

Teilmusterlösung - zweite und vierte Aufgabe

Martin C. Götze

18. Januar 2008

Aufgabe 2. Sei C ein binärer (n, k) -Linearcode, in dem es Codewörter ungeraden Gewichts gibt. Bezeichne C^* den Code $\{a_1 a_2 \dots a_n a_{n+1} \mid a_1 \dots a_n \in C \text{ und } a_{n+1} = \bigoplus_{i=1}^n a_i\}$, das ist der sogenannte erweiterte Code zu C .

- (i) Zeigen Sie, dass C^* ein $(n+1, k)$ -Linearcode ist.
- (ii) Falls $d(C)$ ungerade ist, so ist $d(C^*) = d(C) + 1$.
- (i) Wir bemerken zunächst, dass die Abbildung

$$\varphi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2, \quad (a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i$$

linear ist, denn es ist für $a, b \in \mathbb{F}_2^n$:

$$\begin{aligned} \varphi(a+b) &= \sum_{i=1}^n (a_i + b_i) \\ &= \sum_{i=1}^n a_i + \sum_{i=1}^n b_i \\ &= \varphi(a) + \varphi(b). \end{aligned}$$

Mithin ist auch die zusammengesetzte Abbildung

$$\psi := \text{id} \oplus \varphi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^{n+1}, \quad (a_1, \dots, a_n) \mapsto \left(a_1, \dots, a_n, \sum_{i=1}^n a_i \right)$$

linear.

Nun ist ψ offenbar injektiv, denn ist $a \in \mathbb{F}_2^n$ mit $\psi(a) = 0$, so ist insbesondere $a_i = 0$ für $1 \leq i \leq n$, also $a = 0$. Als Bild des k -dimensionalen Unterraums $C \subset \mathbb{F}_2^n$ unter der linearen Injektion ψ ist $C^* = \psi(C) \subset \mathbb{F}_2^{n+1}$ ein k -dimensionaler Unterraum, mithin ein $(n+1, k)$ -Linearcode.

(ii) Sei $c \in C$ mit geradem Gewicht. Dann ist $\varphi(c) = 0$, also $\psi(c) = c0$, d. h.

$$w(\psi(c)) = w(c)$$

hat c ungerades Gewicht, so $\varphi(c) = 1$, mithin $\psi(c) = c1$, also

$$w(\psi(c)) = w(c) + 1$$

Wir haben also stets $w(\psi(c)) \geq w(c)$, woraus $d(C^*) \geq d(C)$ folgt, ist $d(C)$ ungerade, so haben die Bilder aller Codewörter mit Abstand $d(C)$ den Abstand $d(C) + 1$, mithin ist $d(C^*) = d(C) + 1$, falls $d(C)$ ungerade ist.

Aufgabe 4. Konstruieren Sie die Checkmatrix eines $(4, 2, 3)$ -Codes über einem möglichst kleinem Alphabet. Konstruieren Sie dann aus der Checkmatrix die Generatormatrix Ihres Codes.

Ein $(4,2,3)$ -Linearcode C über \mathbb{F}_q ist als Code mit Minimalabstand drei gerade 1-fehlerkorrigierend. Wegen $|C| = q^2$ muss also

$$\begin{aligned} q^2 \cdot \sum_{i=0}^1 \binom{4}{i} (q-1)^i &\leq q^4 \\ \iff q^2(1 + 4(q-1)) &\leq q^4 \\ \iff 4q - 3 &\leq q^2 \\ \iff (q-2)^2 - 1 &\geq 0 \\ \iff (q-2)^2 &\geq 1 \end{aligned}$$

Die kleinste Primpotenz q , die diese Ungleichung erfüllt, ist $q = 3$. Um die Kontrollmatrix zu konstruieren, schreiben wir sie zunächst also $H = (A|E_2)$. Wegen $d(C) = 3$ müssen je zwei Spalten von H linear unabhängig sein. Wir wählen also

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$$

Wir erhalten dann die Generatormatrix als

$$G = \begin{pmatrix} E_2 \\ -A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 2 \\ 2 & 1 \end{pmatrix}$$

Damit ist alles getan.