UE Einführung in die Algebra und Diskrete Mathematik

13. Übungszettel, 25. Juni 2013

1. Sei C ein linearer binärer Code mit Kontrollmatrix

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

   (a) Wieviele Codewörter enthält C insgesamt? Geben Sie eine Basis an, die alle Codewörter aufspannt. Was ist die Informationsrate von C?

   (b) Wie viele Fehler können erkannt werden? Wie viele Fehler können korrigiert werden? Was ist die Korrekturrate von C?

   (c) Es wurden 10100001 und 10110101 empfangen. Rekonstruieren Sie die gesendeten Codewörter.
   Hinweis: Für die Rekonstruktion eines Codewörters vergleichen Sie es mit jenen Codewörtern, die lediglich eine 1 *aufweisen, jeweils multipliziert mit der Kontrollmatrix. Welche Annahme treffen wir dabei?*

Lösung: ad a) Es handelt sich um einen linearen $(8,4)$-Code und somit enthält C genau 16 Codewörter. Wir benötigen eine Basis des Nullraums von H. Dazu formen wir H auf Zeilenstufenform um,

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

und bekommen als Basis $B = (10100001, 10010010, 00110100, 11111000)$. Die Informationrate ist $\frac{4}{8} = \frac{1}{2}$.

ad b) Da keine der Spalten ident sind und die 6. plus die 7. die 8. Spalte ergibt, ist $rg(H) = 2$ und somit die Minimaldistanz $d_{min}(C) = 3$. Es können also 2 Fehler erkannt werden und 1 Fehler korrigiert werden. Die Korrekturrate ist $\frac{3}{8}$.

ad c) Da $H.(1,0,1,0,0,0,0,1)^t = (0,0,0,0)^t$, ist das Codewort richtig übertragen wordern. Da $H.(1,0,1,1,0,1,0,1)^t = (1,1,1,0)^t$, ist das Codewort nicht richtig übertragen wordern. Um Heruaszufinden an welcher Stelle der Fehler passiert ist, betrachten wir $H.x$ wobei x das Wort ist mit genau einer 1. Also

$$\begin{aligned} H.(1,0,0,0,0,0,0,0)^t &= (1,0,1,1)^t \\ H.(0,1,0,0,0,0,0,0)^t &= (0,1,1,0)^t \\ H.(0,0,1,0,0,0,0,0)^t &= (1,1,1,0)^t \\ H.(0,0,0,1,0,0,0,0)^t &= (0,0,0,1)^t \\ H.(0,0,0,0,1,0,0,0)^t &= (0,0,1,0)^t \\ H.(0,0,0,0,0,1,0,0)^t &= (1,1,1,1)^t \\ H.(0,0,0,0,0,0,1,0)^t &= (1,0,1,0)^t \\ H.(0,0,0,0,0,0,0,1)^t &= (0,1,0,1)^t \end{aligned}$$

und da 00100000 bei Multiplikation mit H das selbe Ergebnis liefert wie 10110101, ist der Fehler an der dritten Stelle aufgetreten. Das richtige Codewort ist also 10010101.

---

2. Sei C ein linearer binärer Code mit Kontrollmatrix

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

   (a) Berechnen Sie die Hamming-Distanz von drei verschiedenen Paaren von Codewörtern aus C.

   (b) Berechnen Sie die Minimaldistanz von C mittels Hamming-Gewicht.

   (c) berechnen Sie die Minimaldistanz von C mittels $rg(H)$.

Lösung: Die Codewörter sind die Elemente des Nullraums:

$$C = \{000000, 100110, 010101, 001110, 110011, 101000, 011011, 111101\}$$

Wir bezeichnen die Codewörter im Folgenden mit $x_1, \dots, x_8$ entsprechend der Reihenfolge von oben.

ad a) z.b.: $d(x_2, x_4) = d(100110, 001110) = 2$, $d(x_3, x_8) = d(010101, 111101) = 2$ und $d(x_6, x_7) = d(101000, 011011) = 4$ ad b) Wir berechnen zuerst die Hamming-Gewichte der Codewörter $x_2, \dots, x_8$. $w_2 = d(x_2, 000000) = 3$, $w_3 = 3$, $w_4 = 3$, $w_5 = 4$, $w_6 = 2$, $w_7 = 4$ und $w_8 = 5$. Die Minimaldistanz von C ist somit $d_{min}(C) = 2$.

ad c) Gesucht ist $rg(H)$ also das größte r sodass je r Spalten linear unabhängig sind. Da die erste und die dritte Spalte ident sind, ist $rg(H) = 1$ und somit $d_{min}(C) = 2$

---

3. Geben Sie die Kontrollmatrix des binären $(15, 11)$-Hamming-Codes an. Korrigieren Sie gegebenfalls folgende Codewörter und geben Sie die eigentlichen Nachrichten an:

   (a) 001010001000101

   (b) 111010101011111

(c) 101110001010000

Lösung: Die Kontrollmatrix des $(15, 11)$ Hamming-Codes ist eine 4×15 Matrix:

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

Die i-te Spalte ergibt sich aus der dyadischen Darstellung von i, z.B. ist der 10. Spaltenvektor wegen $10 = 1 * 2^3 + 0 * 2^2 + 1 * 2^1 + 0 * 2^0$ gegeben durch $(1, 0, 1, 0)^t$. Wir multiplizieren nun die Codewörter mit der Kontrollmatrix um diese auf eventuelle Übertragungsfehler zu überprüfen und korrigieren sie gegebenenfalls.

ad a) Da $H.(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)^t = (1, 1, 0, 1)^t$, ist an der Stelle $1*2^3+1*2^2+0*2^1+1*2^0 = 13$ ein Fehler passiert und das Codewort sollte 001010001000001 lauten. Die Nachricht ist 00101000100.

ad b) Da $H.(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)^t = (0, 0, 0, 0)^t$, ist das Codewort korrekt übertragen worden. Die Nachricht ist 11101010101.

ad c) Da $H.(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)^t = (0, 0, 0, 1)^t$, ist an der Stelle $0*2^3+0*2^2+0*2^1+1*2^0 = 1$ ein Fehler passiert und das Codewort sollte 001110001010000 lauten. Die Nachricht ist 00111000101.

---

4. Geben Sie die Kontrollmatrix des BCH-Codes mit $q = 2$, $c = 1$, $n = 7$ und $d = 5$ an.

Lösung: Da $m = \text{ord}(q) = \text{ord}(2) = 3$ in $\mathbb{Z}_7$ ist, benötigen wir ein primitives Element e in $GF(8)$. Wir wählen das irreduzible und maximalperiodische Polynom $f = x^3 + x + 1$ und nehmen als primitves Element $e = a = [x]_f$. Die Kontrollmatrix H ist nun gegeben durch

$$H = \begin{pmatrix} 1 & e & e^2 & e^3 & e^4 & e^5 & e^6 \\ 1 & e^2 & e^4 & e^6 & e^8 & e^{10} & e^{12} \\ 1 & e^3 & e^6 & e^9 & e^{12} & e^{15} & e^{18} \\ 1 & e^4 & e^8 & e^{12} & e^{16} & e^{20} & e^{24} \end{pmatrix}.$$

Da man jene Zeilen streichen kann die eine q-te Potenz einer anderen ist, ergibt sich also

$$H = \begin{pmatrix} 1 & e & e^2 & e^3 & e^4 & e^5 & e^6 \\ 1 & e^3 & e^6 & e^9 & e^{12} & e^{15} & e^{18} \end{pmatrix}.$$

Mit unsere Wahl von f und $e = a$ erhalten wir folgende Kontrollmatrix (die Log-Tabelle haben wir auf Ü-Zettel 11 ausgearbeitet)

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