Formale Grundlagen: Übung 6

Alexander Waldenmaier, Tutorin: Constanze Merkt

20. Dezember 2020

Aufgabe 6.1

a) Nein, da $00110 \oplus 11010 = 11101 \notin C$.

b) $d(01101, 11010) = 1 + 0 + 1 + 1 + 1 = 4$.

c) Bestimmung des Hammingabstands der empfangenen Nachrichten zu allen Codewörtern $x \in C$:

$x \in C$	$d(01010, x)$	$d(10100, x)$
00110	4	2
11010	**1**	2
10001	4	2
01101	3	3

Die erste empfangene Nachricht entspricht am ehesten dem zweiten Codewort: 11010. Die zweite Nachricht hat hingegen zu den ersten drei Codewörtern den selben Hammingabstand, nämlich 2. Somit kann die zweite Nachricht nicht eindeutig zugeordnet werden.

d) Bestimmung des Minimalabstands des Codes C:

$d(x, y)$	00110	11010	10001	01101
00110	-	3	4	3
11010	-	-	3	3
10001	-	-	-	3
01101	-	-	-	-

Der Minimalabstand beträgt $d(C) = 3$. Somit ist C $\lfloor (d(C)-1)/2 \rfloor = \lfloor (3-1)/2 \rfloor = 1$-fehlerkorrigierend.

e) C ist nicht 1-systematisch, da z.B. die erste Stelle sowohl beim ersten als auch zweiten Codewort den Wert 1 annimmt.

C ist nicht 2-systematisch, da z.B. die letzten zwei Stellen vom ersten und zweiten Codewort den Wert 10 haben.

C ist 3-systematisch, da für keine Stellen i_1, i_2, i_3 ein Vektor $u = (u_1, u_2, u_3)$ gefunden werden kann, der an den entsprechenden i-ten Stellen in zwei Codewörtern $c_1, c_2 \in C$ vorkommt.

Aufgabe 6.2

a) Über das Paritätsbit c'_{n+1} in C' lässt sich sagen:

$$c'_{n+1} = \begin{cases} 0 & \text{gerade Anzahl an 1-Bits} \\ 1 & \text{ungerade Anzahl an 1-Bits} \end{cases}$$

Seien x, y zwei Codewörter $\in C'$. Da C ein linearer Code ist, ist $x \oplus y$ unter Betrachtung der ersten n Stellen ebenfalls $\in C'$. Zu prüfen ist, ob das allerdings auch der Fall ist, wenn das Paritätsbit mit betrachtet wird.

Keine Ahnung wie das geht ...

b) Ein 2-perfekter Code ist gleichzeitig ein 2-korrigierender Code. Somit lässt sich für den Minimalabstand von C' folgern:

$$\begin{aligned} &\lfloor (d(C') - 1)/2 \rfloor = 2 \\ \Rightarrow\ &d(C') \in \{5, 6\} \end{aligned}$$

Aufgabe 6.3

a) Ein [13,12,7]-Code ist ein $k = 12$-systematischer Code mit Wortlänge $n = 13$ und Minimalabstand $d = 7$. Damit folgt, dass der Code $\lfloor (7-1)/2 \rfloor = 3$-fehlerkorrigierend ist. Außerdem gilt $|C| = 2^1 2$, wie aus der Vorlesung bekannt. Damit der Code perfekt ist, muss gelten:

$$\begin{aligned} |C| &\overset{!}{=} 2^{13} / \left(\binom{13}{0} + \binom{13}{1} + \binom{13}{2} + \binom{13}{3} \right) \\ 2^1 2 &\overset{!}{=} 2^{13} / (1 + 13 + 78 + 286) \\ 1 &\overset{!}{=} 2^1 / 378 \\ 1 &\neq 1/189 \end{aligned}$$

Der Code ist also nicht perfekt.

b)

$$\begin{aligned} |C| &\leq 2^5 / \left(\binom{5}{0} + \binom{5}{1} + \binom{5}{2} \right) \\ &\leq 32/(1 + 5 + 10) \\ &\leq 32/16 \\ &\leq 2 \end{aligned}$$

Ein Beispiel für einen solchen Code ist der Wiederholungscode mit Länge 5: 00000, 11111.

c) ??

Aufgabe 6.4

a) Wenn C k-fehlerkorrigierend ist, dann bedeuet das, dass k Bits abweichend sein dürfen und dabei noch immer die richtige Nachricht dekodiert werden kann. Wir jedes nun in C' m mal wiederholt, so sind pro Bit $\lfloor (m-1)/2 \rfloor$ viele Fehler pro „Ursprungsbit“ erlaubt. Damit ergibt sich: C' ist $k \cdot \lfloor (m-1)/2 \rfloor$-fehlerkorrigierend.

b) C' ist $m \cdot l$-systematisch, wenn C l-systematisch ist.

c) Linearität von C bedeutet, dass $x \oplus y \in C$ für beliebige $x, y \in C$. Anders ausgedrückt: Das Ergebnis der bitweise-XOR-Operation aller Bits eines beliebigen Codeworts mit einem anderen beliebigen Codewort ist ebenfalls eine Codewort in C. Im Falle von C' trifft das immer noch zu, da jedes Codewort in C' genau einem Codewort aus C mit m-fach wiederholten Bits entspricht. Die XOR-Operation von zwei Codewörtern aus C' liefert somit ein neues Codewort, das, wieder eine Entsprechung in C hat. Somit ist C' ebenfalls linear.