

Markus Hufschmid

Information und Kommunikation

Grundlagen und Verfahren der Informationsübertragung

Mit 147 Abbildungen und 24 Tabellen



Inhaltsverzeichnis

1	Einleitung	1
	INFORMATIONSTHEORIE	5
2	Was ist ein „bit“?	7
2.1	Ungewissheit	8
2.2	Information	13
2.3	Zusammenfassung	16
3	Quellencodierung	17
3.1	Einleitung	17
3.2	Codebäume mit Wahrscheinlichkeiten	19
3.3	Kraft'sche Ungleichung	20
3.4	Huffman Code	22
3.5	Aussagen über die mittlere Codewortlänge bei optimalen präfixfreien Codes	26
3.6	Codierung von Symbolketten	28
3.7	Blockcodierung von Nachrichtenquellen	29
4	Kanalkapazität	33
4.1	Informationsrate	33
4.2	Shannons Theorem, Kanalkapazität	33
4.3	Kanalkapazität des Gauss'schen Kanals	35
	KANALCODIERUNG	37
5	Einleitung	39
5.1	Definition einiger Begriffe	39
5.2	Rechnen in Restklassen	40
5.3	Ein einfaches Beispiel	42
6	Blockcodes	43
6.1	Definition	43
6.2	Hamming Codes	43
6.3	Codeeigenschaften	48
6.4	Berechnung der Restfehlerwahrscheinlichkeit	52
6.5	Dichtgepackte Codes	54
7	Lineare Blockcodes	55
7.1	Systematische Form der Generatormatrix	58
7.2	Prüfmatrix	60
7.3	Decodierung	61
7.4	Mathematischer Exkurs	63
8	Zyklische Codes	65
8.1	Polynomdarstellung	65
8.2	Generatorpolynom	66
8.3	Systematische Form	67
8.4	Codierung von zyklischen Codes	69
8.5	Decodierung von zyklischen Codes	73
8.6	Fehlererkennende CRC-Codes	74
9	Reed-Solomon Codes	77
9.1	Einleitung	77
9.2	Rechnen im endlichen Körper $GF(2^m)$	79
9.3	Diskrete Fouriertransformation	81
9.4	Reed-Solomon Codes	84

10 Faltungscodes	87
10.1 Darstellung eines Faltungscodes	88
10.2 Decodierung	90
11 Turbo Codes	95
11.1 Encoder	95
11.2 Decoder	97
11.3 Maximum a posteriori Decoding	98
11.4 Leistungsfähigkeit	101
11.5 Anwendungen	102
STOCHASTISCHE PROZESSE UND RAUSCHEN	105
12 Beschreibung stochastischer Signale	107
12.1 Linearer Mittelwerte	109
12.2 Quadratischer Mittelwerte	109
12.3 Autokorrelationsfunktion	110
12.4 Spektrale Leistungsdichte	111
12.5 Zufallssignale in linearen, zeitinvarianten Systemen	112
12.6 Kreuzkorrelation	115
13 Rauschen in technischen Systemen	117
13.1 Ursachen des Rauschens	117
13.2 Rauschzahl und Rauschtemperatur	119
13.3 Kaskadierung von rauschenden Zweitoren	120
DIGITALE MODULATIONSVERFAHREN	123
14 Grundlagen	125
14.1 Darstellung von Bandpass-Signalen	125
14.2 Rauschen	127
14.3 Berechnung der Bitfehlerwahrscheinlichkeit	132
15 Beispiele von Modulationsarten	137
15.1 Binäre Amplitudenumtastung	137
15.2 Binäre Phasenumtastung	138
15.3 Binäre Frequenzumtastung	140
15.4 Mehrstufige Modulationsverfahren	146
15.5 Orthogonal Frequency Division Multiplexing – OFDM	150
15.6 Trelliscodierte Modulation – TCM	152
16 Vergleich der Modulationsverfahren	155
17 Matched Filter	157
17.1 Aufgabenstellung	157
17.2 Berechnung der Entscheidungsvariablen	157
17.3 Optimierungskriterium	158
17.4 Interpretation des matched Filters im Frequenzbereich	160
18 Matched Filter Empfänger	163
18.1 Herleitung des optimalen binären Empfängers	163
18.2 Berechnung der Bitfehlerwahrscheinlichkeit	166
18.3 Bitfehlerwahrscheinlichkeit bei antipodaler Signalisierung	169
18.4 Bitfehlerwahrscheinlichkeit bei orthogonaler Signalisierung	169
18.5 Verallgemeinerung auf mehrstufige Modulationsverfahren	170
BASISBANDÜBERTRAGUNG	171
19 Digitalsignalübertragung in Tiefpasssystemen	173
19.1 Modell des Übertragungssystems	173
19.2 Intersymbol-Interferenz	175
19.3 Erstes Nyquist-Kriterium	176
19.4 Zweites Nyquist-Kriterium	180

19.5	Drittes Nyquist-Kriterium	182
ANALOGUE MODULATIONSVERFAHREN		183
20	Amplitudenmodulation	185
20.1	Mathematische Beschreibung	185
20.2	Demodulation	190
20.3	Modulatoren	193
20.4	Einseitenbandmodulation	195
20.5	Restseitenbandmodulation	202
21	Winkelmodulation	205
21.1	Einleitung	205
21.2	Frequenzmodulation	205
21.3	Phasenmodulation	212
21.4	Modulatoren	214
21.5	Demodulatoren	217
KRYPTOLOGIE		221
22	Einleitung	223
22.1	Was ist Kryptologie?	223
22.2	Begriffe	224
23	Symmetrische Algorithmen	227
23.1	Cäsar-Methode	227
23.2	Ein (beweisbar) sicheres Verschlüsselungsverfahren	229
23.3	Data Encryption Standard (DES)	230
23.4	International Data Encryption Algorithm (IDEA)	236
23.5	Advanced Encryption Standard	239
23.6	Betriebsmodi von Blockchiffren	240
24	Asymmetrische Algorithmen	243
24.1	Prinzip	243
24.2	RSA-Algorithmus	244
24.3	Elliptische Kurven	250
25	Kryptographische Protokolle	259
25.1	Schlüsselübermittlung	259
25.2	Digitale Unterschriften	261
25.3	Hashfunktionen	262
26	Quantenkryptographie	267
26.1	Einige Quanteneffekte	268
26.2	BB84-Protokoll	270
26.3	Schlüsselaustausch mit verschränkten Quantenpaaren	272
26.4	Praktische Probleme	272
26.5	Quantencomputer	273
27	Elektronische Zahlungsformen	275
27.1	Klassifizierung	275
27.2	Elektronisches Geld	276
ANHÄNGE		281
A	Cauchy-Schwarz-Ungleichung	283
B	Die Euler'sche Phi-Funktion	285