	71
2.1.1. Quasi-projective Varieties	72
2.1.2. Quasi-projective Curves	79
2.1.3. Divisors	81
2.1.4. Jacobians	88
2.1.5. Riemann Surfaces	90
2.2. Riemann–Roch Theorem	93
2.2.1. Differential Forms	93
2.2.2. Riemann–Roch Theorem	97
2.2.3. Hurwitz Formula	102
2.2.4. Special Divisors	104
2.2.5. Cartier Operator	106
2.3. Singular Curves	108
2.3.1. Normalization	108

2.3.2.	Double-Point Divisor	109
2.3.3.	Plain Curves	110
2.4.	Elliptic Curves	113
2.4.1.	Group Law	113
2.4.2.	Isomorphisms and the j -invariant	116
2.4.3.	Isogenies	117
2.4.4.	Complex Elliptic Curves	120
2.5.	Curves over Non-Closed Fields	122
2.5.1.	Function Fields	122
2.5.2.	Places of a Function Field	124
2.5.3.	Divisors	127
2.5.4.	Function Fields and Algebraic Curves	128
	Historical and Bibliographic Notes	133
Chapter 3.	Curves over Finite Fields	135
3.1.	Zeta Function	135
3.1.1.	Definition and Rationality	136
3.1.2.	Functional Equation	140
3.1.3.	Weil Theorem and Its Corollaries	143
3.1.4.	Explicit Formula	145
3.1.5.	Pellikaan's Two-Variable Zeta Function	146
3.2.	Asymptotics	148
3.2.1.	Drinfeld–Vlăduț Theorem	148
3.2.2.	Lower Asymptotic Bounds	149
3.2.3.	Points of Higher Degrees	149
3.2.4.	Asymptotics for the Jacobian	151
3.2.5.	Asymptotically Exact Families	153
3.3.	Elliptic Curves over Finite Fields	160
3.3.1.	Isomorphism Classes	160
3.3.2.	Isogeny Classes	163
3.3.3.	Endomorphism Ring and the Zeta Function	164
3.3.4.	Structure of $E(\mathbb{F}_q)$	165
3.4.	Some Remarkable Examples	167
3.4.1.	Hermitian, Sub-Hermitian, and Maximal Curves	167
3.4.2.	Kummer and Artin–Schreier Covers	169
3.4.3.	García–Stichtenoth Towers	179
3.4.4.	Curves of Small Genera	180
3.5.	Connection with Exponential Sums	182
3.5.1.	Number of Points on Fermat Curves	182
3.5.2.	L -functions of Characters	183
3.5.3.	Estimates for Exponential Sums	185
	Historical and Bibliographic Notes	189
Chapter 4.	Algebraic Geometry Codes	193
4.1.	Constructions and Properties	193
4.1.1.	Basic Algebraic Geometry Constructions and Their Parameters	194
4.1.2.	Duality and Spectra	200
4.1.3.	Decoding Problem	205

4.2.	Additional Bounds and Constructions	209
4.2.1.	Some Extra Bounds	209
4.2.2.	Variants of the Basic Construction	219
4.2.3.	Partial Algebraic Geometry Codes	222
4.3.	Characterization of Algebraic Geometry Codes	228
4.3.1.	Three AG Levels	228
4.3.2.	All Linear Codes Are Weakly AG	229
4.3.3.	Criteria	231
4.4.	Examples	235
4.4.1.	Codes of Small Genera	235
4.4.2.	Elliptic Codes	237
4.4.3.	Hermitian Codes	244
4.4.4.	Other Examples	248
4.4.5.	Some Generalized Algebraic Geometry Codes	249
4.5.	Asymptotic Results	253
4.5.1.	The Basic Algebraic Geometry Bound and Its Variants	253
4.5.2.	Expurgation Bound and Codes with Many Light Vectors	256
4.5.3.	Constructive Bounds	266
4.5.4.	Other Bounds	269
4.6.	Non-linear Algebraic Geometry Constructions	274
4.6.1.	Elkies Codes	274
4.6.2.	Xing Codes	283
	Historical and Bibliographic Notes	287
Appendix A. Summary of Results and Tables		289
A.1.	Codes of Finite Length	289
A.1.1.	Bounds	289
A.1.2.	Parameters of Some Codes	290
A.1.3.	Parameters of Some Constructions	291
A.2.	Asymptotic Bounds	295
A.2.1.	List of Bounds	295
A.2.2.	Comparison Diagrams	298
A.2.3.	Behaviour at the Endpoints	301
A.2.4.	Numerical Values	301
A.3.	Additional Bounds	309
A.3.1.	Constant-Weight Codes	309
A.3.2.	Self-dual Codes	309
A.3.3.	Bounds for Higher Weights	310
Appendix B. Tables of Curves with a Large Number of Points		313
<i>(G. van der Geer, M. van der Vlugt)</i>		
B.1.	Introduction	313
B.2.	The Tables	316
Appendix C. Tables of Linear Codes		325
<i>(A. E. Brouwer)</i>		
C.1.	Code Parameters for $q = 2$	326
C.2.	Code Parameters for $q = 3$	335
C.3.	Code Parameters for $q = 4$	348

C.4. Code Parameters for $q = 5$	353
C.5. Code Parameters for $q = 7$	356
C.6. Code Parameters for $q = 8$	357
C.7. Code Parameters for $q = 9$	359
Bibliography	363
List of Names	385
Index	389