Diskrete Mathematik

Andreas Paffenholz

TECHNISCHE UNIVERSITÄT DARMSTADT

WiSe 2022/23
26. Januar 2023
Aufgabenblatt 13

Aufgabe 13.1: Reed-Solomon Codes

Wir betrachten einen zyklischen Code C über dem endlichen Körper $K := \mathbb{Z}_q^n$ für eine Primzalhpotenz q. Sei α ein primitives Element der multiplikativen Gruppe K^*. Dann ist $K^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$ und

$$x^{q-1} \;=\; (x-1)(x-\alpha)\cdots(x-\alpha^{q-2})\,.$$

Sei $1 \leq d \leq q-2$. Wir setzen

$$g(x) \;:=\; (x-1)(x-\alpha)\cdots(x-\alpha^{d-2})\,,$$

und fassen $g(x)$ als Erzeugerpolynom eines Codes C der Länge $n := q-1$ auf.

1. Sei $a(x) = \sum_{i=0}^{n-1} a_i x^i \in C$. Zeigen Sie, dass $a(\alpha^j) = 0$ für $0 \leq j \leq d-2$.
2. Wir setzen $\alpha_j := \alpha^j$. Folgern Sie, dass $\sum_{i=0}^{n-1} a_i \alpha_j^i = 0$ für $1 \leq j \leq d-2$, und daraus, dass

$$H \;:=\; \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1^{n-1} & \alpha_1^{n-2} & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ \alpha_{d-2}^{n-1} & \alpha_{d-2}^{n-2} & \cdots & 1 \end{bmatrix}.$$

   die Kontrollmatrix von C ist.
3. Zeigen Sie, dass je $d-1$ Spalten von H linear unabhängig sind.

   Hinweis: Es kann helfen, sich an Vandermonde-Matrizen zu erinnern.
4. Folgern Sie, dass $d(C) \geq d$.
5. Stellen Sie die Kontrollmatrix für $q = 7$ und $d = 5$ auf und bestimmen Sie eine Generatormatrix.

Bemerkung: Diese Codes heißen *Reed-Solomon*-Codes. Sie werden unter anderem bei der Speicherung auf CDs eingesetzt.

Aufgabe 13.2: Singleton-Schranke

Sei $C \subseteq \mathbb{Z}_q^n$ ein linearer Code mit $d(C) = d$.

1. Zeigen Sie, dass $|C| \leq q^{n-d-1}$.

   Hinweis: Wählen Sie $r := n-d+1$ Koordinaten und betrachten Sie die Projektion $\mathbb{Z}_q^n \to \mathbb{Z}_q^r$ auf diese Koordinaten.
2. Codes, die diese Ungleichung mit Gleichheit erfüllen, heißen *Maximum-Distance-Separable* oder *MDS*-Codes. Zeigen Sie, dass die Reed-Solomon-Codes aus Aufgabe 13.1 MDS-Codes sind.

Aufgabe 13.3: Affine Ebenen

Sei Q eine projektive Ebene der Ordnung q, also mit q^2+q+1 Punkten. Sei g eine beliebige Gerade in Q und A die Konfiguration, die wir erhalten, wenn wir g mit allen Punkten, die auf g liegen, aus Q löschen.

1. Zeigen Sie, dass A ein $2-(q^2,q,1)$-Design ist, also eine Punktmenge von q^2 Punkten P und Mengen B von je q Punkten, so dass jedes Paar aus P in genau einem B enthalten ist.
2. Zeigen Sie, dass sich B so in $q+1$ Mengen partitionieren lässt, dass sich zwei Geraden aus B genau dann schneiden, wenn sie nicht in der gleichen Menge liegen.

Bemerkung: Eine solche Menge A heißt *endliche affine Ebene*. Die Partitionen im zweiten Teil sind die Äquvalenzklassen paralleler Geraden.

Aufgabe 13.4: 1-Designs

Zeigen Sie, dass es genau dann ein 1-(ν,k,λ)-Design gibt, wenn k ein Teiler von $\nu\lambda$ ist.

Hinweis: Zur Konstruktion eines solchen Designs können Sie mit beliebigen β Mengen der Größe k beginnen und sich überlegen, dass Sie ein Element, dass noch nicht λ oft vorkommt, mit einem vertauschen können, das zu oft vorkommt.

$*$ Aufgabe 13.5: 3-Färbungen eines triangulierten Graphen

Sei $G=(V,E)$ ein ebener Graph, bei dem alle Länder (auch das äußere) Dreiecke sind, also genau drei Kanten am Rand haben. Sei $c:V\to[3]$ eine beliebige Abbildung. Zeigen Sie, dass dann die Zahl der Länder, an deren Ecken alle drei Farben vorkommen, gerade ist.

$*$ Aufgabe 13.6: Binäre Codes

Sei C ein binärer linearer Code. Zeigen Sie, dass in C entweder alle Codewörter gerades Gewicht haben, oder die Hälfte der Codewörter gerades Gewicht und die andere Hälfte ungerades Gewicht haben.