

Luca Giuzzi

Codici correttori

Un'introduzione

 Springer

Indice

Prefazione	XI
------------------	----

Introduzione	XIII
--------------------	------

Parte I Teoria generale

1 Teoria della comunicazione	3
1.1 Sistemi di comunicazione	3
1.2 Il caso privo di rumore	4
1.3 Il caso con rumore	8
1.4 Modelli di canale	10
1.5 Conclusioni	16
2 Protocolli e codici	17
2.1 Comunicazione a pacchetto	18
2.2 Alfabeti	20
2.3 Codici a lunghezza variabile	25
2.4 Adattamento dei codici alla sorgente	30
Esercizi	33
3 Codici a blocchi	35
3.1 Blocchi di informazione	35
3.2 Metrica di Hamming	36
3.3 Algoritmi di codifica e decodifica	37
3.4 Efficienza di un codice	40
3.5 Distanza minima	41
3.6 Limitazioni	45
3.7 Codici equivalenti	48
Esercizi	51

Parte II Codici lineari

4	Codici lineari	55
4.1	Generalità	56
4.2	Codici lineari astratti	57
4.3	Proprietà dei codici lineari	59
4.4	Matrice generatrice di un codice lineare	61
4.5	Equivalenza e isomorfismo	63
4.6	Ortogonalità e codice duale	72
4.7	Controllo di parità	77
4.8	Enumeratori dei pesi	78
4.9	Codici di Hamming	83
4.10	Decodifica del codice di Hamming binario	85
4.11	Decodifica mediante matrice standard	86
4.12	Decodifica assistita con sindrome	89
4.13	Codici lineari e canali di comunicazione	93
4.14	Alcune limitazioni sui codici lineari	96
	Esercizi	101
5	Codici ciclici	103
5.1	Sottospazi ciclici	103
5.2	Rappresentazione mediante polinomi	104
5.3	Polinomio generatore di un codice ciclico	107
5.4	Matrice generatrice di un codice ciclico	109
5.5	Polinomio di controllo di parità	110
5.6	Codifica dei codici ciclici	113
5.7	Decodifica dei codici ciclici	115
	Esercizi	122
6	Radici e idempotente di un codice ciclico	125
6.1	Radici di un codice ciclico	125
6.2	Idempotente di un codice ciclico	128
6.3	Classi ciclotomiche e codici ciclici minimali	130
6.4	Insiemi di definizione	133
6.5	Descrizione dei codici ciclici mediante traccia	137
	Esercizi	138
7	Errori concentrati o burst	139
7.1	Descrizione dei burst di errore	140
7.2	Limitazioni	142
7.3	Campi di ordine non primo	144
7.4	Codici ciclici per errori burst	145
7.5	Codici fortemente correttori e codici di Fire	150

Esercizi	153
8 Trasformata di Fourier e codici BCH	155
8.1 Trasformata di Fourier e polinomio di Mattson-Solomon	155
8.2 Costruzione BCH	158
8.3 Descrizione compressa dell'errore	161
8.4 L'equazione chiave	162
8.5 Polinomio sindrome per codici BCH	165
8.6 L'algoritmo Euclideo Esteso	167
8.7 Decodifica dei codici BCH	172
Esercizi	175
9 Codici di Reed-Solomon	177
9.1 Costruzione di Reed-Solomon	177
9.2 Codifica e decodifica dei codici di Reed-Solomon	180
9.3 Il problema della correzione	180
9.4 Algoritmo di Welch-Berlekamp	182
9.5 Codici di Reed-Solomon come BCH	184
9.6 Decodifica a lista	189
9.7 Decodifica a lista dei codici di Reed-Solomon	190
9.8 Applicazioni dei codici di Reed-Solomon	195
Esercizi	196
10 Cancellature o erasures	199
10.1 Il canale q -ario con cancellatura	199
10.2 Decodifica di cancellature	200
10.3 Codici di Reed-Solomon e canali con cancellatura	202
Esercizi	207
11 Disegni e codici	209
11.1 Strutture di incidenza	209
11.2 Disegni	211
11.3 Matrici di incidenza	215
11.4 Piani proiettivi	219
11.5 Codici da disegni	220
11.6 Piani proiettivi e codici	223
Esercizi	226
12 Codici di Golay	227
12.1 Codice di Golay binario esteso e disegni di Mathieu	227
12.2 Unicità del $(24, 2^{12}, 8)$ -codice binario	231
12.3 Codice binario di Golay	234
12.4 L'esacodice e la codifica del codice di Golay	237
12.5 Decodifica a logica di maggioranza	239
12.6 Codice ternario di Golay	239

Esercizi	242
13 Codici di Reed-Müller	243
13.1 Codici di Reed-Müller q -ari	243
13.2 Il caso binario	245
13.3 Codici del primo ordine	247
13.4 Codice ortogonale	248
13.5 Geometria e codici di Reed-Müller	251
Esercizi	252
14 Modifica e combinazione di codici	253
14.1 Accorciamento	253
14.2 Estensione	255
14.3 Allungamento	256
14.4 Punzonatura	257
14.5 Aumento e epurazione	258
14.6 Condivisione temporale	258
14.7 Somma	260
14.8 Codifica seriale	260
14.9 Costruzione $u v$	261
14.10 Codici prodotto	262
14.11 Intrecciamento	265
Esercizi	266
15 Limitazioni asintotiche	267
15.1 Famiglie di codici	267
15.2 Limitazioni universali sui codici	268
15.3 Insiemi di Wozencraft	277

Parte III Argomenti avanzati

16 Codici Algebrico-Geometrici	283
16.1 Codici di valutazione	283
16.2 Costruzione dei codici geometrici	285
16.3 Stime sui codici geometrici	288
16.4 Codice Hermitiano	290
16.5 Sequenze di codici asintoticamente buone	292
16.6 Decodifica dei codici di Goppa	295
17 Codici LDPC e grafi di Tanner	299
17.1 Matrici sparse e grafi	299
17.2 Grafi di Tanner	300
17.3 Codici LDPC	302
17.4 Grafi espansori	304

17.5	Decodifica mediante scambio sequenziale	305
18	Codici convoluzionali	309
18.1	Motivazione	309
18.2	Codificatori convoluzionali	310
18.3	Funzioni generatrici	313
18.4	Matrici generatrici	315
18.5	Traliccio di Wolf e codici lineari	317
18.6	Decodifica di Viterbi per codici lineari	320
18.7	Tralicci per codici convoluzionali	323
<hr/>		
Parte IV Appendici		
<hr/>		
A	Campi finiti	327
A.1	Anelli	327
A.2	Campi	330
A.3	Anelli di polinomi	332
A.4	Estensioni di campo	336
A.5	Struttura dei campi finiti	340
A.6	Polinomi irriducibili su campi finiti	343
A.7	Automorfismi di un campo finito	345
A.8	Traccia e norma	346
A.9	Radici dell'unità e polinomi ciclotomici	348
B	Geometria proiettiva e Curve algebriche	351
B.1	Spazi affini e proiettivi	351
B.2	Insiemi algebrici e varietà	353
B.3	Funzioni razionali	354
B.4	Curve	355
B.5	Divisori	356
B.6	Il genere e il teorema di Riemann-Roch	357
Soluzioni degli esercizi		
	Capitolo 2	359
	Capitolo 3	361
	Capitolo 4	363
	Capitolo 5	364
	Capitolo 6	365
	Capitolo 7	367
	Capitolo 8	368
	Capitolo 9	371
	Capitolo 10	374
	Capitolo 11	379

X **Indice**

Capitolo 12	381
Capitolo 13	383
Capitolo 14	384
Bibliografia	387
Elenco dei simboli	393
Indice analitico	397