

Wilfried Dankmeier

Codierung

Professional Computing

Die Reihe „Professional Computing“ des Verlags Vieweg richtet sich an professionelle Anwender bzw. Entwickler von IT-Produkten. Sie will praxiserichte Lösungen für konkrete Aufgabenstellungen anbieten, die sich durch Effizienz und Kundenorientierung auszeichnen.

Unter anderem sind erschienen:

Die Feinplanung von DV-Systemen

von Georg Liebetrau

Microcontroller-Praxis

von Norbert Heesel und Werner Reichstein

DB2 Common Server

von Heinz Axel Pürner und Beate Pürner

Softwarequalität durch Meßtools

von Reiner Dumke, Erik Foltin u.a.

QM-Verfahrensweisungen für Softwarehersteller

von Dieter Burgartz und Stefan Schmitz

Die CD-ROM zum Software-Qualitätsmanagement

von Dieter Burgartz und Stefan Schmitz

Businessorientierte Programmierung mit Java

von Claudia Piemont

JSP

von Klaus Kilberth

Erfolgreiche Datenbankanwendungen mit SQL

von Jürgen Marsch und Jörg Fritze

Softwaretechnik mit Ada 95

von Manfred Nagl

Unternehmensorientierte Software-Entwicklung mit Delphi

von Daniel Basler

Standardisation Processes in IT

von Kai Jakobs

Codierung

von Wilfried Dankmeier

Vieweg

Wilfried Dankmeier

Codierung

(Fast) alles über Daten-Verschlüsselung,
Kompression und Fehlerbeseitigung

2., überarbeitete und erweiterte Auflage



Die Deutsche Bibliothek – CIP-Einheitsaufnahme
Ein Titeldatensatz für diese Publikation ist bei
Der Deutschen Bibliothek erhältlich.

Die 1. Auflage erschien unter dem Buchtitel „Codierung“ in der Buchreihe
„DuD-Fachbeiträge“.

1. Auflage 1994

2., überarbeitete und erweiterte Auflage Februar 2001

ISBN 978-3-528-15399-1 ISBN 978-3-663-09494-4 (eBook)

DOI 10.1007/978-3-663-09494-4

Alle Rechte vorbehalten

© Springer Fachmedien Wiesbaden 2001

Ursprünglich erschienen bei Friedr. Vieweg & Sohn Verlagsgesellschaft mbH,
Braunschweig/Wiesbaden 2001.



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

www.vieweg.de

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

Konzeption und Layout des Umschlags: Ulrike Weigel, www.CorporateDesignGroup.de

Gedruckt auf säurefreiem Papier

Inhalt

1	Einleitung	1
2	Aufgabenstellung und Ziel	3
2.1	Beispiele für Codes	3
2.2	Ein Schnupperkurs	7
2.2.1	Verschlüsselung	9
2.2.2	Fehlerbeseitigung	10
2.2.3	Kompression	14
2.3	Einige Begriffe aus der Informations- und Nachrichtentechnik	15
2.4	Aufgabenstellung	20
2.5	Ziel	27
3	Mathematische Hilfsmittel	29
3.1	Grundlagen aus der allgemeinen Ingenieurmathematik	29
3.2	Weitere mathematische Hilfsmittel	32
4	Fehlerbeseitigung	47
4.1	Unmittelbare Ausnutzung des Hammingabstandes	47
4.2	Hammingcode	49
4.2.1	Aufbau	49
4.2.2	Generatormatrix G	54
4.2.3	Paritätsprüfmatrix H	55
4.2.4	Syndrom	57
4.2.5	Technischer Gebrauch des Hammingcodes	59
4.3	Leistungsbeurteilung von Codes	60
4.3.1	Beschreibungsmerkmale für fehlerbehaftete Übertragungssysteme	61
4.3.2	Anforderungen an einen Code und theoretische Ergebnisse	66
4.3.3	Das Theorem von Shannon und die Shannon-Grenze	73
4.3.4	Zusammenfassung	78
4.4	Verallgemeinerung des Codierungsverfahrens von Hamming	79
4.4.1	Mehrfachfehler-Korrektur	79
4.4.2	Andere Ganzzahlbasen	81
4.4.3	Erweiterung um zusätzliche Fehlererkennung	85
4.5	Zyklische Codes	89
4.5.1	Vorüberlegungen	89
4.5.2	Bildung der Codewörter	90
4.5.3	Das Generatorpolynom	98
4.5.4	BCH-Code	110
4.5.5	Reed-Solomon-Code	132
4.5.6	Erkennung von Fehlerbündeln	145
4.5.7	Syndrompolynom, Meggitt-Decodierung, Fehlerfallen-Decodierung	154
4.5.8	Technische Verwirklichung von Verfahren mit zyklischen Codes	160
4.6	Goppacode	163
4.6.1	Erzeugung der Codewörter	164

4.6.2	Zwei Lösungswege für die Decodierung.....	174
4.6.3	Der BCH-Code als Sonderfall des Goppa-Codes und ein schnelles Decodierverfahren	188
4.7	Reed-Muller-Code.....	199
4.8	Interleaving.....	210
4.9	Produkt-Codes, Turbo-Produkt-Codes, Faltungs-Codes.....	213
5	Rückgekoppelte Schieberegister	223
5.1	Eigenschaften	223
5.2	Fehlerbeseitigung bei verdrahteten Nutzsignalen durch Kreuzkorrelation	236
5.3	Zufallserzeugung von Schlüsselwörtern.....	241
6	Datenverschlüsselung	255
6.1	Datenverschlüsselung als Teilgebiet der Informationssicherung.....	256
6.2	Verschlüsselung nach dem Data-Encryption-Standard (DES).....	258
6.3	Verschlüsselung mit dem RSA-Algorithmus	270
6.4	Das Rechnen mit großen Ganzzahlen.....	278
6.5	Erzeugung großer Pseudoprimzahlen.....	282
6.6	Verschlüsselung mit Hilfe des Goppa-Codes (McEliece-Verfahren).....	287
6.7	Ansätze zur Suche nach Schwachstellen	292
6.8	Verfahren zum Austausch von Schlüsseln (Diffie-Hellmann-Schlüsseltausch) ...	294
6.9	Nachweis der Berechtigung (Benutzer-Authentikation).....	296
6.10	Nachweis der Unversehrtheit einer Nachricht (Nachrichtenintegrität, Hash-Summen)	303
6.11	Nachweis der Absenderidentität (Nachrichten-Authentikation, digitale Unterschrift, DSA)	309
6.12	Hinweise auf weitere Entwicklungen	312
7	Datenkompression	313
7.1	Verlustfreie Kompression	313
7.1.1	Laufängen-Codierung (Run Length Encoding = RLE)	313
7.1.2	Huffman- und Fano-Codierung	315
7.1.3	Lempel-Ziv-Welch- Codierung (= LZW-Codierung).....	319
7.1.4	Arithmetische Codierung	324
7.2	Verlustbehaftete Kompression	328
7.2.1	Wesentliche Einspar-Potentiale	328
7.2.2	Fourier-Transformationen	330
7.3	JPEG	346
7.4	MPEG.....	352
7.4.1	MPEG-1 Video.....	352
7.4.2	MPEG-1 Audio Layer III und MP3.....	353
7.5	Konkurrenz für die Fourier-Transformation: Fraktale und Wavelets.....	360
	Literaturverzeichnis.....	365
	Sachwortverzeichnis	368