Anton Betten
Harald Fripertinger
Adalbert Kerber
Alfred Wassermann
Karl-Heinz Zimmermann

Codierungstheorie

Konstruktion und Anwendung linearer Codes

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Vorwort

Die *Algebraische Codierungstheorie* ist eine noch junge Teildisziplin der Diskreten Mathematik. Ihre Ergebnisse finden im Zuge des sich rasch vollziehenden technologischen Wandels immer häufiger dort Anwendung, wo *sichere Datenübermittlung* notwendig ist. Mittlerweile benutzt oder kennt jeder CDs und weiß von der Übertragung der Satellitenaufnahmen vom Mond oder den Planeten des Sonnensystems zur Erde. Hierbei werden zur Sicherung der Kommunikation und zur Korrektur von Übermittlungsfehlern mit großem Erfolg *lineare Codes* verwendet, das sind endliche Vektorräume mit Hammingmetrik. Den Reiz ihrer Theorie macht — neben ihrer technischen Verwendbarkeit — auch die Vielseitigkeit der hier anwendbaren mathematischen Methoden aus: sie kommen aus der Linearen Algebra, der Algebra, der Darstellungstheorie und der Kombinatorik.

Wir geben in dem vorliegenden Buch eine *Einführung* in diese Theorie. Darüberhinaus werden spezielle Serien linearer Codes genauer diskutiert, nämlich die zyklischen und einige daraus abgeleitete Codes. Besonderes Gewicht haben wir dabei auf die Frage nach der Konstruktion aller zyklischen Codes zu gegebener Länge gelegt. Auch die Betonung des darstellungstheoretischen Aspekts der Theorie der zyklischen und der Reed-Muller Codes unterscheidet den vorliegenden Text von den allermeisten anderen Publikationen auf diesem Gebiet.

Danach *klassifizieren* wir die linearen Codes nach ihren metrischen Eigenschaften, denn diese entscheiden über die Qualität bei der Fehlerkorrektur. Methoden für die *Abzählung* dieser *Isometrieklassen* werden hergeleitet, und Algorithmen für die *Konstruktion von Repräsentanten* dieser Klassen werden beschrieben. Insbesondere kann man damit die *besten* linearen Codes systematisch und (für kleine Paramter) vollständig ermitteln. Dies wird abgerundet durch die Angabe von Verfahren, Repräsentanten der Isometrieklassen von linearen Codes und von Blockcodes *gleichverteilt* und *zufällig* zu erzeugen und aus einem gegebenen Repräsentantensystem der Isometrieklassen von linearen Codes kleiner Blocklängen durch experimentelle Suchverfahren Codes größerer Blocklängen zu generieren.

Auch in der eingehenden Schilderung von Verfahren zur Klassifizierung, Abzählung, Konstruktion und Zufallserzeugung von Codes differiert das vorliegende Buch von den bisher publizierten Werken zur Codierungstheorie, wir haben besonderen Wert auf diese Aspekte gelegt. Es ging uns darum zu zeigen, wie man — zumindest im Prinzip — *systematisch eine vollständige Übersicht* über die linearen Codes gewinnen kann, soweit Computer dies heute ermöglichen. Wir haben uns deshalb nicht gescheut, die in unseren Computerprogrammen verwandten Methoden im Detail zu

schildern, zumal sich diese als in der konstruktiven Theorie diskreter Strukturen ganz allgemein verwendbar erwiesen haben. Der interessierte Leser soll in die Lage versetzt werden, die Algorithmen zur Abzählung, Konstruktion und zufälligen Generierung von linearen Codes eigenständig zu implementieren.

Viele der hier aufgeführten Methoden und Resultate zur Abzählung von Isometrieklassen und zur Konstruktion von Repräsentanten sind neu. Sie erweitern die Ergebnisse von Slepian, auch auf nicht binäre Codes, stellenweise korrigieren sie diese.

Abzählung und Konstruktion gehören zusammen, denn die gefundenen Anzahlen verschaffen zunächst einen Überblick über den Umfang der Konstruktionsaufgabe, und sie dienen auch der Kontrolle über die Transversalenkonstruktion: Die ermittelten Anzahlen bestätigen die Längen der konstruierten Repräsentantensysteme.

Mit den vorgelegten Methoden zur Konstruktion von solchen Transversalen ist es nicht nur möglich, zu vorgegebenen Dimensionen und Längen Generatormatrizen von Codes mit der maximal erzielbaren Minimaldistanz anzugeben, sondern auch aufzuzeigen, wie viele wesentlich verschiedene lineare Codes mit dieser optimalen Minimaldistanz es wirklich gibt.

Es sollte ebenfalls nicht unerwähnt bleiben, daß die benutzten Konstruktionsverfahren auch in vielen anderen Fällen die Berechnung unnumerierter Strukturen wie Graphen, molekulare Graphen und Designs ermöglichen. Sie sind deshalb in voller Allgemeinheit beschrieben, weil sie die konstruktive Theorie diskreter Strukturen in bisher nicht erreichte Gebiete voranzutreiben erlauben.

Auch die hier beschriebene verbesserte Version des LLL-Algorithmus hat interessante neue Resultate gebracht, zum Beispiel gelang hiermit eine verbesserte Abschätzung der Minimaldistanz eines quadratische Reste-Codes, die bisher noch nicht bekannt war.

Beim Leser setzen wir Grundkenntnisse der Linearen Algebra und der Algebra voraus. Viele Grundbegriffe werden in den zahlreichen Übungsaufgaben aufgefrischt.

Es soll jetzt noch ein kurzer *Leitfaden* durch das Buch angegeben werden. Das Buch gliedert sich in drei Kapitel, die im wesentlichen unabhängig voneinander gelesen werden können:

- Das erste Kapitel dient der *Einführung in die Algebraischen Codierungstheorie.*
- Im zweiten Kapitel werden *zyklische Codes* und daraus abgeleitete weitere Klassen linearer Codes behandelt.
- Das dritte Kapitel ist den *Isometrieklassen* linearer Codes gewidmet, vor allem der computerunterstützten Abzählung und der Berechnung von Repräsentanten dieser Klassen.

Zur Schilderung der gegenseitigen Abhängigkeiten soll der Inhalt dieser Kapitel noch etwas ausführlicher angegeben werden:

Die ersten drei Abschnitte des einführenden Kapitels zur Algebraischen Codierungstheorie enthalten die wichtigsten Grundbegriffe dieser Theorie und der Theorie endlicher Körper, die folgenden Abschnitte können im wesentlichen unabhängig voneinander gelesen werden. Im weiteren Verlauf von Kapitel 1 lernt der Leser einerseits wichtige Klassen linearer Codes kennen und andererseits elementare Werkzeuge dieser Theorie.

Für das Kapitel 2 über zyklische Codes sind nur die Abschnitte 1.1, 1.2 sowie 1.3 Voraussetzung, allerdings wird in 2.1 eine Gruppenaktion der Galoisgruppe benutzt, so daß Grundkenntnisse über Gruppenoperationen, die in 3.1 detailliert geschildert werden, nützlich sind. Die in diesem Kapitel benötigte Polynomarithmetik ist in den Abschnitten 2.1 bis 2.4 zusammengefaßt. Sie ist grundlegend für den Aufbau der Theorie zyklischer Codes. Jedoch wird der Abschnitt 2.2 über die Summenzerlegung nur in 2.15, in den auch noch 2.14 einfließt, benötigt. In den Abschnitt 2.16 über Reed-Muller-Codes geht sowohl 2.13 und 2.14 als auch 1.8 ein.

Kapitel 3 ist weitgehend unabhängig von Kapitel 2 und beschäftigt sich intensiv mit der Abzählung und der Konstruktion der Äquivalenzklassen linearer Codes. Die Abzählung erfolgt in den Abschnitten 3.1 bis 3.4 mit algebraisch-kombinatorischen Hilfsmitteln, die der Theorie der endlichen Gruppenoperationen entstammen. In 3.5 bis 3.9 wenden wir uns der Konstruktion linearer Codes zu, auch hierfür spielen endliche Gruppenoperationen eine wichtige Rolle. Die Abschnitte 3.10 bis 3.12 bringen Ergänzungen und Anwendungen. Zunächst wird ein verfeinerter Ansatz zur Bestimmung der Minimaldistanz linearer Codes geschildert. Dann wird in 3.11 gezeigt, wie man lineare (n,k)-Codes zufällig und auf die Isometrieklassen gleichverteilt generieren kann. In 3.12 wird dies auf die Abzählung und Zufallserzeugung von Blockcodes verallgemeinert. In 3.13 wird abschließend ein kurzer Blick auf den Zusammenhang zwischen Matroiden und linearen Codes geworfen.

Wir möchten an dieser Stelle insbesondere den folgenden Kollegen danken, denen dieses Buch wertvolle Anregungen und Diskussionsbeiträge verdankt: E. F. Assmus Jr., T. Beth, I. Blake, M. de Boer, U. Eidt, A. Kohnert, W. Knapp, W. Müller, R. Laue, J. H. van Lint, A. Niemeyer, T. Scharf, D. Zerfowski.

Besonderer Dank der Autoren gilt der Deutschen Forschungsgemeinschaft und dem Österreichischen Fonds zur Förderung der wissenschaftlichen Forschung für hilfreiche finanzielle Unterstützung begleitender Forschungsprojekte. Die Durchführung dieser Projekte hat viel zur Vertiefung der Theorie beigetragen, sie hat zu Implementierungen entsprechender Programme und zum Sammeln umfangreichen Datenmaterials geführt. Viele dieser Daten und Programme sind mittlerweile auch den Interessenten via email oder Internet zugänglich.

Bayreuth, Graz, Hamburg-Harburg, im Juli 1998

A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, K.-H. Zimmermann

Inhaltsverzeichnis