Korrekturen und Ergänzungen zu:
Codierungstheorie. Eine Einführung
2.Auflage Vieweg Verlag, 2003
Ralph-Hardo Schulz

(Zeilen-Nummern ohne Berücksichtigung der Kopfzeile und von Leerzeilen oder Figuren. Zeile *–n* heißt *n*-te Zeile von unten –einschließlich Fußnotenzeilen.)

Seite 5 Zeile 4: Auch bei der digitalen Fotografie nach dem **JPEG**[1]-Standard werden diskrete Cosinus-Transformation (angewandt auf den sogenannten YC_BC_R -Farbraum von Helligkeitsmaß Y und 2 Farbkomponenten, der aus dem RGB-Farbraum nach Aufteilung in Bildblöcke von $8 \times 8-$ Pixels erzeugt wird) sowie Quantifizierung und eine Variante des Huffman-Codes (vgl. 6.3) verwendet.
Das im Jahre 2000 entwickelte alternative JPEG 2000-Verfahren ersetz u.a. die Cosinus-Transformation durch eine diskrete Wavelet-basierte Transformation[2].
Inzwichen wird über weitere Kompressionen geforscht, z.B. unter Verwendung homogener Wärmeleitungsgleichungen oder mittels anderer partieller Differentialgleichungen[3].

Seite 7 Zeile 14: $A^* := \bigcup_{i \in \mathbb{N}} A^i$.

Seite 34 Zeile 1: binary

Seite 53 Bildunterschrift: aus dem Mutter-Wavelett

Seite 55 Zu 8.1: Die alte ISBN-Nr. (ISBN-10) wird seit dem 1. Januar 2007 nicht mehr vergeben; sie ist durch die **ISBN-13** ersetzt worden, die in das EAN-System integriert ist. Wie die anderen EAN's wird die ISBN durch eine Prüfziffer so ergänzt, dass die Summe der im Wechsel mit den Gewichten 1 und 3 multiplizierten Ziffern mod 10 Null ergeben. Für die EAN, bei der normalerweise die ersten drei Ziffern für ein Land stehen, wurde ein 'Buchland' mit den Ziffern 978 und 979 eingeführt. Hinter diesen Ziffern folgen Gruppen-Nr., Verlags-Nr., Titel-Nr. und Prüfziffer[4].

---

[1] Joint Photographic Experts Group

[2] s. z.B. http://en.wikipedia.org/wiki/JPEG_2000

[3] vgl. J.Weickert: Mathematische Bildverarbeitung mit Ideen aus der Natur. Mitteilungen der DMV 20/20122, p.82-90.

[4] vgl.: http://de.wikipedia.org/wiki/Internationale_Standardbuchnummer#Formel_zur_Berechnung_der_Pr.C3.BCfziffer und http://www.german-isbn.org/PDF/isbn_13_handbuch.pdf

Seite 58 nach Zeile 2: Die 1-dim Strichcodes (Barcodes, Balkencodes)[5] werden zunehmend von den 2-dim **Matrix-Codes** (z.B. **QR-Codes**, d.h. Quick responce codes, s.u. Ergänzung zu den Seite 153 und 156)[6] verdrängt, da bei letzteren nicht nur die Erkennung eines Fehlers, sondern sogar eine Fehlerkorrekturmöglichkeit vorgesehen ist, z.B. bei einem Data-MatrixCode mit höchstem Fehlerkorrekturniveau von bis zu 30% der Fehler in den einzelnen Elementen (mit der Reed-Solomon- Fehlerkorrektur) .

Der Begriff Code steht hier wie beim Barcode für die Abbildung von Daten in binäre Symbolstrukturen zur Verarbeitung durch optische Lesegeräte, z.B. Scanner.

Seite 58 Zeile 9: $n = 13$

Seite 58 vor Zeile -1: Ein weiteres Beispiel liefern die Prüfziffern des **Deutschen Personalausweises**: Dessen Nummer hat die Form

wwwwNNNNNpD< <yyMMddX<YYmmDDx< < < < < <n;

hierbei steht
'wwww' für die Kennzahl des Erstwohnsitzes
'NNNNN' für die laufende Nummer des Ausweises
'p' für die Prüfsumme von wwwwNNNNN
'D' für die Staatszugehörigkeit
'yyMMdd' für Geburts-Jahr, -Monat,-Tag
'X' für die Prüfsumme des Geburtsdatums
'YYmmDD' für Ablauf-Jahr, -Monat,-Tag
'x' für die Prüfsumme des Ablaufdatums und
'n' für die Prüfsumme aller Ziffern.
Die Gewichte für die Berechnung der Prüfsummen sind
7,3,1,7,3,1,7,3,1 7,3,1,7,3,1 7,3,1,7,3,1;
und die Summenbildung erfolgt mod 10.

Seite 60 nach Zeile 2.
Auch bei der Deutschen Post werden noch lineare Bar-Codes verwendet, z.B. zur Darstellung von Briefzusatzleistungen. Dabei wird mod 11 gerechnet und mit den Faktoren 8,6,4,2,3,5,9,7 gewichtet[7].

[5] s.z.B. http://de.wikipedia.org/wiki/Strichcode

[6] Vorschläge zur Behandlung von QR-Codes im Informatikunterricht findet man z.B. in der Beilage zu LOG IN, 34.Jhg. (2014) Heft Nr.178/179: Claudia Strödter: Von der Informatiion zum QR-Code und wieder zurück.

[7] vgl.: http://www.deutschepost.de/downloadServlet?target=/mlm.nf/dpag/images/download/broschueren/dv_freimachung/dv_freimachung_1_3_10.pdf

Seite 60 Einschub: **8.7a Prüfungen bei hexadezimalem Alphabet**

Hexadezimale Zahlen werden verwandt z.B. bei den "International Standard Audiovisial Numbers (ISAN)" (benutzt zur Identifikation von audivisionellen Arbeiten) und dem "International Mobile Equipment Identifier (MEID)" (benutzt zur Kennung mobiler Stationen).

Bei **ISAN** werden die Zeichen von rechts nach links nummeriert:

$$a_{16}a_{15}...a_2a_1 \in \{0,1,\ldots,9,A,B,C.D,E,F\}^{16}$$

Die Prüfziffer a_1 wird dann nach ISO 7064, MOD 17,16 berechnet: Dazu setzt man $j = 1, P_1 = 16$ und bildet rekursiv $S_j = P_j(\mod 17) + a_{17-j}$ und $P_{j+1} = 2 \cdot S_j(\mod 16)$. (Dabei wird mit A als 10, B als 11 usw. gerechnet.) a_1 erhält man dann mit $S_{16} = P_{16}(\mod 17) + a_1$ aus der Gleichung $S_{16}(\mod 16) = 1$.

(Vgl.: http://www.pruefziffernberechnung.de/Originaldokumente/wg1n130.pdf)

Das Prüfzeichen von **MEID** ist nicht Teil der 14-stelligen hexadezimalen MEID, sondern wird nur bei gedruckten MEID hinzugesetzt. Die Berechnung ist eine Abwandlung der "Luhn Formel" (ISO/IEC 7812-1) von Basis 10 zu Basis 16.

S. https://www.tiaonline.org/sites/default/files/pages/X.S0008-0_v2.0_051018.pdf

Das Prüfzeichen-System von **Markku Niemenmaa** für hexadezimale Ziffern lässt alle Einzelfehler, Nachbar- und Sprung-Transpositionen sowie Zwillings- und Sprung-Zwillingsfehler erkennen. Dabei werden die hexadezimalen Ziffern als Elemente der elementar-abelschen Gruppe

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

aufgefasst. Das Prüfzeichen a_{n+1} für $a_1a_2\ldots a_na_{n+1}$ wird dann so bestimmt, dass mit

$$P((a,b,c,d)) = (a+b,c,d,a)$$

die Prüfgleichung $P(a_1) + P^2(a_2) + \ldots P^n(a_n) + P^{n+1}(a_{n+1}) = 0$ erfüllt ist. P und P^2 sind anti-symmetrische und fixpunktfreie Automorphismen von G. Daher die Fehlererkennungs-Möglichkeiten.

S. http://link.springer.com/content/pdf/10.1007%2Fs00200-011-0139-3.pdf

Seite 62 Voraussetzung zu **8.13**: Sei zusätzlich G endlich. (Es gibt im Fall der unendlichen Gruppe $(\mathbb{Z},+)$ ein Gegenbeispiel– cf.Jerry Chang. Ich danke Herrn Daniel Bardutzky für diesen Hinweis.)

Seite 75 Ab dem Jahr 2014 verändert "SEPA" (Single Euro Payments Area, d.h. einheitlicher Euro-Zahlungsverkehrsraum) den bargeldlosen Zahlungsverkehr: An die Stelle der bisherigen Konto-Nummer und Bankleitzahl tritt künftig die **"IBAN"** (International Bank Account Number), die aus der bisheri-

gen 10-stelligen Konto-Nummer, der 8-stelligen Bankleitzahl zusammen mit vorangestellten Länderkennung und 2-stelligem Prüfzeichen besteht, z.B.

$$\text{DE23}\underbrace{10000000}_{\text{BLZ}}\underbrace{1234567890}_{\text{Kontonummer}}$$

(mit Ländercode DE für Deutschland und Prüfziffern 23). Das zweistellige Prüfzeichen wird dabei gemäss Verfahren "ISO 7064 (Modulo 97,10)" berechnet, und zwar wie folgt[8]:

(a) Anstelle der zu berechnenden Prüfziffern wird als Platzhalter 00 gesetzt.
Beispiel: $Z_1 = \text{DE}\mathbf{00}100000001234567890$.

(b) Die ersten 4 Stellen werden ans Ende verschoben.
Beispiel: $Z_2 = 100000001234567890\mathbf{DE00}$.

(c) Die Alphazeichen der Länderkennung werden gemäß folgender Konversionstabelle ersetzt:

A	B	C	D	E	F	G	.....	V	W	X	Y	Z
10	11	12	13	14	15	16	.....	31	32	33	34	35

Beispiel: $Z_3 = 100000001234567890\mathbf{1314}00$

(d) Die so entstandene Zahl Z_3 wird durch 97 dividiert und der Rest von 98 subtrahiert. Diese Differenz ergibt das Prüfzeichen P. Also:

$$P = 98 - Z_3 \bmod 97.$$

Beispiel[9]:
$\bmod(100000001234567890131400, 97) = 75$ und $P = 98 - 75 = 23$.

(e) Diese Prüfziffern wird an die Stelle des Prüfziffern-Platzhalters in die ursprüngliche alphanumerische Ziffernfolge eingesetzt, die so zur IBAN wird.
Beispiel: $Z_1 \mapsto Z = \text{DE}\mathbf{23}100000001234567890$.

Und wie wird umgekehrt die IBAN geprüft?

1. Die Länderkennung und die beiden Prüfziffern werden an das Ende der IBAN verschoben. Beispiel:
$Z = \mathbf{DE23}100000001234567890 \mapsto 100000001234567890\mathbf{DE23}$.

[8] Quellen: Sparkasse Rhein-Nahe und
http://www.pruefziffernberechnung.de/Originaldokumente/IBAN/Prufziffer_07.00.pdf
sowie http://code.google.com/p/checkdigits/wiki/CheckDigitSystems

[9] Berechnung z.B. mit SAGE

2. Die Alphazeichen der Länderkennung werden gemäß Konversionstabelle ersetzt. Beispiel:
   $10000000123456789\mathbf{DE}23 \mapsto 10000000123456789\mathbf{1314}23$.
3. Die so erhaltene Zahl muss bei Division durch 97 Rest 1 haben.

   Beispiel: $\mod(100000001234567890 1314, 97) = 1$.

   Begründung: Nach Umstellen und Konversion wird die IBAN laut Berechnungsteil (d) zu $Z_3 + P$; daraus ergibt sich

$$Z_3 + P = Z_3 + (98 - Z_3 \bmod 97) \equiv 98 \equiv 1 \pmod{97}.$$

Seite 90 Zeile 12: Für $t > 2$ und beliebige Alphabetgröße q sind ebenfalls alle $t-$perfekten Codes bekannt (s.z.B. M. Best [1983], Y. Hong [1984] und H. Laakso[1979]).

Seite 96 Zeile –6: $(U^{\perp})^{\perp}$

Seite 100 Zeile 8: Mat**r**ix

Seite 108 Zeile 4: Die verbliebene Implikation '(iv) impliziert (i)' folgt sofort aus '(i) impliziert (iv)' und 10.16 (d).

Seite 110 Zeile –14: G_2

Seite 111 Zeile –2: Si**n**gleton

Seite 112 Zeile –15: A 11.8 (ii)

Seite 120 Zeile –1: Sie

Seite 123 Zeile 16/17: im Widerspruch zum Grad von Q.

Seite 124 Zeile –18: $K =$GF $(2), n = 4, P(X) \ldots$

Seite 153 Zeile 14: Reed-Solomon-Fehlerkorrekturen werden nach Wikipedia auch bei 2-dim Matrix-Codes (s.o., Ergänzung zu Seite 58) eingesetzt, z.B. bei dem DataMatrixCode für die elektronische Briefmarke (STAMPIT) der Deutschen Post (bis 2011) bzw. dessen Nachfolger [10], Datamatrix-Codes der Größe 22×22 bzw. 26×26 (s. Bild) und beim (von Andrew Longacre Jr. und

[10] s. z.B. http://de.wikipedia.org/wiki/Stampit bzw. http://de.wikipedia.org/wiki/DataMatrix-Code

DataMatrixcode
der Deutschen Post
(Beispiel)

Rob Hussey entwickelten) Aztec-Code[11] , der u.a. von der Deutschen Bahn auf Online-Tickets verwendet wird.

Aztec-Code der Deutschen Bahn (Beispiel)

Seite 156 Zeile 8: Man beachte, dass die Bezeichnung QR-Code neuerdings auch für den sogenannten Quick-Response-Code steht, einen 2-dim Strichcode (oder besser Matrix-Code, da die Daten in einer Matrix aus schwarzen und weißen Punkten binär dargestellt sind)[12].
Viele Smartphones verfügen über eine Software, die das Interpretieren von mittels QR-Codes codierten Web-Adressen und Telefon-Nummern ermöglichen.

Seite 203 Als Erstem gelang es wohl Charles Babbbage 1854, den passenden Schlüssel aus einem nach Vigenère verschlüsselten Text zu filtern. Da er sein Verfahren aber nicht veröffentlichte, wurde das erst nach seinem Tod bekannt.(Vgl. Wikipedia: Charles Babbagge.)

Seite 206 Wie inzwischen bekannt wurde (s.z.B. Wikipedia: Asymmetrisches Kryptosystem), hatten Anfang der 1970er Jahre James Ellis, Clifford Cocks und Malcolm Williamson, Mitarbeiter des englischen Government Communications Headquarters, ein dem späteren (abstrakten) Konzept von Diffie und Hellman ähnliches asymmetrisches Verfahren entwickelt, dieses aber aus Geheimhaltungsgründen nicht veröffentlichen können. (Es ging diesen Wissenschaftlern also ähnlich wie Alan Mathison Turing, der im 2.Weltkrieg die Rechenmaschinen zur Enigma-Entschlüsselung mit entwickelte, ein Geheimnis bis in die 1970er Jahre.)

[11] s.z.B. http://de.wikipedia.org/wiki/Aztec-Code oder http://en.wikipedia.org/wiki/Aztec-Code bzw. das US-Patent http://www.freepatentsonline.com/5591956.pdf

[12] siehe z.B. http://de.wikipedia.org/wiki/QR-Code

Seite 206 Man beachte folgenden Satz (vgl. z.B. Goldreich 2001,2006) (für die Begriffe siehe dort!):
Wenn (1-1 oder oder reguläre) Einwegfunktionen existieren, dann existiert auch ein Pseudozufallszahlengenerator. Existiert umgekehrt ein Pseudozufallsgenerator mit Expansionsfaktor $l(n) = 2n$, so existiert auch eine (starke) Einwegfunktion.
Und die Existenz einer Einwegfunktion impliziert $\mathcal{P} \neq \mathcal{NP}$.

Seite 207 Zum RSA-Verfahren,insbesondere zur Länge und Anzahl der Schlüssel, zu Primzahltests und Faktorisierungsalgorithmen, sowie zur Alternative mit elliptischen Kurven s. auch die (für Informatiklehrer geschriebenen) Artikel Witten/Schulz[2006,2008,2010, 2011/12], Witten/Schulz/Esslinger[2015], Schulz/Witten[2010], Schulz/Witten/Esslinger[2015]!

Seite 209 Literaturhinweise: Goldreich [2001/2006], Karpfinger/Kiechle [2010], Katz/Lindell [2007], Schulz/Witten[2010], Schulz/Witten/Esslinger[2015], Witten/Schulz[2006,2008,2010, 2011/12], Witten/Schulz/Esslinger [2015].

Seite 213 Literaturhinweise: Quisquater, Guillou & Berson[1990]

Seite 230 Best, M.R., 1983. A contribution to the nonexistence of perfect codes . Amsterdam: Math. Centrum. Zbl 0526.94014)

Seite 231 Buchmann,J. ...2010[5]..

Seite 232 Goldreich, Oded, 2001,2006: Foundations of Cryptography. Basic Tools. Cambridge University Press.
Goldreich, Oded, 2005: Foundations of Cryptography: A Primer (Foundations and Trends in Theoretical Computer Science). Now Publishers Inc.

Seite 234 Hong, Yiming 1984: On the existence of unknown perfect 6- and 8-codes in Hamming schemes H(n,q) with q arbitrary. Osaka J. Math. 21, 687-700 (Zbl 0551.94011)

Seite 234 Katz, Jonathan & Yehuda Lindell, 2007: Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall/Crc Cryptography and Network Security Series.

Seite 234 Laakso, Hannu, 1979: Nonexistence of nontrivial perfect codes in the case $q = p_1^a p_2^b p_3^c$, $e \geq 3$. Ann. Univ. Turku., Ser A I 177 (Zbl 0407.94011)

Seite 234 Van Lint, J.H. 1982, 1999[3]: Introduction to coding theory. Sringer Verlag Berlin etc..

Seite 235 Karpfinger, C.; Kiechle, H., 2010: Kryptologie – Algebraische Methoden und Algorithmen. Wiesbaden: Vieweg + Teubner.

Seite 236 Zeile –18: 1990

Seite 237 Schulz, R.-H. & H.Witten, 2010: Zeitexperimente zur Faktorisierung . Ein Beitrag zur Didaktik der Kryptographie. LogIn Heft Nr. 166/167 (2010) 113-120.
Schulz, R.-H. & H.Witten, 2011: Faktorisieren mit dem Quadratischen Sieb Ein Beitrag zur Didaktik der Algebra und Kryptologie. LogIn Heft Nr.172/ 173 (2011/2012) 70-78.
Schulz, R.-H., H. Witten & B. Esslinger: Rechnen mit Punkten einer Elliptischen Kurve. LogIn, Heft 181/182 (2015) 103-115 .

Seite 239 Witten, H. & R.-H.Schulz: RSA und Co in der Schule. Moderne Kryptologie, alte Mathematik, raffinierte Protokolle. Neue Folge – Teil 1: RSA für Einsteiger. LogIn 26. Jg. (2006) Heft 140, p. 45-54.– Teil 2: RSA für große Zahlen. LogIn Jg. (2006) Heft 143, p. 50-58.– Teil 3: RSA und die elementare Zahlentheorie. LogIn (2008) Heft 152, p. 60-70. – Teil 4: Gibt es genügend Primzahlen für RSA. LogIn (2010) Heft Nr. 163/164, p. 97-103. – Teil 5: Der Miller-Rabin-Primzahltest oder Falltüren für RSA mit Primzahlen aus Monte Carlo. LogIn Heft Nr.166/167 (2010) 98-112. – Teil 6: Das Faktorisierungsproblem oder: Wie sicher ist RSA? LogIn (2011/2012) Heft Nr.172/173, p. 59-69.

Seite 239 Witten,H, R.-H.Schulz und B. Esslinger: RSA und Co in der Schule. Moderne Kryptologie, alte Mathematik, raffinierte Protokolle. Neue Folge Teil 7: Alternativen zu RSA oder Diskreter Logarithmus statt Faktorisierung. LogIn, Heft 181/182 (2015) 85-102.

Anmerkungen: Die Internet-Adressen wurden zuletzt nach dem 22.7.2012 geprüft. Alle Quellen sind sorgfältig dargestellt; es kann jedoch keine Gewähr für die Vollständigkeit und Richtigkeit der Informationen übernommen werden.
Für einige Hinweise danke ich Herrn Dipl.Math.Tobias Schwarz. Weitere Hinweise sind willkommen.

E-mail-Adresse des Autors:
rhschulz@zedat.fu-berlin.de

17. Mai 2019