
Inhaltsverzeichnis

1	Aufgabenstellung und Ziel	1
1.1	Beispiele für Codes	1
1.2	Ein Schnupperkurs	4
1.2.1	Verschlüsselung	6
1.2.2	Fehlerbeseitigung	7
1.2.3	Kompression	10
1.3	Begriffe aus der Informations- und Nachrichtentechnik	11
1.4	Aufgabenstellung	21
1.5	Ziel	25
1.6	Was blieb?	26
2	Mathematische Hilfsmittel	27
2.1	Ein paar Begriffe aus Algebra und Wahrscheinlichkeitsrechnung	27
2.2	Weitere mathematische Hilfsmittel	30
2.3	Was blieb?	42
3	Fehlerbeseitigung	43
3.1	Der Prozess der Fehlerentstehung und seine Auswirkungen auf die Informationsübertragung	43
3.1.1	Wie wird die Leistung der Fehlerbeseitigung dargestellt? Der Codierungsgewinn = Coding Gain	44
3.1.2	Was sind Fehler und wie entstehen sie?	45
3.1.3	Welche Ergebnisse lassen sich mit Fehlerkorrektur-Verfahren erzielen?	50
3.1.4	HD und SD: Hard- und Softdecision-Decodierung	56
3.1.5	Versuch einer kleinen Systematik	70
3.2	Die Prüfstellen: Notwendige und hinreichende Bedingungen für die Korrektur mit dem Hard Decison-Verfahren	72
3.3	Direkte Nutzung des Hammingabstandes	75
3.4	Hamming-Code	77
3.4.1	Aufbau, Codierung und Hard Decision-Decodierung	77
		IX

3.4.2	Generatormatrix G	81
3.4.3	Paritätsprüfmatrix H	82
3.4.4	Syndrom und Fehlerposition bei HD-Decodierung	82
3.4.5	Technischer Gebrauch des Hamming-Codes	85
3.4.6	Was blieb?	86
3.5	Leistungsbeurteilung von Codes	87
3.5.1	Beschreibung fehlerbehafteter Übertragungssysteme	87
3.5.2	Verteilung der Fehler auf die Codewörter	90
3.5.3	Einfluss der Informationsrate auf die Übertragungsrate	93
3.5.4	Kriterien: Asymptotisches Verhalten bei langen Codes	96
3.5.5	Ein Beispiel	98
3.5.6	Grenzen: Das Theorem von Shannon	100
3.5.7	Was blieb?	112
3.6	Erweiterungen des Hamming-Verfahrens	112
3.6.1	Verallgemeinerung auf andere Ganzzahlbasen	112
3.6.2	Erweiterung um zusätzliche Fehlererkennung	116
3.6.3	Was blieb?	119
3.7	Zyklische Codes	119
3.7.1	Der Weg und die Mittel: Generatorpolynome und Reste	120
3.7.2	Bildung der Codewörter	121
3.7.3	Generatorpolynom, irreduzible Polynome und Dekodierung	129
3.7.4	Generatorpolynome für Mehrbitfehler-Korrektur	133
3.7.5	Eignungstest für $g(x)$ zur t -Bitfehlerkorrektur	135
3.7.6	Irreduzible Polynome über Z_2 und Galoisfelder $GF(2^m)$	137
3.7.7	BCH-Code	142
3.7.8	Reed-Solomon-Code für Mehrfach-Bündelfehler-Korrektur	157
3.7.9	Vergleich zwischen BCH- und Reed-Solomon-Codes	169
3.7.10	Erkennung von Einzelfehlern und Fehlerbündeln	171
3.7.11	Was blieb?	175
3.8	Hinweis zum Goppa-Code	176
3.9	Reed-Muller-Code	176
3.10	Interleaving	186
3.11	Produkt-Codes	189
3.12	Maximum a Posteriori-Prinzip und Turboprodukt-Codes	195
3.13	LDPC-Codes	207
3.14	Faltungs-Codes (Convolutional Codes)	216
3.14.1	Codewortaufbau und HD-Decodierung	216
3.14.2	SD-Decodierung mit dem Viterbi-Verfahren	225
3.14.3	SD-Dekodierung mit dem BCJR-Verfahren	227
3.14.4	Hinweise zum BCJR-Algorithmus	234
3.14.5	Was blieb?	240

4	Rückgekoppelte Schieberegister	243
4.1	Eigenschaften	243
4.2	Fehlerbeseitigung durch Kreuzkorrelation	257
4.3	Zufallserzeugung von Schlüsselwörtern	260
4.4	Was blieb?	268
5	Datenverschlüsselung	271
5.1	Datenverschlüsselung zur Informationssicherung	272
5.2	Verschlüsselung nach dem Data-Encryption-Standard (DES)	274
5.3	Hinweise zum Advanced Encryption Standard AES	285
5.4	Verschlüsselung mit dem RSA-Algorithmus	287
5.5	Verschlüsselung mit dem Verfahren der elliptischen Kurven	295
5.5.1	Allgemeines	295
5.5.2	Berechnungsvorschrift $2P = P + P$	297
5.5.3	Berechnungsvorschrift $R = P + Q$ bei $P \neq Q$	298
5.5.4	Beispiel	298
5.6	Das Rechnen mit großen Ganzzahlen	302
5.7	Erzeugung großer (Pseudo-) Primzahlen	305
5.8	Was blieb?	310
5.9	Hinweis zur Verschlüsselung mithilfe des Goppa-Codes	310
5.10	Ansätze zur Suche nach Schwachstellen	311
5.11	Verfahren zum Austausch von Schlüsseln (Diffie-Hellmann)	312
5.12	Nachweis der Berechtigung (Benutzer-Authentikation)	314
5.13	Nachweis der Unversehrtheit einer Nachricht (Hash-Algorithmen)	319
5.14	Nachweis der Absenderidentität (digitale Unterschrift, DSA)	325
5.15	Hinweise zu PGP und GnuPG	329
5.16	Weitere Entwicklungen, Quantenkryptographie	331
5.17	Was blieb?	334
6	Datenkompression	335
6.1	Verlustfreie Kompression	335
6.1.1	Laufängen-Codierung (Run Length Encoding)	336
6.1.2	Huffman- und Fano-Codierung	337
6.1.3	Lempel-Ziv-Welch-Codierung (=LZW-Codierung)	340
6.1.4	Arithmetische Codierung	346
6.1.5	Was blieb?	349
6.2	Verlustbehaftete Kompression	350
6.2.1	Wesentliche Einspar-Potenziale	350
6.2.2	Diskrete Fourier-Transformation, Diskrete Cosinus-Transformationen	351
6.2.3	JPEG	372
6.2.4	MPEG	381
6.2.5	MPEG-1 Audio Layer III und MP3	382

XII

Inhaltsverzeichnis

6.2.6

Konkurrenz: Fraktale und Wavelets.

399

6.2.7

Was blieb?

404

Literaturauswahl.

407

Stichwortverzeichnis.

409