Gruppe $\boxed{9}$ Phil Pützstück, 377247
Lineare Algebra für Informatiker

Hausaufgabe 5

Aufgabe 28

a) Sei $v \in K^n, i \in [0, n]$. Dann ist $d(v, w) = |\{j \mid v_j - w_j \neq 0\}|$ für $w \in K^n$.
Insbesondere: wenn $d(v, w) = i$, dann gibt es Indizes $j_1, \cdots, j_i \in [1, n]$ sodass

$$\forall k \in [1, i] : v_{j_k} - w_{j_k} \neq 0$$

Auf deutsch; wir können i verschieden Indizes aus $[1, n]$ wählen an denen sich v und w unterscheiden. Offensichtlich gibt es genau $\binom{n}{i}$ Möglichkeiten diese i Indizes von den möglichen n zu wählen. Weiter folgt aus $|K| = q$, dass es genau $q - 1$ Elemente aus K ungleich 0 gibt.
Wir haben also zu jedem der gewählten Indizes $(j_k)_{k \in [1,i]}$ genau $q - 1$ Möglichkeiten w_{j_k} einen Wert aus K zuzuweisen, sodass $v_{j_k} - w_{j_k} \neq 0$ ist. Um also ein $w \in K^n$ zu finden, sodass $d(v, w) = i$, wählen wir zuerst die i Indizes an denen sich w von v unterscheidet und dann für jeden dieser Indizes einen Wert aus $q - 1$ Möglichkeiten.

Insgesamt haben wir nach der Produktregel der Kombinatorik damit:

$$|\{w \in K^n \mid d(v, w) = i\}| = \binom{n}{i} \prod_{k=1}^{i} (q - 1) = \binom{n}{i} (q - 1)^i$$

b) Da $d(C) = 2e + 1$ haben wir $e \leq d(C) \leq n$, wir können also das Resultat aus a) verwenden:

$$|B_{e+1}(v)| = |\{w \in K^n \mid d(v, w) < e + 1\}| = |\dot{\bigcup_{i \in [0,e]}} \{w \in K^n \mid d(v, w) = i\}| = \sum_{i=0}^{e} \binom{n}{i} (q - 1)^i$$

c) Da $d(C) = 2e + 1$ und $e \in \mathbb{N}$ ist $d(C)$ ungerade und $e + 1 = \frac{d(C)+1}{2}$.
Ebenso ist auch stets $d(w, w') \in \mathbb{N}$ für $w, w' \in K^n$. Insbesondere folgt damit:

$$B_{e+1}(c) = B_{\frac{d(C)+1}{2}}(c) = B_{\frac{d(C)}{2}}(c)$$

Da durch die Parität von $d(C)$ dann $\{x \in \mathbb{N}_0 \mid x < \frac{d(C)+1}{2}\} = \{x \in \mathbb{N}_0 \mid x < \frac{d(C)}{2}\} = [0, e]$ gilt.

Wir wissen weiter, dass für $c, c' \in C$ gilt:

$$B_{\frac{d(C)}{2}}(c) \cap B_{\frac{d(C)}{2}}(c') = \varnothing \qquad \text{sowie} \qquad B_{\frac{d(C)}{2}}(c) \cap C = \{c\}$$

Aus dieser Disjunktheit folgt dann

$$\forall c \in C : |B_{\frac{d(C)}{2}}(c)| = \sum_{i=0}^{e} \binom{n}{i} (q - 1)^i$$

Da also alle diese Kugeln disjunkt sind, haben wir mindestens $|C| \cdot \sum_{i=0}^{e} \binom{n}{i}(q-1)^i$ verschiedene Elemente aus K^n in den Kugeln der Codes von C. Offensichtlich sind das kleiner oder gleichviele wie alle Elemente von K^n. Ferner ist $|K| = q$ also $|K^n| = q^n$. Insgesamt folgt:

$$|C| \sum_{i=0}^{e} \binom{n}{i} (q-1)^i \leq q^n \qquad \Longleftrightarrow \qquad |C| \leq \frac{q^n}{\sum_{i=0}^{e} \binom{n}{i}(q-1)^i}$$

Aufgabe 29

a) Wir wählen $\mathcal{B} := \left(\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right)$. Da $\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \mathcal{B}_1 + \mathcal{B}_2$, ist $\mathcal{B}$ ein EZS von C.

Weiter gilt für $a_1, a_2, a_3, a_4 \in K = \mathbb{F}_2$:

$$\sum_{i=1}^{4} a_i \mathcal{B}_i = \begin{pmatrix} a_1 + a_3 + a_4 \\ a_1 + a_4 \\ a_3 + a_4 \\ a_2 + a_4 \\ a_2 \end{pmatrix} = 0 \Longrightarrow a_2 = 0 \Longrightarrow \begin{pmatrix} a_1 + a_3 + a_4 \\ a_1 + a_4 \\ a_3 + a_4 \\ a_4 \\ 0 \end{pmatrix} = 0 \Longrightarrow a_4 = 0$$

$$\Longrightarrow \begin{pmatrix} a_1 + a_3 \\ a_1 \\ a_3 \\ 0 \\ 0 \end{pmatrix} = 0 \Longrightarrow a_1 = a_2 = a_3 = a_4 = 0$$

Folglich ist $\mathcal{B}$ auch l.u. und damit eine Basis von C.

b) Nach Proposition 3.73 gilt

$$\mathrm{Sol}(H, 0) = \mathrm{Col}(A) \qquad \Longleftrightarrow \qquad \mathrm{Sol}(A^{\mathrm{tr}}, 0) = \mathrm{Col}(H^{\mathrm{tr}})$$

Sei also $A \in K^{5 \times 4} = \mathbb{F}_2^{5 \times 4}$ mit $A_{-,i} = \mathcal{B}_i$ für $i \in [1, 4]$. Dann ist $\mathrm{Col}(A) = C$.
Ferner ist damit $\mathrm{rk}\ A = \mathrm{rk}\ A^{\mathrm{tr}} = 4$, also

$$\dim\ \mathrm{Col}(H^{\mathrm{tr}}) = \dim\ \mathrm{Sol}(A^{\mathrm{tr}}, 0) = \dim\ \mathrm{Ker}(\varphi_{A^{\mathrm{tr}}}) = 5 - \mathrm{rk}\varphi_{A^{\mathrm{tr}}} = 5 - \mathrm{rk}\ A = 1$$

Wenn also der Spaltenraum von H^{tr} dim 1 hat, so hat der Zeilenraum von H ebenfalls dim 1. Die minimale Anzahl an Zeilen um dies zu erreichen ist 1.

Folglich gibt es ein $H \in K^{1 \times 5} = \mathbb{F}_2^{1 \times 5}$ sodass $\mathrm{Sol}(H, 0) = C$.

c)

Wir gehen nach dem Algorithmus 3.74 vor und berechnen zuerst $\mathrm{Sol}(A^{\mathrm{tr}}, 0)$:

$$\left(\begin{array}{ccccc|c} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right) \xrightarrow{\mathrm{III + I,\ IV + I}} \left(\begin{array}{ccccc|c} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right) \xrightarrow{\mathrm{I + III}} \left(\begin{array}{ccccc|c} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right)$$

$$\xrightarrow{\mathrm{I + IV,\ III + IV}} \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right) \xrightarrow{\mathrm{I + II,\ III + II,\ IV + II}} \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right)$$

Es folgt $\mathrm{Sol}(A^{\mathrm{tr}}, 0) = \langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \rangle$. Offensichtlich ist dann auch $(\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix})$ eine Basis von $\mathrm{Sol}(A^{\mathrm{tr}}, 0)$.

Nach dem Algorithmus ist nun $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$ die gesuchte Matrix H mit $\mathrm{Sol}(H, 0) = C$.

d) Für $c \in K^{5\times 1} = \mathbb{F}_2^{5\times 1}$ gilt also $Hc = 0 \iff c \in C$. Da durch H nur einfach alle Einträge ausummiert werden, lässt sich sagen, dass für $c \in C$ stets $\sum_{i=1}^{5} c_i = 0$ gilt. Da wir über $\mathbb{F}_2$ rechnen, ist dies analog dazu, dass c eine gerade Anzahl an 1 besitzt.

e) Nach 4.30 haben wir $d(C) = 2$, also $\frac{d(C)}{2} = 1$. Wir können also alle 1-Fachen Fehler erkennen, da dann das Produkt $Hc' = 1$ für ein fehlerhaftes Codewort c' ist. Jedoch können wir weniger als $\frac{d(C)}{2} = 1$, also gar keine Fehler korrigieren. Beispielsweise ist

$$d(\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}) = d(\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}) = 1$$

Es gibt also keinen eindeutigen nächsten Nachbarn in C für $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$.