

## Lösung 14

### Aufgabe 53.

- (1) Die Länge ist  $N = 8$ , die Dimension ist  $k = 4$ . Die Zeilenstufenform der Erzeugermatrix ist

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1+\iota & \iota & -1 \\ 0 & 1 & -\iota & 0 & 0 & 1+\iota & \iota & 1 \\ 0 & 0 & 0 & 1 & 0 & \iota & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1+\iota & 1-\iota & 1 \end{pmatrix} \in \mathbf{F}_9^{4 \times 8}.$$

Somit ist eine Kontrollmatrix gegeben durch

$$\begin{pmatrix} \boxed{0} & \boxed{-1-\iota} & \boxed{-\iota} & \boxed{1} \\ \boxed{\iota} & \boxed{-1-\iota} & \boxed{-\iota} & \boxed{-1} \\ 1 & 0 & 0 & 0 \\ \boxed{0} & \boxed{-\iota} & \boxed{0} & \boxed{-1} \\ \boxed{0} & \boxed{1-\iota} & \boxed{-1+\iota} & \boxed{-1} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathbf{F}_9^{8 \times 4}.$$

Keine zwei Zeilen dieser Kontrollmatrix bilden ein linear abhängiges Tupel. Also ist  $d \geq 3$ . Zufällig erkennen wir, daß die dritte Zeile der Zeilenstufenform der Erzeugermatrix zeigt, daß auch  $d \leq 3$ . Also  $d = 3$ . (Hätten wir dies nicht zufällig gesehen, so hätten wir Tupel aus drei Zeilen aus unserer Prüfmatrix auf lineare Abhängigkeit untersucht, und hätten z.B. feststellen können, daß die vierte, sechste und achte Zeile ein linear abhängiges Tupel bilden.)

- (2) Die Hammingsschranke ergibt sich zu

$$\begin{aligned} N - \log_q(V_q(N, \lfloor \frac{d-1}{2} \rfloor)) &= 8 - \log_9(V_9(8, 1)) \\ &= 8 - \log_9\left(\binom{8}{0}(9-1)^0 + \binom{8}{1}(9-1)^1\right) \\ &= 8 - \log_9(65) \\ &\approx 6.1002. \end{aligned}$$

Die Gilbert-Varshamov-Schranke ergibt sich zu

$$\begin{aligned} N - \log_q(V_q(N, d-1)) &= 8 - \log_9(V_9(8, 2)) \\ &= 8 - \log_9\left(\binom{8}{0}(9-1)^0 + \binom{8}{1}(9-1)^1 + \binom{8}{2}(9-1)^2\right) \\ &= 8 - \log_9(1857) \\ &\approx 4.5744. \end{aligned}$$

Es ist  $k \leq K_9(8, 3)$ , und letzterer Wert liegt zwischen den beiden Schranken. Also können wir schließen (und verifizieren), daß  $k = 4$  unter der Hammingsschranke liegt. Jedoch liegt  $k$  nicht über der Gilbert-Varshamov-Schranke. Letztere garantiert nur die *Existenz eines* linearen Codes mit gegebenen Parametern  $N$  und  $d$  und einer Dimension über der Gilbert-Varshamov-Schranke – damit ist noch lange nicht gesagt, daß dies für unseren speziellen Code auch gilt.

### Aufgabe 54.

- (1) Wir erstellen Erzeugermatrizen in den folgenden Fällen.

$\mathcal{R}(0, 0)$ . Als Erzeugermatrix ergibt sich  $(1)$ .

$\mathcal{R}(0, 1) = (\mathcal{R}(0, 0)|\mathcal{R}(-1, 0))$ . Als Erzeugermatrix ergibt sich  $(1|1)$ .

$\mathcal{R}(1, 1)$ . Als Erzeugermatrix ergibt sich  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ .

$\mathcal{R}(0, 2) = (\mathcal{R}(0, 1)|\mathcal{R}(-1, 1))$ . Als Erzeugermatrix ergibt sich  $(1|1|1)$ .

$\mathcal{R}(1, 2) = (\mathcal{R}(1, 1)|\mathcal{R}(0, 1))$ . Als Erzeugermatrix ergibt sich  $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ .

$\mathcal{R}(2, 2)$ . Als Erzeugermatrix ergibt sich  $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ .

$\mathcal{R}(0, 3) = (\mathcal{R}(0, 2)|\mathcal{R}(-1, 2))$ . Als Erzeugermatrix ergibt sich

$$(1 \ 1 \ 1 \ 1 | 1 \ 1 \ 1) .$$

$\mathcal{R}(1, 3) = (\mathcal{R}(1, 2)|\mathcal{R}(0, 2))$ . Als Erzeugermatrix ergibt sich

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} .$$

$\mathcal{R}(2, 3) = (\mathcal{R}(2, 2)|\mathcal{R}(1, 2))$ . Als Erzeugermatrix ergibt sich

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} .$$

$\mathcal{R}(3, 3)$ . Als Erzeugermatrix ergibt sich

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} .$$

- (2) Bis auf Äquivalenz zueinander dual sind allgemein gesprochen  $\mathcal{R}(r, m)$  und  $\mathcal{R}(m - r - 1, m)$ . Bei uns heißt das folgendes.

$\mathcal{R}(0, 1)$  ist bis auf Äquivalenz selbstdual. Eine direkte Inspektion zeigt, daß  $\mathcal{R}(0, 1)$  in der Tat selbstdual ist.

$\mathcal{R}(0, 2)$  ist bis auf Äquivalenz dual zu  $\mathcal{R}(1, 2)$ . Eine direkte Inspektion zeigt, daß  $\mathcal{R}(0, 2)$  in der Tat dual zu  $\mathcal{R}(1, 2)$  ist.

$\mathcal{R}(0, 3)$  ist bis auf Äquivalenz dual zu  $\mathcal{R}(2, 3)$ . Eine direkte Inspektion zeigt, daß  $\mathcal{R}(0, 3)$  in der Tat dual zu  $\mathcal{R}(2, 3)$  ist.

$\mathcal{R}(1, 3)$  ist bis auf Äquivalenz selbstdual. Eine direkte Inspektion zeigt, daß  $\mathcal{R}(1, 3)$  in der Tat selbstdual ist.

- (3) Wir vergleichen die Dimension und deren Schranken in den folgenden Fällen.

$\mathcal{R}(1, 2)$ . Der Minimalabstand ist  $d = 2^{2-1} = 2$ . Die Länge ist  $N = 2^2 = 4$ . Die Dimension ergibt sich (aus der Formel oder aus obigem) zu  $k = 3$ . Die Hammingsschranke ist

$$4 - \log_2(V_2(4, 0)) = 4 - \log_2(1) = 4 ,$$

welche von  $k$  unterschritten wird. Die Gilbert-Varshamov-Schranke ist

$$4 - \log_2(V_2(4, 1)) = 4 - \log_2(1 + 4) \approx 1.6781 ,$$

welche von  $k$  überschritten wird (d.h. der Code ist noch recht gut).

$\mathcal{R}(1, 3)$ . Der Minimalabstand ist  $d = 2^{3-1} = 4$ . Die Länge ist  $N = 2^3 = 8$ . Die Dimension ergibt sich zu  $k = 4$ . Die Hammingsschranke ist

$$8 - \log_2(V_2(8, 1)) = 8 - \log_2(1 + 8) \approx 4.8301 ,$$

welche von  $k$  unterschritten wird. Die Gilbert-Varshamov-Schranke ist

$$8 - \log_2(V_2(8, 3)) = 8 - \log_2(1 + 8 + 28 + 56) \approx 1.4608 ,$$

welche von  $k$  überschritten wird (d.h. der Code ist noch recht gut).

$\mathcal{R}(2, 3)$ . Der Minimalabstand ist  $d = 2^{3-2} = 2$ . Die Länge ist  $N = 2^3 = 8$ . Die Dimension ergibt sich zu  $k = 7$ . Die Hamming-Schranke ist

$$8 - \log_2(V_2(8, 0)) = 8 - \log_2(1) = 8,$$

welche von  $k$  unterschritten wird. Die Gilbert-Varshamov-Schranke ist

$$8 - \log_2(V_2(8, 1)) = 8 - \log_2(1 + 8) \approx 4.8301,$$

welche von  $k$  überschritten wird (d.h. der Code ist noch recht gut).

### Aufgabe 55.

- (1) Die Aussage ist richtig. Es ist  $d((C|C')) = 2d(C)$ . Sei  $(u, u+v)$  ein Element in  $(C|C') \setminus \{0\}$  mit  $u \in C$  und  $v \in C'$ .

Ist  $v \neq 0$ , so ist

$$w((u, u+v)) = w(u) + w(u+v) \geq w(u) + (w(v) - w(u)) = w(v) \geq d(C') > 2d(C),$$

da ja  $w(v) = w(u + (u+v)) \leq w(u) + w(u+v)$ . Somit ist diesenfalls  $(u, u+v)$  nicht von minimalem Gewicht in  $(C|C')$ .

Ist  $v = 0$ , so ist  $w(u, u) = 2w(u)$ , so daß  $(u, u)$  genau dann von minimalem Gewicht in  $(C|C')$  ist, wenn  $u$  von minimalem Gewicht in  $C$  ist.

Somit gibt es genausoviele Wörter minimalen Gewichts in  $(C|C')$  wie in  $C$ . Formal: wir haben eine Bijektion  $M(C) \longrightarrow M((C|C'))$ ,  $u \longmapsto (u, u)$ .

- (2) Die Aussage ist richtig. Es ist  $d((C|C')) = 2d(C) = d(C')$ . Ist  $v \in M(C')$ , so ist  $(0, v) \in M((C|C'))$ . Ist  $u \in M(C)$ , so ist  $(u, u) \in M((C|C'))$ . Somit gibt es in  $M(C')$  und  $M(C)$  zusammengekommen gleichviele oder weniger Elemente als in  $M((C|C'))$ . Formal: wir haben eine Injektion  $M(C) \sqcup M(C') \longrightarrow M((C|C'))$ , welche  $u \in M(C)$  nach  $(u, u)$  und  $v \in M(C')$  nach  $(0, v)$  schickt.

- (3) Die Aussage ist falsch. Dazu genügt es, nachzuweisen, daß die in (2) verwandte Injektion nicht in allen Fällen surjektiv ist. Seien z.B.  $C = \mathcal{R}(1, 1)$  und  $C' = \mathcal{R}(0, 1)$ . Dann hat  $C$  die Erzeugermatrix  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , und  $C'$  die Erzeugermatrix  $\begin{pmatrix} 1 & 1 \end{pmatrix}$ . Es wird  $\mathcal{R}(1, 2) = (C|C')$ , mit der Erzeugermatrix  $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ .

Der Minimalabstand ist  $2^{2-1} = 2$ .

Sei  $u = (10)$ , sei  $v = (11)$ . Es ist  $(u, u+v) = (1001)$  von minimalem Gewicht 2, und somit wird  $(u, u+v) \in M((C|C'))$ . Aber es ist weder  $u = 0$  noch  $v = 0$ . Also liegt  $(u, u+v)$  nicht im Bild der Abbildung aus (2).