Pädagogische Hochschule Karlsruhe

Institut für Mathematik und Informatik

Vorlesung: Codierung und Kryptographie
WS 2002/2003
Prof. Dr. J. Ziegenbalg

Hausarbeit

Die Diedergruppe D_5 und deren Anwendung bei der Numerierung bundesdeutscher DM-Geldscheine

von
Christian Stellfeldt
Meerlachstr. 4
68163 Mannheim
stellfeldt@onlinehome.de

Inhalt

1. Vorbemerkung

Prüfziffern sind uns allen bekannt und allgegenwärtig. Banken setzen sie ein, um falsch erfaßte Kontonummern zu entdecken, der Buchhandel erkennt mit ihrer Hilfe falsche ISBN-Nummern, und schließlich kennt jeder von uns auch den Strichcode, oder besser: die Europäische Artikelnummer (EAN) für die Kasse im Supermarkt.
Die Seriennummern der (ehemaligen) bundesdeutschen DM-Geldscheine, die die Bundesbank ab Herbst 1990 herausgegeben hat, stellen ebenfalls Prüfziffern dar, deren System in dieser Hausarbeit näher vorgestellt werden soll.

Das Prinzip des Prüfzifferverfahrens ist denkbar einfach: Um eine Zahl gegen Eingabe- oder Übertragungsfehler zu sichern, berechnet man aus ihr eine zusätzliche Ziffer und baut sie in die Zahl mit ein. Wenn die Prüfziffer später nicht mit der errechneten Ziffer übereinstimmt, so hat sich irgendwo ein Fehler eingeschlichen.

Die einfachste Möglichkeit eine Prüfziffer zu erhalten, wäre z.B. die Quersummenbildung. oder die Bildung des Querprodukts. Der Nachteil wäre hier, daß die Prüfziffer hier wahrscheinlich sehr schnell mehrstellig werden wird. Abhilfe könnte hier eine Division durch 10 verschaffen und den Rest (Modus) als Prüfziffer zu verwenden. Es leuchtet jedem sofort ein, daß Zahlenverdreher, insbesondere Nachbarvertauschungen gar nicht und Einzelfehler eventuell nicht sicher erkannt werden. Solche einfache Prüfzifferverfahren scheiden also schnell aus bzw. sind untauglich.

Es empfiehlt sich also vor Überlegung eines geeigneten Prüfziffersystems einen Blick auf die häufigsten Fehler zu werfen, die ein solches System erkennen muß.

2. Fehlertypen

Zur Beurteilung von Prüfziffern-Verfahren ist eine Untersuchung möglicher Fehler und der Häufigkeit des Auftretens nötig. VERHOEFF ist im Rahmen seiner Dissertation auf die folgenden Ergebnisse gekommen:

- Zu 79% wird eine Ziffer verwechselt. Man spricht dann von einem Einzelfehler oder einem einfachen Fehler.
- Bei 10,2% aller Fehler handelt sich um (Nachbar-)Transpositionen (Ziffer-Dreher, Vertauschung benachbarter Ziffern).
- Bei 2,2% aller Fehler handelt sich um Sprungtranspositionen (acb-bca), Zwillingsfehler (aa-bb), phonetische Fehler (z.B. fünfzehn und fünfzig), Sprung-Zwilling-Fehler (aca-bca)
- Und schließlich tauchen zu 8,6% zufällige Fehler auf.

Es leuchtet an dieser Stelle ein, daß ein gutes Prüfzifferverfahren möglichst vieler solcher Fehlertypen erkennen sollte.
(SCHULZ, 1991, S. 58)

3. Die Diedergruppe D_5

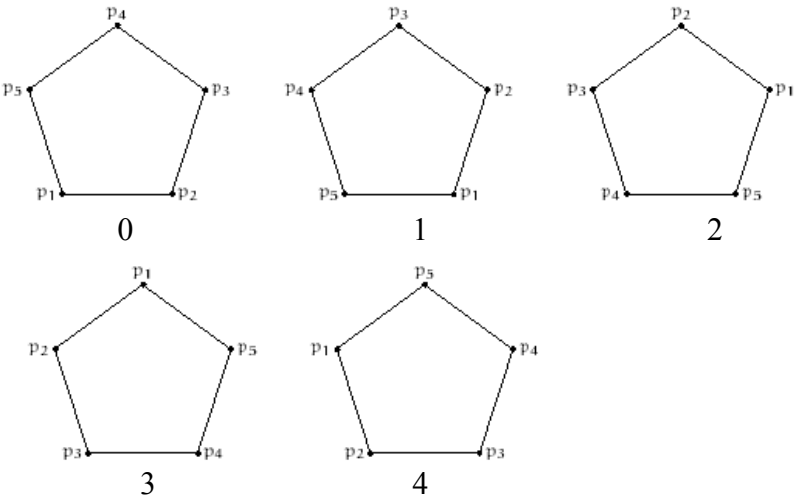
Bei manchen Prüfzifferverfahren (insbesondere beim ISBN-Verfahren) handelt es sich um Modulo-11-Verfahren. Dabei kann unglücklicherweise auch ein zweistelliger Rest von 10 auftauchen. Entweder muß man daher auf Zahlen verzichten, deren Prüfziffer 10 wäre, oder ein nicht-numerisches Ersatzzeichen einsetzen. Bei ISBN-Nummern dient zum Beispiel ein X als "elfte Ziffer".

Wenn man auf solche "Ersatzziffern" verzichten möchte, muß man auf ein anderes Verfahren ausweichen. Gesucht ist also ein Verfahren, daß erstens möglichst alle Fehler erkennt und zweitens nur Prüfziffern ermittelt, die zwischen 0 und 9 liegen.

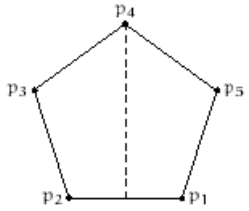
Es liegt deshalb nahe, daß die Berechnung der Prüfziffer innerhalb einer zehnelementigen Menge verläuft, insbesondere diese Menge die mathematische Struktur einer Gruppe besitzt. Es werden an dieser Stelle die wesentlichen Kennzeichen einer Gruppe vorausgesetzt.

Es gibt zwei verschiedene Gruppen mit zehn Elementen, deren mathematische Strukturen unterschiedlich sind. Die eine Gruppe ist die gewöhnliche Addition von Zahlen modulo 10. Sie ist kommutativ.
Die andere Gruppe ist die Diedergruppe D_5. Die Elemente von D_5 können geometrisch gedeutet werden. Es sind dies die 5 Drehungen (um 72, 144, 216, 288 und 360 Grad) und 5 Achsenspiegelungen, die ein regelmäßiges Fünfeck auf sich selbst abbilden. Neutrales Element ist die Drehung um 360 Grad. Die Hintereinanderausführung je zweier Abbildungen stellt die Verknüpfung der Gruppe dar. Die Verknüpfung wird in dieser Hausarbeit mit einem * gekennzeichnet, gelegentlich wird auch die Bezeichnung "Diedermultiplikation" verwendet. Die Verknüpfungen sind i.a. nicht kommutativ. Es ist eben ein Unterschied ob man erst dreht und dann spiegelt oder umgekehrt. Und genau das ist für ein Prüfzifferverfahren von Vorteil, denn dann ändert sich bei Transpositionen (Zifferdreher) die Prüfziffer automatisch. Die Elemente von D_5 können mit den Ziffern 0 bis 9 codiert werden:

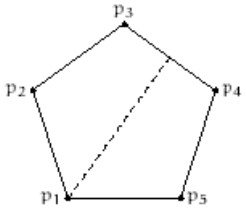
5 Drehungen



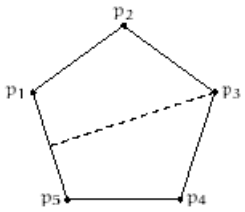
5 Spiegelungen



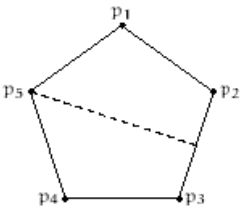
5



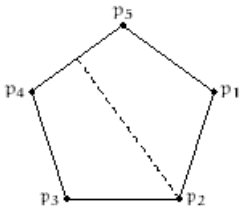
6



7



8



9

Damit ergibt sich die folgende Verknüpfungstafel:

		dann									
	*****	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
	0	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
	1	**1**	**2**	**3**	**4**	**0**	**6**	**7**	**8**	**9**	**5**
	2	**2**	**3**	**4**	**0**	**1**	**7**	**8**	**9**	**5**	**6**
	3	**3**	**4**	**0**	**1**	**2**	**8**	**9**	**5**	**6**	**7**
	4	**4**	**0**	**1**	**2**	**3**	**9**	**5**	**6**	**7**	**8**
zuerst	**5**	**5**	**9**	**8**	**7**	**6**	**0**	**4**	**3**	**2**	**1**
	6	**6**	**5**	**9**	**8**	**7**	**1**	**0**	**4**	**3**	**2**
	7	**7**	**6**	**5**	**9**	**8**	**2**	**1**	**0**	**4**	**3**
	8	**8**	**7**	**6**	**5**	**9**	**3**	**2**	**1**	**0**	**4**
	9	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**

(Tab.1)

(MICHAEL, 1997 / SCHULZ, 1991, S. 64 f.)

4. Die Diedergruppe D_5 in der Numerierung bundesdeutscher DM-Geldscheine

Nun könnte man der Auffassung sein, daß es ausreichen würde, allein mit Hilfe der Diedermultiplikation eine Prüfziffer zu berechnen. Man nimmt einfach ein paar Ziffern und verknüpft sie gemäß der Diedermultiplikation. Dieser Ansatz ist sicherlich besser, als die gewöhnliche Multiplikation und er erkennt auch tatsächlich alle Einzelfehler und immerhin bereits zwei Drittel der Nachbarvertauschungen. Ein Drittel der Nachbarvertauschungen können also nicht erkannt werden. So ist zwar zum Beispiel 2 * 6 = 8 und 6 * 2 = 9, jedoch ist 3 * 4 = 2 und 4 * 3 = 2. Die Diedermultiplikation ist eben nur *i.a.* nicht kommutativ.

Eine Lösung des Problems besteht in der Erweiterung des Verfahrens. Vor der Diedermultiplikation werden alle Ziffer noch transformiert. Dies führt auf den folgenden Term:

$$t_1(x_1) * t_2(x_2) * \ldots * t_n(x_n)$$

Die Funktionen t_i sind jeweils beliebige Permutationen der Ziffern von 0 bis 9.

Es ist klar, daß die Permutationen sich unterscheiden müssen. Das Kunststück besteht darin, die Permutationen so zu wählen, daß das Verfahren möglichst viele Nachbarvertauschungen erkennt. Um *alle* Nachbarvertauschungen erkennen zu können, muß die folgende Bedingung an allen Positionen i (i = 1 ... n-1) und für alle Ziffern $x_i \neq x_{i+1}$ erfüllt sein:

$$t_i(x_i) * t_{i+1}(x_{i+1}) \neq t_i(x_{i+1}) * t_{i+1}(x_i)$$

Das Problem ist nur, daß es insgesamt über 3,6 Mio. Permutationen (≈ 10!) der Menge $\{0, 1, \ldots 9\}$ gibt. Bei einer n-stelligen Seriennummer wächst die Zahl der Möglichkeiten dann auf $(10!)^n$. Eine Möglichkeit, den Suchbereich einzuschränken, besteht darin, die Permutationen t_i also Potenzen T^i einer Basispermutation T anzusetzen: $t_1 = T$, $t_2 = T^2$ und so weiter. Dann bleiben "nur" noch ungefähr eben 3,6 Mio. Basispermutationen. Von diesen ermöglichen 34040 eine vollständige Erkennung aller Einzelfehler und Nachbarvertauschungen.

VERHOEFF hat eine Basispermutation gefunden, die alle Einzelfehler, Nachbarvertauschungen und 95,3% der phonetischen Fehler entdeckt. Und genau diese wurde bei den Seriennummern der ehemaligen DM-Geldscheinen verwendet.

$$T = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 6 & 7 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix} \qquad T^2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 0 & 3 & 7 & 9 & 6 & 1 & 4 & 2 \end{pmatrix}$$

$$T^3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 1 & 6 & 0 & 4 & 3 & 5 & 2 & 7 \end{pmatrix} \qquad T^4 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 5 & 3 & 1 & 2 & 6 & 8 & 7 & 0 \end{pmatrix}$$

$$T^5 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 8 & 6 & 5 & 7 & 3 & 9 & 0 & 1 \end{pmatrix} \qquad T^6 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 9 & 3 & 8 & 0 & 6 & 4 & 1 & 5 \end{pmatrix}$$

$$T^7 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 0 & 4 & 6 & 9 & 1 & 3 & 2 & 5 & 8 \end{pmatrix} \qquad T^8 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

$$T^9 = T \qquad T^{10} = T^2$$

$$T^{11} = T^8$$

Die elfte Ziffer (x_{11}) ist die Prüfziffer. Sie ist so gewählt, so daß die Seriennummern die Prüfgleichung

$$T(x_1) * T^2(x_2) * \ldots * T^{10}(x_{10}) * T^{11}(x_{11}) = 0$$

erfüllen.

Daß es stets eine Prüfziffer (x_{11}) gibt, die diese Prüfgleichung erfüllt, folgt unmittelbar aus der Eigenschaft, daß die Diedergruppe eine Gruppe ist (Existenz von inversen Elementen) und daß zu jeder Permutation, insbesondere zur "identischen" Permutation die Umkehrabbildung existiert.

Die Seriennummern der bundesdeutschen DM-Geldscheine enthalten an den Positionen 1, 2 und 10 Buchstaben statt Ziffern. Wäre die vorletzte Stelle (10. Stelle) kein Buchstabe, sondern eine Ziffer, dann würde das Verfahren eine Vertauschung der letzten mit der vorletzten Ziffer nicht sicher erkennen, sondern nur mit 95,5prozentiger Wahrscheinlichkeit.
Die Buchstaben müssen also vorher noch nach der folgenden Tabelle (Tab.2) ersetzt werden:

A	D	G	K	L	N	S	U	Y	Z
0	1	2	3	4	5	6	7	8	9

(Tab.2)

Nun sind aber ein paar Beispiele längst fällig:

Die Prüfung erfolgt in drei Schritten:
1. Ersetzung der Buchstaben nach Tab.2
2. Die Ziffern werden transformiert
3. Die transformierten Ziffern werden gemäß der Diedermultiplikation verknüpft (Tab.1)
4. Wenn das Ergebnis 0 beträgt, so existiert die Seriennummer, andernfalls nicht.

Seriennummer	G	S	8	2	1	6	8	0	3	L	6
codierte Zahl x_i (nach Tab.2)	2	6	8	2	1	6	8	0	3	4	6
Permutation $T^i(x_i)$	7	6	2	5	2	6	5	0	6	7	6
Diedermultiplikation (nach Tab.1)		1	3	8	6	0	5	5	4	6	**0**
verwendete Permutation	T	T^2	T^3	T^4	T^5	T^6	T^7	T^8	T^9	T^{10}	T^{11}

Seriennummer	A	D	5	3	3	9	6	6	0	L	5
codierte Zahl x_i (nach Tab.2)	0	1	5	3	3	9	6	6	0	4	5
Permutation $T^i(x_i)$	1	8	4	3	6	5	3	6	1	7	5
Diedermultiplikation (nach Tab.1)		9	5	7	1	6	8	2	3	5	**0**
verwendete Permutation	T	T^2	T^3	T^4	T^5	T^6	T^7	T^8	T^9	T^{10}	T^{11}

Seriennummer	A	A	6	6	3	5	0	4	4	U	0
codierte Zahl x_i (nach Tab.2)	0	0	6	6	3	5	0	4	4	7	0
Permutation $T^i(x_i)$	1	5	3	6	6	0	7	4	2	1	0
Diedermultiplikation (nach Tab.1)		6	8	2	8	8	1	0	2	3	**3**
verwendete Permutation	T	T^2	T^3	T^4	T^5	T^6	T^7	T^8	T^9	T^{10}	T^{11}

Diese Seriennummer existiert nicht!

Seriennummer	A	A	6	1	8	6	3	0	5	Z	2
codierte Zahl x_i (nach Tab.2)	0	0	6	1	8	6	3	0	5	9	2
Permutation $T^i(x_i)$	1	5	3	4	0	6	6	0	8	2	2
Diedermultiplikation (nach Tab.1)		6	8	9	9	3	9	9	1	3	**0**
verwendete Permutation	T	T^2	T^3	T^4	T^5	T^6	T^7	T^8	T^9	T^{10}	T^{11}

(MICHAEL, 1997 / SCHULZ, 1991, S. 65 ff.)

Die grundlegende Ideen dieses Prüfzifferverfahrens stammen aus einer Dissertation des niederländischen Mathematikers JACOBUS VERHOEFF. Er wurde 1927 geboren und studierte Mathematik in Leiden und Amsterdam. Danach arbeitete er u.a. für Philips in Eindhoven. Später wechselte er als Professor für Informatik an die Universität Rotterdam.

5. Literatur

MICHAEL, J.: Blütenrein. Prüfziffernverfahren auf der Basis von Diedergruppen, c't 04/97

DERS.: Mit Sicherheit. Prüfziffernverfahren auf Modulo-Basis, c't 07/96

SCHULZ, R.-H.: Codierungstheorie. Eine Einführung. Vieweg. Braunschweig, Wiesbaden, 1991

VERHOEFF, J.: Error detecting Decimal Codes, volume 29 of Math. Centre Tracts. Math. Centrum Amsterdam, 1969

Internet
http://theory.gsi.de/~vanhees/faq-pdf/dieder.pdf

http://heise.de/kiosk/archiv/ct/97/04/448/art.htm

http:/www.heise.de/kiosk/archiv/ct/96/07/264/

http://www.ams.org/new-in-math/cover/verhoeff.html