Perfekte Codes

Vorlesung zur Diskreten Mathematik
Sommersemester 2020

Benjamin Sambale
Leibniz Universität Hannover

9. Januar 2022

Bemerkung 1. Sei $\mathbb{F}_q$ ein Körper mit $q < \infty$ Elementen (in der Algebra zeigt man, dass q eine Primzahlpotenz sein muss). Ein *Code* der *Länge* n über $\mathbb{F}_q$ ist eine nichtleere Teilmenge $C \subseteq \mathbb{F}_q^n$. Man nennt C *linear*, falls C ein Unterraum von $\mathbb{F}_q^n$ ist (wir schreiben dann $C \leq \mathbb{F}_q^n$). Man nennt C einen (n,k)-Code, falls $k = \dim C$.

Satz 2 (HAMMING-Schranke)**.** *Sei $C \leq \mathbb{F}_q^n$ ein (n,k)-Code, der e Fehler korrigieren kann. Dann gilt*

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i \leq q^{n-k}$$

mit Gleichheit genau dann, wenn C e-perfekt ist.

Beweis. Nach Definition 1.6 ist $B_e(c) \cap B_e(d) = \varnothing$ für verschiedene $c, d \in C$. Sei $x \in B_e(c)$ mit $d(x,c) = i$. Dann unterscheiden sich x und c an genau i Positionen. Für die Wahl dieser Positionen gibt es $\binom{n}{i}$ Möglichkeiten. An Position j kann sich x_j auf $q-1$ Weisen von c_j unterscheiden. Dies zeigt

$$|B_e(c)| = \sum_{i=0}^{e} \binom{n}{i} (q-1)^i.$$

Es folgt

$$q^k \sum_{i=0}^{e} \binom{n}{i} (q-1)^i = \sum_{c \in C} |B_e(c)| = \Big| \dot{\bigcup_{c \in C}} B_e(c) \Big| \leq |\mathbb{F}_q^n| = q^n$$

mit Gleichheit genau dann, wenn $\mathbb{F}_q^n = \dot{\bigcup}_{c \in C} B_e(c)$. □

Beispiel 3. Sei $C \leq \mathbb{F}_2^n$ ein 3-perfekter Code mit Dimension $k \geq 1$. Dann ist $n \geq 7$ und

$$1 + n + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)}{6} = \sum_{i=0}^{e} \binom{n}{i} = 2^{n-k}.$$

Multiplikation mit 6 liefert

$$(n+1)(6 + n(n-1)) = 3 \cdot 2^{n-k+1}.$$

Die Substitution $N := n + 1 \geq 8$ führt zu

$$N(N^2 - 3N + 8) = 3 \cdot 2^{n-k+1}.$$

Ist N durch 16 teilbar, so ist $N^2 - 3N + 8 \equiv 8 \pmod{16}$ und es folgt $N^2 - 3N + 8 \in \{8, 24\}$. Dies widerspricht $N(N-3) + 8 \geq 8 \cdot 5 + 8 > 24$. Also ist N nicht durch 16 teilbar und man erhält $N \mid 24$. Wegen $N \geq 8$ ergeben sich folgende Fälle:

- $(n, k) = (7, 1)$: Dies sind die Parameter des Wiederholungscodes $\mathbb{F}_2(1, \ldots, 1)$ (siehe Beispiel 10).
- $n = 11$: Hier geht die Gleichung nicht auf: $N^2 - 3N + 8 = 12 \cdot 9 + 8 = 116 = 4 \cdot 29$.
- $(n, k) = (23, 12)$: Ein solcher Code wird in Definition 15 definiert.

Definition 4. Eine Matrix $P \in \mathbb{F}_q^{n \times n}$ heißt *verallgemeinerte Permutationsmatrix*, falls P in jeder Zeile und in jeder Spalte genau einen Eintrag $\neq 0$ besitzt. Codes $C, C' \subseteq \mathbb{F}_q^n$ heißen *äquivalent*, falls eine verallgemeinerte Permutationsmatrix $P \in \mathbb{F}_q^{n \times n}$ mit $C' = \{Px : x \in C\}$ existiert.

Bemerkung 5. Offenbar haben äquivalente Codes die gleichen Parameter (Länge, Dimension, Minimalabstand). Für $q = 2$ ist jede verallgemeinerte Permutationsmatrix eine (gewöhnliche) Permutationsmatrix und äquivalente Codes unterscheiden sich nur durch Permutation der Koordinaten.

Definition 6. Sei $m \geq 2$. Seien $\mathbb{F}_q v_1, \ldots \mathbb{F}_q v_n$ die 1-dimensionalen Unterräume von $\mathbb{F}_q^m$. Der lineare Code $H_n \leq \mathbb{F}_q^n$ mit Kontrollmatrix $M := (v_1, \ldots, v_n) \in \mathbb{F}_q^{m \times n}$ heißt *Hamming-Code* (Erinnerung: $H_n = \{x \in \mathbb{F}_q^n : Mx = 0\}$).

Bemerkung 7. Wählt man andere Repräsentanten $v_1, \ldots, v_n$ für die 1-dimensionalen Unterräume, so erhält man einen äquivalenten Code. Daher hängt H_n nicht wesentlich von der Wahl der $v_1, \ldots, v_n$ ab.

Satz 8. *Der Hamming-Code H_n hat Länge $n = \frac{q^m - 1}{q - 1}$, Dimension $n - m$ und ist 1-perfekt.*

Beweis. Jeder Vektor $v \in \mathbb{F}_q^m \setminus \{0\}$ spannt einen 1-dimensionalen Unterraum mit q Elementen auf. Je zwei 1-dimensionale Unterräume haben den Schnitt $\{0\}$. Dies zeigt $n = \frac{q^m - 1}{q - 1}$. Die Spalten der Kontrollmatrix M von H_n enthalten eine Basis von $\mathbb{F}_q^m$. Insbesondere hat M vollen Rang und H_n hat Dimension $n - m$. Besitzt H_n ein Codewort $c \neq 0$ mit Gewicht $w(c) \leq 2$, so wären zwei Spalten v_i, v_j von M linear abhängig. Dies widerspricht $\mathbb{F}_q v_i \neq \mathbb{F}_q v_j$ für $i \neq j$. Daher ist $d_{\min}(H_n) \geq 3$ und H_n kann einen Fehler korrigieren (Bemerkung 1.8). Die Hamming-Schranke hat die Form

$$\binom{n}{0}(q-1)^0 + \binom{n}{1}(q-1) = 1 + n(q-1) = 1 + q^m - 1 = q^m = q^{n-(n-m)},$$

d. h. H_n ist 1-perfekt. □

Satz 9. *Jeder lineare 1-perfekte Code ist zu einem Hamming-Code äquivalent.*

Beweis. Sei C ein linearer 1-perfekter (n, k)-Code. Die Hamming-Schranke liefert $1 + n(q-1) = q^{n-k}$, d. h. $n = \frac{q^m - 1}{q - 1}$ mit $m := n - k$. Wegen $d_{\min}(C) \geq 3$ sind je zwei Spalten einer Kontrollmatrix $M \in \mathbb{F}_q^{m \times n}$ von C linear unabhängig. Die Anzahl der 1-dimensionalen Unterräume von $\mathbb{F}_q^m$ ist andererseits $\frac{q^m - 1}{q - 1} = n$. Daher ist M eine Kontrollmatrix von H_n. □

Beispiel 10. Der Wiederholungscode $C = \mathbb{F}_2(1, 1, 1) \leq \mathbb{F}_2^3$ ist offenbar 1-perfekt und muss daher zu H_3 äquivalent sein. Allgemeiner sind die Wiederholungscodes $\mathbb{F}_2(1, \ldots, 1) \leq \mathbb{F}_2^{2n+1}$ stets n-perfekt, denn jedes $x \in \mathbb{F}_2^{2n+1}$ unterscheidet sich an höchstens n Stellen von genau einem der beiden Codewörter $(0, \ldots, 0)$ oder $(1, \ldots, 1)$.

Definition 11. Sei $C \leq \mathbb{F}_q^n$ ein linearer Code mit Erzeugermatrix $G \in \mathbb{F}_q^{k \times n}$. Man nennt

$$C^\perp := \{x \in \mathbb{F}_q^n : Gx = 0\} \leq \mathbb{F}_q^n$$

den zu C *dualen* Code. Im Fall $C = C^\perp$ heißt C *selbstdual*.

Bemerkung 12.

(i) Eine Erzeugermatrix (bzw. Kontrollmatrix) von C ist eine Kontrollmatrix (bzw. Erzeugermatrix) von $C^\perp$. Insbesondere ist $\dim C + \dim C^\perp = n$ und $(C^\perp)^\perp = C$. Selbstduale Codes haben daher gerade Länge $n = 2k$ und Dimension k.

(ii) Im Gegensatz zum euklidischen Raum $\mathbb{R}^n$, kann über $\mathbb{F}_q^n$ durchaus $C = C^\perp \neq 0$ eintreten.

Definition 13. Der lineare Code $G_{12} \leq \mathbb{F}_3^{12}$ mit Erzeugermatrix

$$\begin{pmatrix}
1 & . & . & . & . & . & . & 1 & 1 & 1 & 1 & 1 \\
. & 1 & . & . & . & . & 1 & . & -1 & 1 & 1 & -1 \\
. & . & 1 & . & . & . & 1 & -1 & . & -1 & 1 & 1 \\
. & . & . & 1 & . & . & 1 & 1 & -1 & . & -1 & 1 \\
. & . & . & . & 1 & . & 1 & 1 & 1 & -1 & . & -1 \\
. & . & . & . & . & 1 & 1 & -1 & 1 & 1 & -1 & .
\end{pmatrix}$$

heißt *erweiterter ternärer Golay-Code* G_{12}. Das Bild der Projektion $G_{12} \to \mathbb{F}_3^{11}$ auf die ersten 11 Koordinaten ist der *ternären Golay-Code* G_{11} (d. h. G_{11} entsteht durch Streichen der letzten Koordinate aus G_{12}).

Satz 14. *Es gilt*

(i) G_{12} *ist ein selbstdualer* $(12, 6)$*-Code mit Minimalgewicht* 6.

(ii) G_{11} *ist ein* 2*-perfekter* $(11, 6)$*-Code.*

Beweis.

(i) Sei M die in Definition 13 angegebene Erzeugermatrix von G_{12}. Da M Rang 6 hat, ist G_{12} ein $(12, 6)$-Code. Offenbar hat jede Zeile von M Gewicht 6. Wegen $MM^{\mathrm{t}} = 0$ ist G_{12} selbstdual. Für $c = (x_1, \ldots, x_{12}) \in C$ gilt daher

$$w(c) = x_1^2 + \ldots + x_{12}^2 = cc^{\mathrm{t}} \equiv 0 \pmod 3.$$

Zwei verschiedene Zeilen c und d von M unterscheiden sich an genau zwei Stellen auf den ersten sechs Koordinaten. Auf den letzten sechs Koordinaten unterscheiden sich c und d mindestens an den beiden Positionen der Nullen. Jede Linearkombination x von c und d hat daher Gewicht $w(x) = 6$ wegen $3 \mid w(x)$. Also besitzt x genau zwei Nullen auf den letzten sechs Koordinaten. Eine Linearkombination von drei verschiedenen Zeilen von M hat folglich mindestens Gewicht 6. Jede Linearkombination von mehr als drei Zeilen hat bereits mindestens vier von Null verschiedene Einträge auf den ersten sechs Koordinaten. Dies zeigt $d_{\min}(G_{12}) = 6$.

(ii) Wegen $d_{\min}(G_{12}) = 6$ ist die Projektion $G_{12} \to G_{11}$ injektiv. Also ist G_{11} ein $(11, 6)$-Code mit Minimalabstand 5. Die Hamming-Schranke hat die Form

$$1 + \binom{11}{1}2 + \binom{11}{2}4 = 1 + 22 + 220 = 243 = 3^5 = 3^{11-6},$$

d. h. G_{11} ist 2-perfekt. □

Definition 15. Seien C und $\widetilde{C}$ die (äquivalenten) $(8, 4)$-Codes über $\mathbb{F}_2$ mit Erzeugermatrizen

$$G = \begin{pmatrix} 1 & 1 & . & 1 & . & . & . & 1 \\ . & 1 & 1 & . & 1 & . & . & 1 \\ . & . & 1 & 1 & . & 1 & . & 1 \\ . & . & . & 1 & 1 & . & 1 & 1 \end{pmatrix} \qquad \widetilde{G} = \begin{pmatrix} . & . & . & 1 & . & 1 & 1 & 1 \\ . & . & 1 & . & 1 & 1 & . & 1 \\ . & 1 & . & 1 & 1 & . & . & 1 \\ 1 & . & 1 & 1 & . & . & . & 1 \end{pmatrix}.$$

Wegen $GG^{\mathrm{t}} = 0 = \widetilde{G}\widetilde{G}^{\mathrm{t}}$ sind C und $\widetilde{C}$ selbstdual. Wir definieren den *erweiterten binären Golay-Code*

$$G_{24} := \big\{(c + e, d + e, c + d + e) : c, d \in C,\ e \in \widetilde{C}\big\} \leq \mathbb{F}_2^{24}.$$

Der *binäre Golay-Code* $G_{23} \leq \mathbb{F}_2^{23}$ ist das Bild der Projektion $G_{24} \to \mathbb{F}_2^{23}$ auf die ersten 23 Koordinaten.

Satz 16. *Es gilt:*

(i) G_{24} *ist ein selbstdualer* $(24, 12)$*-Code mit Minimalgewicht* 8.

(ii) G_{23} *ist ein* 3*-perfekter* $(23, 12)$*-Code.*

Beweis.

(i) Wir benutzen die Bezeichnungen aus Definition 15. Addiert man die 1., 3. und 4. Zeile von G bzw. $\widetilde{G}$, so erhält man $\mathbb{F}_2(1, \ldots, 1) \subseteq C \cap \widetilde{C}$. Wir zeigen, dass $C \cap \widetilde{C}$ nicht größer ist. Seien dafür $x, y \in \mathbb{F}_2^4$ mit $xG = y\widetilde{G}$. Dann ist $(x, y)\binom{G}{\widetilde{G}} = 0$. Der Gauß-Algorithmus zeigt

$$\binom{G}{\widetilde{G}} \sim \left(\begin{array}{cccccccc} 1 & 1 & . & 1 & . & . & . & 1 \\ . & 1 & 1 & . & 1 & . & . & 1 \\ . & . & 1 & 1 & . & 1 & . & 1 \\ . & . & . & 1 & 1 & . & 1 & 1 \\ \hline . & . & . & . & 1 & 1 & . & . \\ . & . & . & 1 & 1 & . & . & . \\ . & . & 1 & 1 & . & . & . & . \\ . & 1 & 1 & . & . & . & . & . \end{array}\right) \sim \left(\begin{array}{cccccccc} 1 & 1 & . & 1 & . & . & . & 1 \\ . & 1 & 1 & . & 1 & . & . & 1 \\ . & . & 1 & 1 & . & 1 & . & 1 \\ . & . & . & 1 & 1 & . & 1 & 1 \\ \hline . & . & . & . & 1 & 1 & . & . \\ . & . & . & . & . & . & 1 & 1 \\ . & . & . & . & . & 1 & . & 1 \\ . & . & . & . & 1 & . & . & 1 \end{array}\right) \sim \left(\begin{array}{cccccccc} 1 & 1 & . & 1 & . & . & . & 1 \\ . & 1 & 1 & . & 1 & . & . & 1 \\ . & . & 1 & 1 & . & 1 & . & 1 \\ . & . & . & 1 & 1 & . & 1 & 1 \\ \hline . & . & . & . & 1 & 1 & . & . \\ . & . & . & . & . & 1 & . & 1 \\ . & . & . & . & . & . & 1 & 1 \\ . & . & . & . & . & . & . & . \end{array}\right)$$

Also hat $\binom{G}{\widetilde{G}}$ Rang 7 und es folgt $C \cap \widetilde{C} = \mathbb{F}_2(1, \ldots, 1)$. Die Codeworte der Form $(c, 0, c)$, $(0, d, d)$ und (e, e, e) mit $c, d \in C$ und $e \in \widetilde{C}$ bilden ein Erzeugendensystem von G_{24}. Im Fall $(c, 0, c) + (0, d, d) = (e, e, e)$ ist $c = e = d = c + d = 0$. Dies zeigt

$$\dim G_{24} = \dim C + \dim C + \dim \widetilde{C} = 4 + 4 + 4 = 12.$$

Da C und $\widetilde{C}$ selbstdual sind, sind die Vektoren $(c, 0, c)$, $(0, d, d)$ und (e, e, e) paarweise orthogonal. Also ist auch G_{24} selbstdual.

Je zwei Zeilen c und d von G (oder $\widetilde{G}$) haben Gewicht 4. Wegen $cd^{\mathrm{t}} = 0$ haben c und d eine gerade Anzahl von Einsen gemeinsam. In der Summe $c + d$ heben sich die gemeinsamen Einsen

gegenseitig auf. Daraus folgt, dass $w(c+d)$ durch 4 teilbar ist. Für eine weitere Zeile e von G ist nun auch $w(c+d+e)$ durch 4 teilbar usw. Insgesamt ist $4 \mid w(c)$ für alle $c \in C \cup \widetilde{C}$. Mit dem gleichen Argument folgt $4 \mid w(x)$ für alle $x \in G_{24}$, da auch G_{24} selbstdual ist. Insbesondere ist $d_{\min}(G_{24}) \geq 4$. Nehmen wir an, es existiert $x = (c+e, d+e, c+d+e) \in G_{24}$ mit Gewicht 4. Da jede der drei Komponenten gerades Gewicht hat, muss einer der drei Komponenten 0 sein. Dann ist $e \in C \cap \widetilde{C} = \mathbb{F}_2(1, \ldots, 1)$ und man erhält leicht einen Widerspruch. Daher ist $d_{\min}(G_{24}) \geq 8$. Für $c \in C$ mit $w(c) = 4$ ist $w((c, 0, c)) = 8 \leq d_{\min}(G_{24})$.

(ii) Wegen $d_{\min}(G_{24}) = 8$ ist die Projektion $G_{24} \to G_{23}$ injektiv. Also ist G_{23} ein $(23, 12)$-Code mit Minimalgewicht ≥ 7. Nach Bemerkung 1.8 kann G_{23} $e = 3$ Fehler korrigieren. Die Hamming-Schranke hat die Form

$$\sum_{i=0}^{3} \binom{23}{i} = 1 + 23 + 23 \cdot 11 + 23 \cdot 11 \cdot 7 = 1 + 23 \cdot 89 = 2048 = 2^{11} = 2^{23-12},$$

d. h. G_{23} ist 3-perfekt. □

Satz 17 (van Lint, Tietäväinen)**.** *Jeder lineare perfekte Code ist äquivalent zu einem der folgenden Codes:*

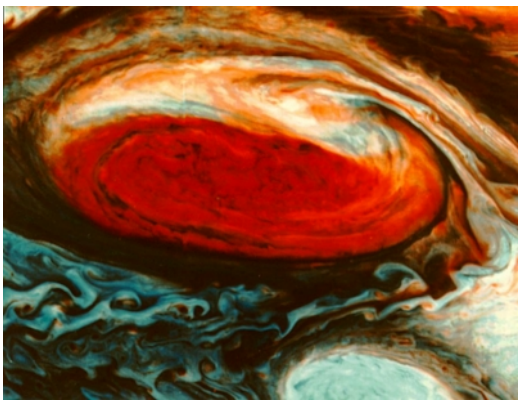
- *der* 0*-perfekte triviale* (n, n)*-Code* $\mathbb{F}_q^n$*.*
- *der* n*-perfekte triviale* $(n, 0)$*-Code* $\{0\}$*.*
- *der* n*-perfekte binäre* $(2n+1, 1)$*-Wiederholungscode* $\mathbb{F}_2(1, \ldots, 1)$*.*
- *der* 1*-perfekte* $(n, n-m)$*-Hamming-Code* H_n*, wobei* $n = \frac{q^m-1}{q-1}$*.*
- *der* 2*-perfekte ternäre Golay-Code* G_{23}*.*
- *der* 3*-perfekte binäre Golay-Code* G_{11}*.*

Beweis. Schwierig. □

Bemerkung 18.

(i) Die Klassifikation nicht-linearer perfekter Codes über beliebigen Alphabeten ist noch offen.

(ii) Die Voyager-Sonden sende(te)n mit Hilfe des Golay-Codes G_{24} Bilder vom Weltraum zur Erde. Zum Beispiel dieses (Was ist zu sehen?):



(iii) Für einen binären Code $C \subseteq \mathbb{F}_2^n$ nennt man

$$\mathrm{Aut}(C) := \{\pi \in S_n : \forall (x_1, \ldots, x_n) \in C : (x_{\pi(1)}, \ldots, x_{\pi(n)}) \in C\}$$

die *Automorphismengruppe* von C. Die Gruppe $M_{24} := \mathrm{Aut}(G_{24})$ heißt *Mathieugruppe* vom Grad 24. Sie gehören zu den sporadisch einfachen Gruppen. John Conway (am 11.04.2020 an Corona gestorben) bezeichnete M_{24} als "most remarkable of all finite groups". Es gilt

$$|M_{24}| = 244.823.040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23.$$