

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	20
1.5	Ziel	24
1.6	Was blieb?	25
2	Mathematische Hilfsmittel	27
2.1	Grundlagen aus der allgemeinen Ingenieurmathematik	27
2.2	Weitere mathematische Hilfsmittel	30
2.3	Was blieb?	44
3	Fehlerbeseitigung	45
3.1	Der Prozess der Fehlerentstehung	46
3.2	Die Prüfstellen: Notwendige und hinreichende Bedingungen für die Korrektur mit dem Hard-Decision-Verfahren	47
3.3	Direkte Nutzung des Hammingabstandes	51
3.4	Hamming-Code	53
3.4.1	Aufbau, Codierung und Hard-Decision-Decodierung	53
3.4.2	Generatormatrix G	56
3.4.3	Paritätsprüfmatrix H	57
3.4.4	Syndrom und Fehlerposition bei HD-Decodierung	58
3.4.5	Soft-Decision-Decodierung	60
3.4.6	Technischer Gebrauch des Hamming-Codes	61
3.4.7	Was blieb?	63
3.5	Leistungsbeurteilung von Codes	63
3.5.1	Beschreibung fehlerbehafteter Übertragungssysteme	63

3.5.2	Verteilung der Fehler auf die Codewörter	67
3.5.3	Einfluss der Informationsrate auf die Übertragungsrate	68
3.5.4	Kriterien: Asymptotisches Verhalten bei langen Codes	72
3.5.5	Ein Beispiel	74
3.5.6	Grenzen: Das Theorem von Shannon	77
3.5.7	Was blieb?	88
3.6	Erweiterungen des Hamming-Verfahrens	89
3.6.1	Verallgemeinerung auf andere Ganzzahlbasen	89
3.6.2	Erweiterung um zusätzliche Fehlererkennung	92
3.6.3	Was blieb?	96
3.7	Zyklische Codes	96
3.7.1	Der Weg und die Mittel: Generatorpolynome und Reste	96
3.7.2	Bildung der Codewörter	98
3.7.3	Generatorpolynom, irreduzible Polynome und Decodierung	106
3.7.4	Generatorpolynome für Mehrbitfehler-Korrektur	109
3.7.5	Eignungstest für $g(x)$ zur t -Bitfehler-Korrektur	111
3.7.6	Irreduzible Polynome über Z_2 und Galoisfelder $GF(2^m)$	113
3.7.7	BCH-Code	118
3.7.8	Reed-Solomon-Code für Mehrfach-Bündelfehler-Korrektur	133
3.7.9	Vergleich zwischen BCH- und Reed-Solomon-Codes	144
3.7.10	Erkennung von Einzelfehlern und Fehlerbündeln	145
3.7.11	Was blieb?	149
3.8	Goppa-Code	150
3.8.1	Erzeugung der Codewörter	150
3.8.2	Zwei Lösungswege für die Decodierung	159
3.8.3	Der BCH-Code als Sonderfall des Goppa-Codes	174
3.9	Reed-Muller-Code	184
3.10	Interleaving	194
3.11	Produkt-Codes	196
3.12	Maximum A-Posteriori-Prinzip und Turboprodukt-Codes	202
3.13	Faltungs-Codes (Convolutional Codes)	215
3.14	Was blieb?	224
4	Rückgekoppelte Schieberegister	225
4.1	Eigenschaften	225
4.2	Fehlerbeseitigung durch Kreuzkorrelation	240
4.3	Zufallserzeugung von Schlüsselwörtern	242
4.4	Was blieb?	252
5	Datenverschlüsselung	253
5.1	Datenverschlüsselung zur Informationssicherung	254
5.2	Verschlüsselung nach dem Data-Encryption-Standard (DES)	256

5.3	Verschlüsselung mit dem RSA-Algorithmus	268
5.4	Das Rechnen mit großen Ganzzahlen	277
5.5	Erzeugung großer Pseudoprimzahlen	280
5.6	Was blieb?	285
5.7	Verschlüsselung mit Hilfe des Goppa-Codes	285
5.8	Ansätze zur Suche nach Schwachstellen	289
5.9	Verfahren zum Austausch von Schlüsseln (Diffie-Hellmann)	291
5.10	Nachweis der Berechtigung (Benutzer-Authentikation)	293
5.11	Nachweis der Unversehrtheit einer Nachricht	299
5.12	Nachweis der Absenderidentität (digitale Unterschrift, DSA)	304
5.13	Hinweise zu PGP und GnuPG	307
5.14	Weitere Entwicklungen, Quantenkryptographie	308
5.15	Was blieb?	312
6	Datenkompression	313
6.1	Verlustfreie Kompression	313
6.1.1	Laufängen-Codierung (Run Length Encoding = RLE)	314
6.1.2	Huffman- und Fano-Codierung	315
6.1.3	Lempel-Ziv-Welch-Codierung (= LZW-Codierung)	318
6.1.4	Arithmetische Codierung	323
6.1.5	Was blieb?	326
6.2	Verlustbehaftete Kompression	327
6.2.1	Wesentliche Einspar-Potenziale	327
6.2.2	Fourier-Transformationen	328
6.2.3	JPEG	345
6.2.4	MPEG	350
6.2.5	Konkurrenz: Fraktale und Wavelets	360
6.2.6	Was blieb?	365
	Literaturauswahl	367
	Sachwortverzeichnis	369