# Vorwort

Der vorliegende Text ist entstanden aus dem Vorlesungsmanuskript zu meiner Vorlesung Codierungstheorie im Sommersemester 2001 an der Universität Ulm. Die Vorlesung richtete sich an Studenten, die über Grundkenntnisse in elementarer Algebra verfügen. In der Vorlesung wurden die Standardthemen der Codierungstheorie bis hin zu den algebraisch-geometrischen Codes behandelt; das entspricht etwa dem Inhalt der Kapitel 0 bis 6. Besondere Aufmerksamkeit wurde auch den konkreten Anwendungen in der Nachrichtentechnik wie etwa der Codierung von Daten auf Speichermedien gewidmet. Die elementare Codierungstheorie endet im Kapitel 5 mit der sehr schwierigen Frage nach der expliziten Konstruktion von fehlerkorrigierenden *linearen* Codes, die bei vorgegebener Blocklänge $n$ und Korrekturfähigkeit von $e$ Fehlern eine hohe Informationsrate haben. Es geht also um das kombinatorische Problem:

*Zu vorgegebenem $n$ und $e$ konstruiere man Untervektorräume $C \subset \mathbb{F}_q^n$ möglichst großer Dimension $k$, so dass jeweils zwei verschiedene Vektoren $x, y \in C$ sich in mindestens $d := 2e + 1$ Koordinaten unterscheiden.*

Dabei interessiert man sich insbesondere für Codes mit großer Blocklänge $n$. Dann wird diese Frage mit relativen Bezugsgrößen $R := k/n$ und $\delta := d/n$ gestellt. Dabei steht $R$ für die *Informationsrate* und $\delta$ für die *Zuverlässigkeit* des Codes. Diese beiden Größen konkurrieren miteinander. Elementare Überlegungen zeigen, dass $R + \delta \leq 1 + 1/n$ gelten muss. Weiterhin kann man auch sehr leicht die Existenz von kombinatorischen (eventuell nicht linearen) Codes zeigen, so dass $R + \delta \geq 1 - H(\delta)$ für eine gewisse Funktion $H(\delta)$ gilt; vgl. Bild 5.1 auf Seite 100. Jedoch ist es äußerst schwierig, Codes zu konstruieren, die diese untere Schranke erfüllen bzw. noch besser als diese sind und zusätzlich noch *linear* sind.

V.D. Goppa hat zu dieser Frage wichtige Beiträge geliefert; mit Hilfe von algebraischen Kurven konstruierte er Codes, die zur Lösung dieser Frage führten. Die Bearbeitung dieses Themas ist das eigentliche Ziel dieses Buches. In den Kapiteln 6 bis 9 werden die Theorie der algebraisch-geometrischen Codes und die dafür notwendigen Grundlagen über algebraische Kurven detailliert dargestellt. Dieser Teil des Buches fordert den Leser wesentlich mehr als der erste Teil, weil dazu fundierte Grundkenntnisse in Algebra vorausgesetzt sind.

Die Theorie der algebraischen Kurven wird zunächst in sehr kurzer Form in Abschnitt 6.1 referiert, um möglichst schnell zu den algebraisch-geometrischen Codes zu kommen. Zum Verständnis dieser Codes benötigt man im Wesentlichen nur den Satz von Riemann-Roch und den Residuensatz, wobei die Kenntnis der Beweise die-

ser Sätze nicht erforderlich ist. Das Hauptanliegen in Kapitel 6 ist es, die Frage nach optimalen Codes in ein Problem über rationale Punkte auf Kurven zu übersetzen und (optimale) Kurven mit vielen rationalen Punkten zu konstruieren. Diese Beispiele gehen auf die Arbeit von Garcia und Stichtenoth [G-S] zurück. Die hier gegebenen Beweise sind geometrischer Natur im Gegensatz zum Vorgehen in [G-S], wo mittels Funktionenkörper argumentiert wird.

Anschließend wird der Problemkreis der Anzahl von rationalen Punkten auf algebraischen Kurven über endlichen Körpern intensiv weiter verfolgt. In Kapitel 7 wird die Theorie der Zetafunktion einer algebraischen Kurve behandelt; die Rationalität der Zetafunktion sowie die Riemannsche Vermutung im Kurvenfall werden vollständig bewiesen. Damit wird die Hasse-Weil-Schranke für die Anzahl der rationalen Punkte auf einer algebraischen Kurve hergeleitet. Als Folgerungen gewinnt man die Schranken von Serre und Drinfeld-Vladut. Durch die Beispiele in Kapitel 6 wird somit die Drinfeld-Vladut-Schranke als scharfe Abschätzung im Fall eines Grundkörpers mit $q^2$ Elementen nachgewiesen.

In Kapitel 9 wird die Codierung und Decodierung von algebraisch-geometrischen Codes erklärt. Für die Codierung wird ein effektiver Algorithmus zur Berechnung einer Basis von $L(D)$ beschrieben, der originär auf Hensel und Landsberg zurückgeht und von Coates in [Co] wieder aufgegriffen wurde. Das Decodierungsverfahren von Skorobogatov und Vladut, das eigentlich nur für kleine Fehlerraten arbeitet, sowie das Verfahren von Feng und Rao, das Fehlergrößen bis zum designierten Abstand