

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.....	11
1.3 Begriffe aus der Informations- und Nachrichtentechnik.....	12
1.4 Aufgabenstellung.....	21
1.5 Ziel.....	28
1.6 Was blieb?.....	29
2 Mathematische Hilfsmittel.....	31
2.1 Grundlagen aus der allgemeinen Ingenieurmathematik.....	31
2.2 Weitere mathematische Hilfsmittel.....	34
2.3 Was blieb?.....	48
3 Fehlerbeseitigung.....	49
3.1 Der Prozess der Fehlerentstehung.....	49
3.2 Die Prüfstellen: Notwendige und hinreichende Bedingungen.....	52
3.3 Direkte Nutzung des Hammingabstandes	55
3.4 Hamming-Code.....	56
3.4.1 Aufbau, Codierung und Hard Decision-Decodierung.....	56
3.4.2 Generatormatrix G	60
3.4.3 Paritätsprüfmatrix H	61
3.4.4 Syndrom und Fehlerposition bei HD-Decodierung.....	62
3.4.5 Soft Decision-Decodierung.....	64
3.4.6 Technischer Gebrauch des Hamming-Codes.....	65
3.4.7 Was blieb?.....	66
3.5 Leistungsbeurteilung von Codes.....	67
3.5.1 Beschreibung fehlerbehafteter Übertragungssysteme.....	67
3.5.2 Verteilung der Fehler auf die Codeworte.....	70
3.5.3 Einfluss der Informationsrate auf die Übertragungsrate.....	73
3.5.4 Kriterien: asymptotisches Verhalten bei langen Codes.....	76
3.5.5 Ein Beispiel.....	78

Inhaltsverzeichnis

3.5.6	Grenzen: Das Theorem von Shannon.....	82
3.5.7	Was blieb?.....	93
3.6	Erweiterungen des Hamming-Verfahrens.....	93
3.6.1	Verallgemeinerung auf andere Ganzzahlbasen.....	93
3.6.2	Erweiterung um zusätzliche Fehlererkennung.....	97
3.6.3	Was blieb?.....	101
3.7	Zyklische Codes.....	101
3.7.1	Der Weg und die Mittel: Generatorpolynome und Reste.....	101
3.7.2	Bildung der Codewörter.....	103
3.7.3	Generatorpolynom, irreduzible Polynome und Dekodierung.....	111
3.7.4	Generatorpolynome für Mehrbitfehler-Korrektur.....	115
3.7.5	Eignungstest für $g(x)$ zur t -Bitfehlerkorrektur.....	117
3.7.6	Irreduzible Polynome über Z_2 und Galoisfelder $GF(2^m)$	120
3.7.7	BCH-Code.....	125
3.7.8	Reed-Solomon-Code für Mehrfach-Bündelfehler-Korrektur.....	142
3.7.9	Vergleich zwischen BCH- und Reed-Solomon-Codes.....	153
3.7.10	Erkennung von Fehlerbündeln.....	155
3.7.11	Was blieb?.....	160
3.8	Goppa-Code.....	161
3.8.1	Erzeugung der Codewörter	161
3.8.2	Zwei Lösungswege für die Decodierung.....	170
3.8.3	Der BCH-Code als Sonderfall des Goppa-Codes	182
3.9	Reed-Muller-Code.....	192
3.10	Interleaving.....	203
3.11	Produkt-Codes.....	205
3.12	Maximum a Posteriori-Prinzip und Turboprodukt-Codes.....	212
3.13	Faltungs-Codes (Convolutional Codes).....	225
3.14	Was blieb?.....	234
4	Rückgekoppelte Schieberegister.....	235
4.1	Eigenschaften.....	235
4.2	Fehlerbeseitigung durch Kreuzkorrelation.....	249
4.3	Zufallserzeugung von Schlüsselwörtern.....	251
4.4	Was blieb?.....	261
5	Datenverschlüsselung.....	263
5.1	Datenverschlüsselung zur Informationssicherung.....	264
5.2	Verschlüsselung nach dem Data-Encryption-Standard (DES).....	266
5.3	Verschlüsselung mit dem RSA-Algorithmus.....	278
5.4	Das Rechnen mit großen Ganzzahlen.....	286
5.5	Erzeugung großer Pseudoprimzahlen.....	289
5.6	Was blieb?.....	294
5.7	Verschlüsselung mit Hilfe des Goppa-Codes	295

5.8	Ansätze zur Suche nach Schwachstellen.....	299
5.9	Verfahren zum Austausch von Schlüsseln (Diffie-Hellmann).....	301
5.10	Nachweis der Berechtigung (Benutzer-Authentikation).....	303
5.11	Nachweis der Unversehrtheit einer Nachricht.....	308
5.12	Nachweis der Absenderidentität (digitale Unterschrift, DSA).....	314
5.13	Hinweise zu PGP und GnuPG.....	317
5.14	Weitere Entwicklungen, Quantenkryptographie.....	318
5.15	Was blieb?.....	322
6	Datenkompression.....	323
6.1	Verlustfreie Kompression.....	323
6.1.1	Laufängen-Codierung (Run Length Encoding = RLE).....	323
6.1.2	Huffman- und Fano-Codierung.....	325
6.1.3	Lempel-Ziv-Welch-Codierung (= LZW-Codierung).....	329
6.1.4	Arithmetische Codierung.....	333
6.1.5	Was blieb?.....	336
6.2	Verlustbehaftete Kompression.....	337
6.2.1	Wesentliche Einspar-Potenziale.....	337
6.2.2	Fourier-Transformationen.....	339
6.2.3	JPEG.....	357
6.2.4	MPEG.....	362
6.2.5	Konkurrenz: Fraktale und Wavelets	372
6.2.6	Was blieb?.....	378
7	Literaturauswahl.....	379
8	Sachwortverzeichnis.....	381