Musterlösung zur Aufgabe A1.1

a) Allein durch Abzählen der ISBN–Ziffern erkennt man, dass Antwort 2 richtig ist. Die gewichtete Summe über alle Ziffern ergibt ein Vielfaches von 10:

$$S = \sum_{i=1}^{13} z_i \cdot 3^{(i+1) \bmod 2} =$$
$$= (9+8+8+7+7+6+8) \cdot 1 + (7+3+2+3+0+4) \cdot 3 = 110$$
$$\Rightarrow \quad S \bmod 10 = 0.$$

b) Die Antwort ist Nein. Mit einer einzigen Prüfziffer lässt sich nur eine Auslöschung rekonstruieren.

c) Eine Ziffer kann rekonstruiert werden ⇒ Ja. Für die Ziffer z_8 muss gelten:

$$[(9+8+4+3+0+1+2) \cdot 1 + (7+3+5+z_8+7+5) \cdot 3] \bmod 10 = 0$$
$$\Rightarrow \quad [108 + 3z_8] \bmod 10 = 0 \quad \Rightarrow \quad z_8 = 4.$$

d) Durch die Modulo–11–Operation kann z_{10} die Werte 0, 1, ... , 10 annehmen ⇒ $M = 11$. Da „10” keine Ziffer ist, behilft man sich mit z_{10} = „X”. Dies entspricht der römischen Darstellung der Zahl „10”.

e) Die Prüfbedingung lautet:

$$S = \left(\sum_{i=1}^{10} i \cdot z_i \right) \bmod 11 = 0.$$

Die gegebene ISBN erfüllt diese Bedingung:

$$3 \cdot 1 + 8 \cdot 2 + 2 \cdot 3 + 7 \cdot 4 + 3 \cdot 5 + 7 \cdot 6 + 0 \cdot 7 + 6 \cdot 8 + 4 \cdot 9 + 7 \cdot 10 = 264$$
$$\Rightarrow \quad S = 264 \bmod 11 = 0.$$

Richtig ist die Aussage 2, da sich die Prüfsumme $S = 0$ auch bei mehr als einem Fehler ergeben könnte.

Musterlösung zur Aufgabe A1.2

a) Der Codeumfang ist hier zu $|C| = 4$ gegeben. Allgemein gilt $|C| = 2^k$. Daraus folgt $\underline{k = 2}$.

b) Jedes Codewort $\underline{x}$ ist eineindeutig einem Informationsblock $\underline{u}$ zugeordnet. Durch Verfälschungen einzelner der insgesamt n Bit eines Codewortes $\underline{x}$ ergeben sich die Empfangsworte $\underline{y}$. Aus der Anzahl ($16 = 2^4$) der möglichen Empfangsworte folgt $\underline{n = 4}$.

c) Die Coderate ist per Definition $R = k/n$. Mit den obigen Ergebnissen erhält man $\underline{R = 1/2}$.

d) Richtig ist Ja. Ein systematischer Code zeichnet sich dadurch aus, dass jeweils die ersten k Bit der Codeworte identisch sind mit dem Informationsblock.

e) Das Hamming–Gewicht eines binären Codes ist gleich der algebraischen Summe $x_1 + x_2 + \ ... \ + x_n$ über alle Codewortelemente. Damit gilt:

$$w_{\rm H}(\underline{x}_0) \underline{= 0}, \quad w_{\rm H}(\underline{x}_1) \underline{= 2}, \quad w_{\rm H}(\underline{x}_2) \underline{= 2}, \quad w_{\rm H}(\underline{x}_3) \underline{= 4}.$$

f) Die Hamming–Distanz zwischen zwei Codeworten kann hier nur die Werte 2 und 4 annehmen:

$$d_{\rm H}(\underline{x}_0, \underline{x}_1) \underline{= 2}, \quad d_{\rm H}(\underline{x}_0, \underline{x}_2) = 2, \quad d_{\rm H}(\underline{x}_0, \underline{x}_3) \underline{= 4},$$
$$d_{\rm H}(\underline{x}_1, \underline{x}_2) \underline{= 4}, \quad d_{\rm H}(\underline{x}_1, \underline{x}_3) = 2, \quad d_{\rm H}(\underline{x}_2, \underline{x}_3) = 2.$$

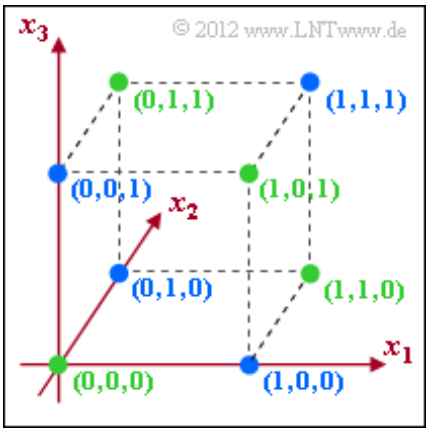
g) Aus dem Ergebnis der Teilaufgabe f) folgt $d_{\rm min}(C) \underline{= 2}$. Allgemein gilt für diese Größe:

$$d_{\rm min}(\mathcal{C}) = \min_{\substack{\underline{x}, \underline{x}' \in \mathcal{C} \\ \underline{x} \neq \underline{x}'}} d_{\rm H}(\underline{x}, \underline{x}').$$

Musterlösung zur Zusatzaufgabe Z1.2

a) Richtig sind die Aussagen 1 und 3: $k = 3$ Informationsbits werden bei dieser Belegung auf $n = 3$ Codebits abgebildet ⇒ $R = k/n = 1$. Die Aussage $\underline{x} = \underline{u}$ würde nur bei systematischer Codierung gelten. Prinzipiell möglich wäre zum Beispiel auch (0, 0, 0) → (0, 1, 1). Die letzte Aussage ist mit Sicherheit falsch: Aus der Grafik erkennt man die Minimaldistanz $d_{min} = 1$.

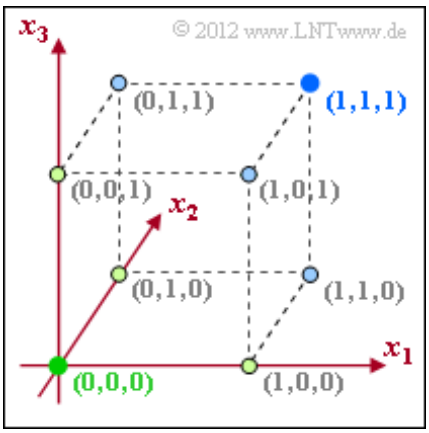
b) C_1 und C_2 beschreiben tatsächlich Codes mit der Rate $R = 2/3$ und der Minimaldistanz $d_{min} = 2$ ⇒ Antwort 1 und 2.



In nebenstehender Grafik markieren die grünen Punkte den Code C_1 und die blauen Punkte den Code C_2. Beim angegebenen Code C_3 – ebenfalls mit Rate $R = 2/3$ – ist die minimale Distanz zwischen zwei Codeworten $d_{min} = 1$, zum Beispiel zwischen (0, 0, 0) und (1, 0, 0) oder auch zwischen (0, 1, 1) und (1, 1, 1).

c) Mit der Minimaldistanz $d_{min} = 2$ kann lediglich ein Bitfehler erkannt werden. In der oberen Grafik kennzeichnen die grünen Punkte zulässige Codeworte von C_1. Wird ein blauer Punkt empfangen, so weist dies auf einen Übertragungsfehler hin. Eine Fehlerkorrektur ist mit $d_{min} = 2$ dagegen nicht möglich ⇒ Antwort 1. *Hinweis:* Der Code C_1 entspricht dem **Single Parity–check Code** (3, 2, 2).

d) C_4 beschreibt den **(3, 1, 3)–Wiederholungscode.** Bei diesem Code sind zwar zwei der insgesamt acht möglichen Punkte belegt, woraus man fälschlicherweise auf die Coderate $R = 1/4$ schließen könnte. Die Coderate berechnet sich aber gemäß $R = k/n = 1/3$.



Aus der unteren Grafik erkennt man, dass wegen $d_{min} = 3$ nun auch ein Bitfehler korrigiert werden kann. Bei der Decodierung werden alle hellgrünen Punkte (mit schwarzer Umrahmung) in den grünen Punkt (0, 0, 0) überführt und alle hellblauen in den blauen Punkt (1, 1, 1). Gleichzeitig können bis zu zwei Bitfehler erkannt werden (einer natürlich auch) ⇒ Richtig sind die Antworten 2, 3 und 4.

Musterlösung zur Aufgabe A1.3

a) Richtig ist die Antwort 1. Das BSC–Modell basiert auf einer einzigen Entscheiderschwelle. Wegen der Eigenschaft *Symmetric* liegt diese bei $G = 0$.

b) Die Wahrscheinlickeit, dass eine Gaußsche Zufallsgröße mit Streuung σ größer ist als 1 oder kleiner ist als –1, ergibt sich gemäß der Angabe zu $\varepsilon = Q(1/\sigma)$. Mit $\sigma = 0.4$ folgt daraus $\varepsilon = Q(2.5) = 0.62\ \%$.

c) Richtig ist hier die Antwort 2. Beim BSEC–Modell gibt es drei Entscheidungsgebiete: je eines für die Symbole 0 und 1 und ein weiteres für *Erasure* (E: keine Entscheidung möglich). Dazu benötigt man zwei Schwellen, die symmetrisch um 0 liegen müssen. Wenn dem nicht so wäre, ergäben sich unterschiedliche Ergebnisse für die Symbole 0 und 1.

d) Es gelte $y_A = \tilde{x} + n$. Eine falsche Entscheidung ergibt sich in diesem Fall für den Rauschterm

- $n > +1.2$, falls $\tilde{x} = -1 \Rightarrow x = 1$,
- $n < -1.2$, falls $\tilde{x} = +1 \Rightarrow x = 0$.

In beiden Fällen erhält man für die Verfälschungswahrscheinlichkeit $\varepsilon = Q(1.2/0.4) = Q(3) = 0.14\ \%$.

Ein *Erasure* (keine Entscheidung) ergibt sich für $-0.2 < y_A < +0.2$. Ausgehend von $\tilde{x} = -1$ gilt somit:

$$\lambda = \Pr(0.8 < n < 1.2) = \Pr(n > 0.8) - \Pr(n > 1.2) =$$
$$= Q(2) - Q(3) \approx 2.28\,\% - 0.14\,\% \approx 2.14\,\%.$$

e) Hier ist ebenfalls die Antwort 2 richtig. Auch beim BEC–Modell gibt es zwei um 0 symmetrische Schwellen. Der Unterschied zum BSEC–Modell ist, dass sich die Verfälschungswahrscheinlichkeit $\varepsilon = 0$ (genauer gesagt: $\varepsilon < 0.5 \cdot 10^{-4}$) ergibt, entweder, weil

- der Sicherheitsbereich ($\pm G$) größer gewählt ist als beim BSEC–Modell, oder
- das AWGN–Rauschen eine kleinere Streuung σ aufweist.

f) In diesem Fall ist die Verfälschungswahrscheinlichkeit vernachlässigbar:

$$\varepsilon = Q(1.6/0.4) = Q(4) \approx 0.32 \cdot 10^{-4} \approx 0.$$

Das heißt: Man kann hier tatsächlich vom BEC–Modell ausgehen. Für die *Erasure*–Wahrscheinlichkeit gilt dabei:

$$\lambda = \Pr(0.4 < n < 1.6) = \Pr(n > 0.4) - \Pr(n > 1.6) =$$
$$= Q(1) - Q(4) \approx Q(1) = 15.87\,\%.$$

Musterlösung zur Aufgabe A1.4

a) Die Hamming–Distanzen zwischen dem spezifischen Empfangswort $\underline{y}$ = (1, 0, 0, 0, 1) und den vier möglichen Codeworten $\underline{x}_i$ ergeben sich wie folgt:

$$d_{\rm H}(\underline{y}, \underline{x}_0) = 2\,, \quad d_{\rm H}(\underline{y}, \underline{x}_1) = 4\,, \quad d_{\rm H}(\underline{y}, \underline{x}_2) = 1\,, \quad d_{\rm H}(\underline{y}, \underline{x}_3) = 3\,.$$

Entschieden wird sich für die Folge mit der geringsten Hamming–Distanz ⇒ Antwort 3.

b) Für $\underline{y}$ = (0, 0, 0, 1, 0) sind Antwort 1 und Antwort 2 richtig, wie die folgende Rechnung zeigt:

$$d_{\rm H}(\underline{y}, \underline{x}_0) = 1\,, \quad d_{\rm H}(\underline{y}, \underline{x}_1) = 1\,, \quad d_{\rm H}(\underline{y}, \underline{x}_2) = 4\,, \quad d_{\rm H}(\underline{y}, \underline{x}_3) = 4\,.$$

c) Entsprechend der Hamming–Distanz wäre eine Entscheidung zugunsten von $\underline{x}_2$ genau so möglich wie für $\underline{x}_3$, wenn der Vektor $\underline{y}$ = (1, 0, 1, 1, 1) empfangen wird:

$$d_{\rm H}(\underline{y}, \underline{x}_0) = 4\,, \quad d_{\rm H}(\underline{y}, \underline{x}_1) = 4\,, \quad d_{\rm H}(\underline{y}, \underline{x}_2) = 1\,, \quad d_{\rm H}(\underline{y}, \underline{x}_3) = 1\,.$$

Der Empfangsvektor $\underline{y}$ unterscheidet sich von $\underline{x}_2$ bezüglich des vierten Bits und von $\underline{x}_3$ im zweiten Bit. Da das vierte Bit unsicherer ist als das zweite, wird er sich für $\underline{x}_2$ entscheiden ⇒ Antwort 3.

d) Da es sich hier um einen systematischen Code handelt, ist die Entscheidung für $\underline{z}$ = (1, 0, 1, 0, 1) gleichbedeutend mit der Entscheidung $v_1 = 1$, $v_2 = 0$. Es ist nicht sicher, dass $\underline{u}$ = (1, 0) tatsächlich gesendet wurde, aber die Wahrscheinlichkeit ist angesichts des Empfangsvektors $\underline{y}$ = (1, 0, 1, 1, 1) hierfür am größten.

Musterlösung zur Aufgabe A1.5

a) Das Prüfbit p wird beim *Single Parity–check Code* so bestimmt, dass die Summe aller Einsen im Codewort $\underline{x} = (u_1, u_2, \ldots, u_4, p)$ geradzahlig ist. Beispielsweise erhält man:

$$\begin{aligned}
\underline{u}_0 &= (0,0,0,0) \;\Rightarrow\; \underline{x}_0 = (0,0,0,0,0) \;\Rightarrow\; p \underline{= 0},\\
\underline{u}_4 &= (0,1,0,0) \;\Rightarrow\; \underline{x}_4 = (0,1,0,0,1) \;\Rightarrow\; p \underline{= 1},\\
\underline{u}_{13} &= (1,1,0,1) \;\Rightarrow\; \underline{x}_{13} = (1,1,0,1,1) \;\Rightarrow\; p \underline{= 1}.
\end{aligned}$$

b) Aufgrund der Tatsache, dass die Anzahl der Einsen geradzahlig sein muss, ist das ausgelöschte Prüfbit $p = 0$. Gesendet wurde also $\underline{u}_0 \Rightarrow$ Antwort 1.

c) Nach gleichen Überlegungen wie in der letzten Teilaufgabe kommt man für $\underline{y} = (0, \text{E}, 0, 0, 1)$ zum Ergebnis $\underline{x} = \underline{x}_4 = (0, 1, 0, 0, 1) \Rightarrow \underline{u}_4 = (0, 1, 0, 0) \Rightarrow$ Antwort 2.

d) Das Ereignis „$\underline{y} = \underline{x}$" tritt nur dann auf, wenn durch den BEC–Kanal keines der $n = 5$ Codebits ausgelöscht wird:

$$\Pr(\underline{y} = \underline{x}) = (1-\lambda)^5 = 0.9^5 \underline{= 0.591}.$$

e) Das Ereignis „$v = u$" tritt dann auf, wenn alle Codebits richtig übertragen werden $\Rightarrow \Pr(\underline{v} = \underline{x})$, aber auch dann, wenn nur ein Codebit ausgelöscht wird. Entsprechend der Binominalverteilung gibt es hierfür 5 Möglichkeiten:

$$\begin{aligned}
\Pr(\underline{v} = \underline{u}) &= \Pr(\underline{y} = \underline{x}) + 5 \cdot (1-\lambda)^4 \cdot \lambda =\\
&= 0.591 + 5 \cdot 0.656^4 \cdot 0.1 \underline{= 0.919}.
\end{aligned}$$

f) Aufgrund des BEC–Modells ist die Verfälschung eines Codewortes $\underline{x}$ per se ausgeschlossen, da keines der Bit von 0 → 1 bzw. von 1 → 0 verfälscht werden kann. Vielmehr gilt:

$$\Pr(\underline{v} = \underline{u}) + \Pr(\underline{v} = \underline{\text{E}}) = 1 \quad \Rightarrow \quad \Pr(\underline{v} = \underline{\text{E}}) = 1 - \Pr(\underline{v} = \underline{u}) \underline{= 0.081}.$$

Musterlösung zur Zusatzaufgabe Z1.5

a) Der Codeumfang gibt die Anzahl der möglichen Codeworte an. Es gilt $|C| = 2^k$, so dass es beim hier betrachteten *Single Parity–check Code* 16 Codeworte gibt ($k = 4$) und beim Wiederholungscode nur zwei Codeworte ($k = 1$).

b) Bei jedem *Single Parity–check Code* ist die Anzahl der Einsen geradzahlig ⇒ Antwort 1 und 3.

c) Bei einem jeden Wiederholungscode gibt es (unabhängig von n) nur zwei Codeworte, die beide hier angegeben sind ⇒ Antwort 1 und 4.

d) Aufgrund von Bitfehlern kann es für den Empfangsvektor $\underline{y}$ stets $N = 2^n = 32$ unterschiedliche Bitkombinationen geben, die alle in die ML–Entscheidung einbezogen werden müssen. Dies gilt sowohl für den SPC (5, 4) als auch für den RC (5, 1).

e) Beim SPC (5, 4) beträgt die Hamming–Distanz zwischen zwei beliebigen Codeworten mindestens $d_{\rm min} = 2$. Dagegen sind beim RC (5, 1) alle Bit der beiden Codeworte unterschiedlich ⇒ $d_{\rm min} = 5$.

f) Eine Fehlererkennung ist möglich, so lange nicht mehr als $e = d_{\rm min} - 1$ Bitfehler in einem Codewort auftreten. Mit dem Ergebnis aus e) erhält man $e = 1$ (SPC) bzw. $e = 4$ (RC).

g) Allgemein gilt für die Anzahl der korrigierbaren Fehler:

$$t = \left\lfloor \frac{d_{\rm min} - 1}{2} \right\rfloor .$$

Bei jedem *Single Parity–check Code* ist $(d_{\rm min} - 1)/2 = 0.5$ ⇒ $t = 0$. Dagegen können mit dem RC (5, 1) ⇒ $d_{\rm min} = 5$ bis zu $t = 2$ Fehler korrigiert werden.

Musterlösung zur Aufgabe A1.6

a) Die Codetabelle hat 16 Einträge: $|C| = 16$. Aus der Gleichung $|C| = 2^k$ folgt damit $k = 4$. Die Länge eines jeden Codewortes ist $n = 7$. Damit ist die Coderate $R = 4/7 = 0.571$.

b) Jedes Codewort $\underline{x}$ beinhaltet zunächst die $k = 4$ Bit des Informationswortes $\underline{u}$. Danach folgen $m = 3$ Prüfbits:

$$\underline{x} = (x_1, x_2, x_3, x_4, x_5, x_5, x_7) = (u_1, u_2, u_3, u_4, p_1, p_2, p_3)\,.$$

Dies entspricht genau der Definition eines **systematischen Codes** ⇒ JA.

c) Bei jedem Hamming–Code beträgt die minimale Distanz $d_{\rm min} = 3$. Aus der Tabelle erkennt man dies daran, dass das minimale **Hamming–Gewicht** (die Anzahl der Einsen in einem Codewort) gleich 3 ist. Ein linearer Code beinhaltet nämlich auch das Nullwort, so dass gilt:

$$d_{\rm min}(\mathcal{C}) = \min_{\substack{\underline{x},\,\underline{x}' \in \mathcal{C} \\ \underline{x} \neq \underline{x}'}} d_{\rm H}(\underline{x},\,\underline{x}') = \min_{\underline{x} \in \mathcal{C}} w_{\rm H}(\underline{x}) = 3\,.$$

d) Die Angabe $d_{\rm min} = 3$ bedeutet, dass $e = 2$ Fehler erkannt und $t = 1$ Fehler korrigiert werden können.

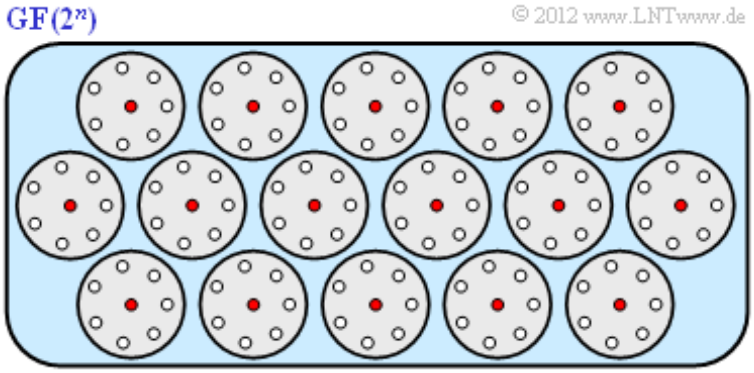
e) Die Bedingung für einen perfekten Code lautet entsprechend der Angabe:

$$2^m = \sum_{f=0}^{t} \binom{n}{f}\,.$$

Beim hier betrachteten (7, 4)–Hamming–Code gilt $n = 7$, $m = 3$ und $t = 1$, so dass sich auf beiden Seiten der Gleichung der Wert 8 ergibt ⇒ JA:

$$2^3 = 8, \quad \sum_{f=0}^{1} \binom{7}{f} = \binom{7}{0} + \binom{7}{1} = 1 + 7 = 8\,.$$

f) Richtig sind nur die beiden letzten Aussagen. Gäbe es einen Kanalcode, der für alle Kanäle die Blockfehlerwahrscheinlichkeit bei endlicher Codewortlänge n zu Null macht, so wäre dieser nicht nur perfekt, sondern ein Wunder. Aufgrund des Kanalcodierungstheorems ist aber Pr(Blockfehler) = 0 bei endlichem n gar nicht möglich.



Veranschaulichen wir uns die Aussage 2 durch die obige Grafik. Der hochdimensionale Raum ist hierbei stark vereinfacht (in 2D) dargestellt. Wir gehen dabei von den Zahlenwerten $k = 4$, $n = 7$, $m = 3$, $t = 1$ des (7, 4, 3)–Hamming–Codes aus:

- Für das Empfangswort sind $2^7 = 128$ Punkte im 7–dimensionalen Raum möglich. Die roten

Punkte markieren die $2^4 = 16$ gültigen Codeworte.

- Die Kreise umfassen jeweils 8 Punkte, nämlich ein gültiges Codewort und $n = 7$ Empfangsworte nach nur einem Fehler, die man bei der Decodierung genau diesem Codewort zuordnet.
- Insgesamt gibt es $2^4 = 16$ solcher Kreise. Wegen $128 = 16 \cdot 8$ liegt deshalb kein einziges Empfangswort $\underline{y}$ außerhalb eines solchen Zuordnungskreises.

Auch die letzte Aussage ist zutreffend, was beispielhaft für $d_{\rm min} = 4$ gezeigt werden soll. Hiermit kann ebenfalls nur $t = 1$ Fehler korrigiert werden. Unterscheidet sich ein Empfangswort $\underline{y}$ von zulässigen Codeworten in 2 Bit, so ist dieser Punkt keinem Kreis zuzuordnen. Es liegen dann auch Punkte außerhalb der Kreise und die Bedingung eines perfekten Codes ist nicht mehr erfüllt.

g) Richtig sind die Aussagen 1, 2, 3 und 5. Alle Hamming–Codes haben die minimale Hamming–Distanz $d_{\rm min} = 3 \Rightarrow t = 1$. Gleichzeitig lässt sich jeder (n, k)–Hamming–Code auch als $(2^m - 1, 2^m - 1 - m)$ Code schreiben, wobei $m = n - k$ die Anzahl der Prüfbits angibt. Damit wird die Gleichung eines perfekten Codes stets erfüllt:

$$\sum_{f=0}^{1} \binom{n}{f} = 1 + n = 2^m .$$

Hierbei bedeuten:

$m = 2$: (3, 1)–Hamming–Code, identisch mit dem *Repetition Code* (3, 1),
$m = 3$: (7, 4)–Hamming–Code,
$m = 4$: (15, 11)–Hamming–Code,
$m = 5$: (31, 26)–Hamming–Code,
$m = 6$: (63, 57)–Hamming–Code.

Auch der Wiederholungscode mit $n = 5$ erfüllt die Bedingung. Mit $d_{\rm min} = 5$, $t = 2$ und $m = 4$ erhält man:

$$\sum_{f=0}^{2} \binom{5}{f} = 1 + 5 + 10 = 16 = 2^m .$$

Die anderen Wiederholungscodes (RC) mit ungeradem n sind ebenfalls perfekt, nicht jedoch RC (4, 1), RC (6, 1), usw. Dies wurde bereits in der Musterlösung zur Teilaufgabe f) begründet.

Musterlösung zur Aufgabe A1.7

a) Die Anzahl der Spalten der Prüfmatrix **H** ist gleich der Codelänge $n = 7$. Die Zeilenzahl ist gleich der Anzahl der Prüfgleichungen, im vorliegenden Fall gilt $m = 3 = n - k$.

b) Ein Vergleich mit der Grafik auf der Angabenseite zeigt, dass alle Aussagen zutreffen. Mit

$$\underline{x} = (x_1, x_2, x_3, x_4, x_5, x_6, x_7) = (u_1, u_2, u_3, u_4, p_1, p_2, p_3)$$

ergeben sich folgende Prüfgleichungen:

$$\begin{aligned} x_1 \oplus x_2 \oplus x_4 \oplus x_5 &= 0 \quad \text{(roter Kreis)}, \\ x_2 \oplus x_3 \oplus x_4 \oplus x_6 &= 0 \quad \text{(grüner Kreis)}, \\ x_1 \oplus x_3 \oplus x_4 \oplus x_7 &= 0 \quad \text{(blauer Kreis)}. \end{aligned}$$

Damit erhält man für die Prüfmatrix:

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

Die Angabe von **H** ist nicht eindeutig. Würde man die Reihenfolge der Prüfgleichungen vertauschen, so ergäbe sich beispielsweise eine zweite, ebenfalls richtige Prüfmatrix:

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

c) Richtig ist die Aussage 2. Bei einem systematischen Code lässt sich die Prüfmatrix in folgender Form darstellen:

$$\mathbf{H} = \left(\mathbf{P}^{\rm T}\,;\,\mathbf{I}_m\right).$$

Im vorliegenden Beispiel gilt mit $m = 3$:

$$\mathbf{P}^{\rm T} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \quad \mathbf{I}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

d) Allgemein lautet der Zusammenhang zwischen der $m \times n$–Prüfmatrix und der $k \times n$–Generatormatrix:

$$\mathbf{H} \cdot \mathbf{G}^{\rm T} = \mathbf{0}.$$

Die Matrix **0** ist nur mit Nullen belegt und hat m Zeilen und k Spalten.

Bei einem systematischen Code – wie hier – besteht folgender Zusammenhang:

$$\mathbf{H} = \left(\mathbf{P}^{\rm T}\,;\,\mathbf{I}_m\right) \quad \Leftrightarrow \quad \mathbf{G} = \left(\mathbf{I}_k\,;\,\mathbf{P}\right).$$

Im vorliegenden Fall erhält man:

$$\mathbf{I}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{P} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \Rightarrow \quad \mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Richtig sind demnach die Aussagen 1 und 3.

e) Die anzuwendende Gleichung lautet:

$$\underline{x}_{11} = \underline{u}_{11} \cdot \mathbf{G} =$$

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

Ein Vergleich mit der Tabelle von **Aufgabe A1.6** zeigt die Richtigkeit dieser Berechnung ⇒ Antwort 3. Die Antwort 1 kann schon deshalb nicht richtig sein, weil das keiner systematischen Codierung entspricht. Und schließlich: (1, 0, 1, 1, 0, 0, 0) gemäß Vorschlag 2 ist kein gültiges Codewort. Hiermit wird die in der Grafik auf der Angabenseite blau markierte Prüfgleichung nicht erfüllt.

Musterlösung zur Aufgabe Z1.7

a) Richtig sind die Aussagen 1 und 2. Deshalb gibt es auch „4 über 2" = 6 Codeworte. Die letzte Aussage ist falsch. Ist zum Beispiel das erste Bit eine „0", so gibt es ein Codewort mit dem Beginn „00" und zwei Codeworte, die mit „01" beginnen.

b) Richtig sind hier die Aussagen 1 bis 4. Alle Codes, die durch eine Generatormatrix **G** und/oder eine Prüfmatrix **H** beschrieben werden können, sind linear. Dagegen erfüllt Code 5 keine der für lineare Codes erforderlichen Bedingungen. Beispielsweise

- fehlt das Nullwort,
- ist der Codeumfang $|C|$ keine Zweierpotenz,
- ergibt $(0, 1, 0, 1) \oplus (1, 0, 1, 0) = (1, 1, 1, 1)$ kein gültiges Codewort.

c) Bei einem systematischen Code müssen stets die ersten k Bit eines jeden Codewortes $\underline{x}$ gleich dem Codewort $\underline{u}$ sein. Dies wird erreicht, wenn der Beginn der Generatormatrix **G** eine Einheitsmatrix $\mathbf{I}_k$ darstellt. Dies trifft für Code 1 (mit Dimension $k = 3$), Code 2 (mit $k = 1$) und Code 3 (mit $k = 2$) zu ⇒ die Aussagen 1 bis 3 sind richtig. Die Generatormatrix von Code 2 ist allerdings nicht explizit angegeben. Sie lautet:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}.$$

d) Von dualen Codes spricht man, wenn die Prüfmatrix **H** des einen Codes gleich der Generatormatrix **G** des anderen Codes ist. Dies trifft zum Beispiel für Code 1 und Code 2 zu. Für den SPC (4, 3) gilt:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}, \quad \mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

und für den Wiederholungscode RC (4, 1):

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}, \quad \mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Das heißt: Die Aussage 1 trifft zu. Aussage 2 ist mit Sicherheit falsch, schon aus Dimensionsgründen: Die Generatormatrix **G** von Code 3 ist eine 2×4–Matrix und die Prüfmatrix **H** von Code 2 eine 3×4–Matrix.

Code 3 und Code 4 erfüllen ebenfalls nicht die Bedingungen dualer Codes. Die Prüfgleichungen von

$$\text{Code 3} = \{(0,0,0,0),\ (0,1,1,0),\ (1,0,0,1),\ (1,1,1,1)\}$$

lauten:

$$x_1 \oplus x_4 = 0,\ \ x_2 \oplus x_3 = 0 \quad \Rightarrow \quad \mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Dagegen ist die Generatormatrix von Code 4 wie folgt gegeben:

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

Musterlösung zur Aufgabe A1.8

a) Der vorgegebene Code C wird durch folgende Kenngrößen charakterisiert:

- Bitanzahl der Codeworte: $\underline{n = 6}$,
- Bitanzahl der Informationsworte: $\underline{k = 3}$,
- Anzahl der Codeworte (Codeumfang): $|C| = 2^k \Rightarrow \underline{|C| = 8}$,
- Coderate: $R = k/n = 3/6 \Rightarrow \underline{R = 1/2}$,
- Anzahl der Prüfbitgleichungen: $\underline{m = n - k = 3}$,
- minimale Hamming–Distanz (siehe Tabelle): $\underline{d_{\rm min} = 3}$.

b) Nach der Singleton–Schranke gilt $d_{\rm min} \le n - k + 1$. Mit $n = 6$ und $k = 3$ erhält man hierfür $d_{\rm min} \le 4$.

Es kann also durchaus ein (6, 3)–Blockcode mit größerer Minimaldistanz konstruiert werden $\Rightarrow$ JA. Wie ein solcher Code aussieht, wurde freundlicherweise nicht gefragt.

Die Minimaldistanz aller Hamming–Codes ist $d_{\rm min} = 3$, und nur der Sonderfall mit $n = 3$ und $k = 1$ erreicht den Grenzwert. Dagegen erreichen das Maximum entsprechend der Singleton–Schranke:

- alle **Wiederholungscodes** (*Repetition Codes*, RC) wegen $k = 1$ und $d_{\rm min} = n$; hierzu gehört auch der (3, 1)–Hamming–Code, der ja bekannterweise identisch ist mit RC (3, 1),
- alle **Single Parity–check Codes** (SPC): $k = n - 1$, $d_{\rm min} = 2$.

c) Vertauscht man Zeilen in der Generatormatrix $\mathbf{G}$, so kommt man zu einem identischen Code C'. Das heißt: Die Codes C und C' beinhalten die genau gleichen Codeworte. Beispielsweise erhält man nach zyklischem Zeilentausch 2 → 1, 3 → 2 und 1 → 3 die neue Matrix

$$\mathbf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Die erste und die letzte Zeile der neuen Matrix entsprechen schon den Vorgaben eines systematischen Codes, nämlich, dass deren Generatormatrix $\mathbf{G}_{\rm sys}$ mit einer Diagonalmatrix beginnen muss. Ersetzt man die Zeile 2 durch die Modulo–2–Summe von Zeile 2 und 3, so erhält man:

$$\mathbf{G}_{\rm sys} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Auch dieser systematische Code beinhaltet genau die gleichen Codeworte wie die Codes C und C'.

Richtig sind die Lösungsvorschläge 2 und 3.

d) Wendet man die Gleichung $\underline{x}_{\rm sys} = \underline{u} \cdot \mathbf{G}_{\rm sys}$ auf die obigen Beispiele an, so erkennt man, dass die beiden ersten Aussagen richtig sind, nicht aber die letzte.

Ohne Rechnung kommt man zum gleichen Ergebnis, wenn man berücksichtigt, dass

- das systematische Codewort $\underline{x}_{\rm sys}$ mit $\underline{u}$ beginnen muss,

- der Code $C_{\rm sys}$ die gleichen Codeworte beinhaltet wie der vorgegebene Code C.

Für $\underline{u}$ = (0, 1, 0) lautet somit das Codewort (0, 1, 0, ?, ?, ?). Ein Vergleich mit der Codetabelle von C auf der Angabenseite führt zum Ergebnis $\underline{x}_{\rm sys}$ = (0, 1, 0, 1, 0, 1).

e) Bei systematischer Codierung besteht folgender Zusammenhang zwischen Generator– und Prüfmatrix:

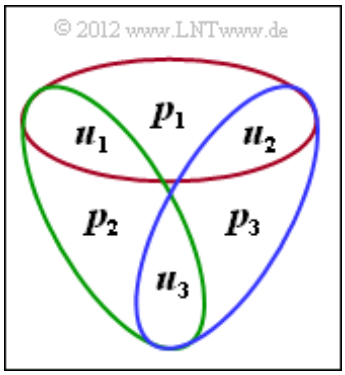
$$\mathbf{G} = (\mathbf{I}_k\,;\,\mathbf{P}) \quad \Leftrightarrow \quad \mathbf{H} = \left(\mathbf{P}^{\rm T}\,;\,\mathbf{I}_m\right)\,.$$

Angewendet auf das aktuelle Beispiel erhält man so:

$$\mathbf{G}_{\rm sys} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad \Rightarrow \quad \mathbf{H}_{\rm sys} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0\\ 1 & 0 & 1 & 0 & 1 & 0\\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}\,.$$

Daraus ergeben sich Prüfgleichungen (siehe Grafik):

$$u_1 \oplus u_2 \oplus p_1 = 0 \quad \Rightarrow \quad p_1 = u_1 \oplus u_2\,,$$
$$u_1 \oplus u_3 \oplus p_2 = 0 \quad \Rightarrow \quad p_2 = u_1 \oplus u_3\,,$$
$$u_2 \oplus u_3 \oplus p_3 = 0 \quad \Rightarrow \quad p_3 = u_2 \oplus u_3\,.$$



⇒ Richtig ist nur die Aussage 1. Die Angaben für p_2 und p_3 sind dagegen genau vertauscht.

Musterlösung zur Zusatzaufgabe Z1.8

a) Für einen systematischen (6, 3)–Blockcode muss gelten

$$\underline{x} = (x_1, x_2, x_3, x_4, x_5, x_6) = (u_1, u_2, u_3, p_1, p_2, p_3).$$

Diese Bedingung erfüllen die Codes A, C und D ⇒ Antwort 1, 2, 4.

b) Nur Code A und Code B sind identische Codes ⇒ Antwort 1. Sie beinhalten genau die gleichen Codeworte und unterscheiden sich nur durch andere Zuordnungen $\underline{u} \rightarrow \underline{x}$. Wie in der Musterlösung zur **Aufgabe A1.8c** angegeben, gelangt man von der Generatormatrix $\mathbf{G}_B$ zur Generatormatrix $\mathbf{G}_A$ allein durch Vertauschen/Permutieren von Zeilen oder durch Ersetzen einer Zeile durch die Linearkombination zwischen dieser Zeile und einer anderen.

c) Code A und Code B sind mehr als äquivalent, nämlich identisch. Code C und D unterscheiden sich zum Beispiel auch durch die minimale Hamming–Distanz $d_{min} = 3$ bzw. $d_{min} = 2$ und sind somit auch nicht äquivalent.

Richtig ist somit allein Antwort 2. Code B und Code C haben gleiche Eigenschaften, beispielsweise gilt für beide $d_{min} = 3$. Sie beinhalten aber andere Codeworte.

d) Richtig ist Antwort 3:

- Die letzte Spalte von $\mathbf{G}_B$ ergibt die erste Spalte von $\mathbf{G}_C$.
- Die erste Spalte von $\mathbf{G}_B$ ergibt die zweite Spalte von $\mathbf{G}_C$.
- Die zweite Spalte von $\mathbf{G}_B$ ergibt die dritte Spalte von $\mathbf{G}_C$, usw.

e) Die Bedingung $\mathbf{H} \cdot \mathbf{G}^T = \mathbf{0}$ gilt für alle linearen Codes ⇒ Alle Aussagen treffen zu.

Musterlösung zur Aufgabe A1.9

a) Die entsprechende Gleichung für die Coderate lautet in beiden Fällen $R = k/n$:

- $C_1 : n = 7, k = 4 \Rightarrow R = 4/7 \underline{= 0.571}$,
- $C_2 : n = 8, k = 4 \Rightarrow R = 4/8 \underline{= 0.5}$.

b) Die minimale Distanz des (7, 4, 3)–Hamming–Codes C_1 beträgt $d_{\rm min} \underline{= 3}$, was allein schon aus der Namensgebung ablesbar ist. Aus der Tabelle auf der Angabenseite ist ersichtlich, dass für den erweiterten Hamming–Code $d_{\rm min} \underline{= 4}$ gilt. C_2 bezeichnet man deshalb in der Literatur auch als einen (8, 4, 4)–Blockcode.

c) Die Prüfmatrix **H** besteht im Allgemeinen aus n Spalten und $m = n - k$ Zeilen, wobei m die Anzahl der Prüfgleichungen angibt. Beim (7, 4, 3)–Hamming–Code ist **H** eine 3 × 7–Matrix. Für den erweiterten Hamming–Code ⇒ Code C_2 gilt demgegenüber $\underline{n = 8}$ (Spaltenzahl) und $\underline{m = 4}$ (Zeilenzahl).

d) Aus der Codetabelle auf der Angabenseite erkennt man, dass allein Antwort 3 richtig ist. Das Prüfbit p_4 ist so zu bestimmen, dass die Modulo–2–Summe über alle Bits des Codewortes den Wert 0 ergibt.

e) Anzumerken ist zunächst, dass die Angabe der Prüfmatrix nie eindeutig ist, schon allein deshalb, weil die Reihenfolge der Prüfgleichungen vertauschbar ist. Unter Berücksichtigung des Hinweises, dass nur eine der vorgegebenen Zeilen falsch ist, ist $\mathbf{H}_2$ allerdings eindeutig bestimmt:

$$\mathbf{H}_2 = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Richtig sind also die Aussagen 1, 2 und 4. Die Zeilen dieser Prüfmatrix stehen in dieser Reihenfolge für die vier Prüfgleichungen:

$$x_1 \oplus x_2 \oplus x_4 \oplus x_5 = 0, \quad x_2 \oplus x_3 \oplus x_4 \oplus x_6 = 0,$$
$$x_1 \oplus x_3 \oplus x_4 \oplus x_7 = 0, \quad x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 = 0.$$

f) Richtig ist Antwort 2: Zu diesem Ergebnis kommt man, wenn man die letzte Zeile durch die Modulo–2–Summe über alle vier Zeilen ersetzt, was erlaubt ist. Der Vorschlag 1 stellt keine Prüfgleichung dar. Der Vorschlag 3 steht für die Prüfgleichung $x_3 \oplus x_5 = 0$, was auch nicht den Gegebenheiten entspricht.

Entsprechend dem richtigen Lösungsvorschlag 2 wird dagegen die Prüfgleichung

$$x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 = 0$$

durch folgende neue Prüfgleichung ersetzt:

$$x_1 \oplus x_2 \oplus x_3 \oplus x_8 = 0.$$

Die modifizierte Prüfmatrix lautet nun:

$$\mathbf{H}_2 = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

g) Nach dieser Matrixmanipulation liegt $\mathbf{H}_2$ in der für systematische Codes typischen Form vor:

$$\mathbf{H}_2 = \left(\mathbf{P}^{\rm T}\,;\,\mathbf{I}_m\right) \quad \Rightarrow \quad m = 4\text{:}\;\; \mathbf{H}_2 = \left(\mathbf{P}^{\rm T}\,;\,\mathbf{I}_4\right) .$$

Damit lautet die Generatormatrix:

$$\mathbf{G_2} = \left(\mathbf{I}_4\,;\,\mathbf{P}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} .$$

Richtig sind also die Aussagen 2 und 3. $\mathbf{G}_2$ beginnt wie $\mathbf{G}_1$ (siehe Angabenblatt) mit einer Diagonalmatrix $\mathbf{I}_4$, hat aber im Gegensatz zu $\mathbf{G}_1$ nun 8 Spalten. Im vorliegenden Fall $n = 8$, $k = 4$ ⇒ $m = 4$ sind sowohl $\mathbf{G}_2$ als auch $\mathbf{H}_2$ jeweils 4×8–Matrizen.

Musterlösung zur Zusatzaufgabe Z1.9

a) Die Rate des (5, 2)–Codes ist $R = 2/5 = 0.4$. Aus dem angegebenen Code erkennt man weiterhin die minimale Distanz $d_{\rm min} = 3$.

b) Bei Erweiterung vom (5, 2)–Code zum (6, 2)–Code wird ein weiteres Prüfbit hinzugefügt. Das Codewort hat somit die Form

$$\underline{x} = (x_1, x_2, x_3, x_4, x_5, x_6) = (u_1, u_2, p_1, p_2, p_3, p_4).$$

Für das hinzugekommene Prüfbit muss dabei gelten:

$$p_4 = x_6 = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 .$$

Das heißt: Das neue Prüfbit p_4 wird so gewählt, dass sich in jedem Codewort eine gerade Anzahl von Einsen ergibt $\Rightarrow$ Antwort 2. Löst man diese Aufgabe mit der Prüfmatrix, so erhält man

$$\mathbf{H}_{(6,2)} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \Rightarrow \quad \mathbf{H}_{(6,2)\,\rm sys} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\Rightarrow \quad \mathbf{G}_{(6,2)\,\rm sys} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Die beiden Zeilen der Generatormatrix **G** ergeben zwei der vier Codeworte, die Modulo–2–Summe das dritte und schließlich ist auch noch das Nullwort zu berücksichtigen.

c) Nach Erweiterung vom (5, 2)–Code auf den (6, 2)–Code

- vermindert sich die Rate von $R = 2/5$ auf $R = 2/6 = 0.333$,
- erhöht sich die Minimaldistanz von $d_{\rm min} = 3$ auf $d_{\rm min} = 4$.

Allgemein gilt: Erweitert man einen Code, so nimmt die Rate ab und die Minimaldistanz erhöht sich um 1, falls $d_{\rm min}$ vorher ungerade war.

d) Bei gleicher Vorgehensweise wie unter c) erhält man

$$\mathbf{H}_{(7,2)} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \Rightarrow \quad \mathbf{H}_{(7,2)\,\rm sys} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\Rightarrow \quad \mathbf{G}_{(6,2)\,\rm sys} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

$\Rightarrow$ Beide Antworten sind richtig.

e) Die Rate beträgt nun $R = 2/7 = 0.266$. Die Minimaldistanz ist weiterhin $d_{\rm min} = 4$, wie man aus den Codeworten des (7, 2)–Codes ablesen kann:

$$\mathcal{C} = \{(0,0,0,0,0,0,0),\ (0,1,0,1,1,1,0),\ (1,0,1,1,0,1,0),\ (1,1,1,0,1,0,0)\}.$$

Allgemein gilt: Ist die Minimaldistanz eines Codes geradzahlig, so kann diese durch Erweiterung nicht

vergrößert werden.

f) Richtig sind die Aussagen 1 und 2. Durch Streichen der letzten Zeile und der letzten Spalte erhält man für die Prüfmatrix bzw. die Generatormatrix (jeweils in systematischer Form):

$$\mathbf{H}_{(4,2)} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad \mathbf{G}_{(4,2)} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} .$$

Aus der Generatormatrix ergeben sich die genannten Codeworte (1, 0, 1, 1), (0, 1, 0, 1), (1, 1, 1, 0) als Zeilensumme sowie das Nullwort (0, 0, 0, 0). Die Minimaldistanz dieses Codes ist $d_{\rm min} = 2$ und damit kleiner als die minimale Distanz $d_{\rm min} = 3$ des (5, 2)–Codes.

Allgemein gilt: Durch Punktierung wird $d_{\rm min}$ um 1 kleiner (wenn sie vorher gerade war) oder sie bleibt gleich. Dies kann man sich verdeutlichen, wenn man durch eine weitere Punktierung (des Prüfbits p_2) den (3, 2)–Blockcode generiert. Dieser Code

$$\mathcal{C} = \{(0, 0, 0),\ (0, 1, 1),\ (1, 0, 1),\ (1, 1, 0)\}$$

besitzt die gleiche Minimaldistanz $d_{\rm min} = 2$ wie der (4, 2)–Code.

Musterlösung zur Aufgabe A1.10

a) Die Codewortlänge ist $n = 6$ ⇒ der (5, 2)–Code kommt nicht in Frage. Bei einem (6, 2)–Code gibt es $2^2 = 4$ verschiedene Codeworte und beim (6, 3)–Code entsprechend $2^3 = 8$. Durch die Angabe von zwei Codeworten lässt sich weder der (6, 2)– noch der (6, 3)–Code ausschließen ⇒ Antwort 2 und 3.

b) Da es sich um einen linearen Code handelt, muss die Modulo–2–Summe

$$(0, 1, 0, 1, 0, 1) \oplus (1, 0, 0, 1, 1, 0) = (1, 1, 0, 0, 1, 1)$$

ebenfalls ein gültiges Codewort sein. Ebenso das Nullwort:

$$(0, 1, 0, 1, 0, 1) \oplus (0, 1, 0, 1, 0, 1) = (0, 0, 0, 0, 0, 0)\,.$$

Richtig ist somit Antwort 2.

c) Richtig sind hier die Aussagen 1 bis 3. Basisvektoren der Generatormatrix **G** sind beispielsweise die beiden gegebenen Codeworte, woraus sich auch die Prüfmatrix **H** bestimmen lässt:

$$\mathbf{G}_{(6,2)} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad \mathbf{H}_{(6,2)} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Allgemein wird durch die k Basisvektoren der Generatormatrix **G** ein k–dimensionaler Untervektorraum aufgespannt und durch die $m \times n$–Matrix **H** (mit $m = n - k$) ein hierzu orthogonaler Untervektorraum der Dimension m.

Anmerkung: Der hier angegebene

$$\mathcal{C}_{(6,2)} = \{(0, 0, 0, 0, 0, 0),\ (0, 1, 0, 1, 0, 1), (1, 0, 0, 1, 1, 0),\ (1, 1, 0, 0, 1, 1)\}$$

ist nicht sonderlich effektiv, da $p_1 = x_3$ stets 0 ist. Durch Punktierung kommt man zum Code

$$\mathcal{C}_{(5,2)} = \{(0, 0, 0, 0, 0),\ (0, 1, 1, 0, 1), (1, 0, 1, 1, 0),\ (1, 1, 0, 1, 1)\}$$

mit gleicher Minimaldistanz $d_{\rm min} = 3$, aber größerer Coderate $R = 2/5$ gegenüber $R = 1/3$.

d) Die drei Zeilen $\underline{g}_1$, $\underline{g}_2$ und $\underline{g}_3$ der Matrix $\mathbf{G}_{\rm A}$ sind als Basisvektoren geeignet, da sie linear unabhängig sind, das heißt, es gilt

$$\underline{g}_1 \oplus \underline{g}_2 \neq \underline{g}_3,$$
$$\underline{g}_1 \oplus \underline{g}_3 \neq \underline{g}_2,$$
$$\underline{g}_2 \oplus \underline{g}_3 \neq \underline{g}_1.$$

Syndrom $\underline{s}_\mu$	Nebenklassenanführer $\underline{e}_\mu$
$\underline{s}_0 = (0, 0, 0)$	$\underline{e}_0 = (0, 0, 0, 0, 0, 0, 0)$
$\underline{s}_1 = (0, 0, 1)$	$\underline{e}_1 = (0, 0, 0, 0, 0, 0, 1)$
$\underline{s}_2 = (0, 1, 0)$	$\underline{e}_2 = (0, 0, 0, 0, 0, 1, 0)$
$\underline{s}_3 = (0, 1, 1)$	$\underline{e}_3 = (0, 0, 1, 0, 0, 0, 0)$
$\underline{s}_4 = (1, 0, 0)$	$\underline{e}_4 = (0, 0, 0, 0, 1, 0, 0)$
$\underline{s}_5 = (1, 0, 1)$	$\underline{e}_5 = (1, 0, 0, 0, 0, 0, 0)$
$\underline{s}_6 = (1, 1, 0)$	$\underline{e}_6 = (0, 1, 0, 0, 0, 0, 0)$
$\underline{s}_7 = (1, 1, 1)$	$\underline{e}_7 = (0, 0, 0, 1, 0, 0, 0)$

Gleiches gilt für Matrix $\mathbf{G}_{\rm B}$. Die Basisvektoren sind hier so gewählt, dass der Code auch systematisch ist.

Für die letzte Generatormatrix gilt: $\underline{g}_1 \oplus \underline{g}_2 = \underline{g}_3$ ⇒ der Rang der Matrix (2) ist kleiner als deren Ordnung (3). Hier führt nicht nur $\underline{u} = (0, 0, 0)$ zum Codewort (0, 0, 0, 0, 0, 0), sondern auch $\underline{u} = (1, 1, 1)$. Richtig sind die Lösungsvorschläge 1 und 2.

Musterlösung zur Aufgabe A1.11

a) Es gibt insgesamt $2^7 = 128$ verschiedene Codeworte $\underline{x}$ und entsprechend dem BSC–Modell auch 2^7 unterschiedliche Empfangsworte $\underline{y}$ und ebenso viele Fehlervektoren $\underline{e}$.

Mit $m = 3$ Prüfbits gibt es $2^3 = 8$ unterschiedliche Werte für das Syndrom,

$$\underline{s} \in \{\underline{s}_0, \underline{s}_1, \ldots, \underline{s}_7\} = \{\underline{s}_\mu\}, \quad \mu = 0, \ldots, 7,$$

und ebenso viele Nebenklassen. Da beim Hamming–Code, der ja perfekt ist, alle Fehlervektoren zu einer der 8 Nebenklassen Ψ_μ gehören und zudem die Anzahl aller Vektoren in allen Nebenklassen gleich ist („Warum sollte es anders sein?" Genügt Ihnen das als Beweis?), erhält man

$$N_0 = \frac{2^n}{2^m} = 2^k \underline{= 16}.$$

Zur Nebenklasse Ψ_0 gehören beispielsweise – siehe Musterlösung zur **Aufgabe Z1.11** – die Vektoren

- $\underline{e} = (1, 1, 0, 0, 0, 0, 1)$,
- $\underline{e} = (1, 1, 1, 1, 1, 1, 1)$.

b) Entsprechend den Kommentaren des letzten Teilergebnisses gilt gleichermaßen $N_7 \underline{= 16}$.

c) Richtig ist Antwort 3: Der Nebenklassenanführer $\underline{e}_\mu$ ist derjenige Fehlervektor $\underline{e}$ mit dem geringsten **Hamming–Gewicht** $w_{\rm H}(\underline{e})$, der zum Syndrom $\underline{s}_\mu$ führt. Der hier betrachtete Hamming–Code (7, 4, 3) ist perfekt. Das heißt: Alle 8 Nebenklassenanführer beinhalten deshalb

- keine „Eins" ($\underline{e}_0 \Rightarrow$ es ist keinerlei Korrektur erforderlich), oder
- genau eine einzige „Eins" ($\underline{e}_1$, ... , $\underline{e}_7 \Rightarrow$ es muss ein Informations– oder Prüfbit korrigiert werden).

d) Es gilt $\underline{s} = \underline{e} \cdot \mathbf{H}^{\rm T}$:

$$\underline{s} = \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0\end{pmatrix} \cdot \begin{pmatrix}1 & 0 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 1\end{pmatrix} = \underline{s}_5 \quad \Rightarrow \quad \underline{\mu = 5}.$$

e) Ein Vergleich mit der Lösung zur letzten Teilaufgabe zeigt, dass $(0, 1, 0, 0, 0, 0, 0) \cdot \mathbf{H}^{\rm T}$ als Syndrom die zweite Zeile der transponierten Matrix ergibt:

$$\begin{pmatrix}0 & 1 & 0 & 0 & 0 & \ldots\end{pmatrix} \cdot \mathbf{H}^{\rm T} = \begin{pmatrix}1 & 1 & 0\end{pmatrix} = \underline{s}_6$$

$$\Rightarrow \quad \underline{\mu = 6}, \quad \underline{e}_6 = \begin{pmatrix}0 & 1 & 0 & 0 & 0 & 0 & 0\end{pmatrix}.$$

In gleicher Weise erhält man:

$$\begin{pmatrix}0 & 0 & 1 & 0 & 0 & \ldots\end{pmatrix} \cdot \mathbf{H}^{\rm T} = \begin{pmatrix}0 & 1 & 1\end{pmatrix} = \underline{s}_3$$

$$\Rightarrow \quad \underline{\mu = 3}, \quad \underline{e}_3 = \begin{pmatrix}0 & 0 & 1 & 0 & 0 & 0 & 0\end{pmatrix}.$$

Syndrom $\underline{s}_\mu$	Nebenklassenanführer $\underline{e}_\mu$
$\underline{s}_0 = (0, 0, 0)$	$\underline{e}_0 = (0, 0, 0, 0, 0, 0, 0)$
$\underline{s}_1 = (0, 0, 1)$	$\underline{e}_1 = (0, 0, 0, 0, 0, 0, 1)$
$\underline{s}_2 = (0, 1, 0)$	$\underline{e}_2 = (0, 0, 0, 0, 0, 1, 0)$
$\underline{s}_3 = (0, 1, 1)$	$\underline{e}_3 = (0, 0, 1, 0, 0, 0, 0)$
$\underline{s}_4 = (1, 0, 0)$	$\underline{e}_4 = (0, 0, 0, 0, 1, 0, 0)$
$\underline{s}_5 = (1, 0, 1)$	$\underline{e}_5 = (1, 0, 0, 0, 0, 0, 0)$
$\underline{s}_6 = (1, 1, 0)$	$\underline{e}_6 = (0, 1, 0, 0, 0, 0, 0)$
$\underline{s}_7 = (1, 1, 1)$	$\underline{e}_7 = (0, 0, 0, 1, 0, 0, 0)$

$$(0 \quad 0 \quad 0 \quad 1 \quad 0 \ \ldots) \cdot \mathbf{H}^{\rm T} = (1 \quad 1 \quad 1) = \underline{s}_7$$

$$\Rightarrow \quad \underline{\mu = 7}, \quad \underline{e}_7 = (0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0) \ .$$

Die nebenstehende Grafik fasst das Ergebnis der Teilaufgaben (c) und (d) nochmals zusammen.

f) Beim betrachteten (7, 4, 3)–Hamming–Code wird dann für das richtige Informationswort entschieden, wenn bei der Übertragung höchstens ein Bit innerhalb des Codewortes verfälscht wird. Daraus folgt:

$$\begin{aligned}\text{Pr(Blockfehler)} &= \text{Pr(zwei Bitfehler oder mehr)} = \\ &= 1 - \text{Pr(kein Bitfehler)} - \text{Pr(ein Bitfehler)} = \\ &= 1 - 0.9^7 - 7 \cdot 0.1 \cdot 0.9^7 \ \underline{= 0.15}.\end{aligned}$$

Bei uncodierter Übertragung eines Blocks mit $n = k = 4$ Bit ergäbe sich beim gleichen BSC–Kanal:

$$\text{Pr(Blockfehler)} = 1 - 0.9^4 \approx 0.344 .$$

Der Vergleich ist allerdings nicht ganz fair, da mit $n = 4$ eine kleinere Verfälschungswahrscheinlichkeit ε anzusetzen wäre als mit $n = 7$ (kleinere Symbolrate ⇒ kleinere Bandbreite ⇒ kleinere Rauschleistung).

Musterlösung zur Zusatzaufgabe Z1.11

a) Die Antwort ist JA, wie man aus der vorgegebenen Prüfmatrix **H** erkennt. Diese beinhaltet am Ende eine 3×3–Diagonalmatrix. Die Codeworte lauten demzufolge:

$$\underline{x} = (x_1, x_2, x_3, x_4, x_5, x_6, x_7) = (u_1, u_2, u_3, u_4, p_1, p_2, p_3)\,.$$

b) Mit diesem Empfangsvektor $\underline{y}$ werden alle Prüfgleichungen erfüllt:

$$u_1 \oplus u_2 \oplus u_4 \oplus p_1 = 1 \oplus 0 \oplus 1 \oplus 0 = 0,$$
$$u_2 \oplus u_3 \oplus u_4 \oplus p_2 = 0 \oplus 0 \oplus 1 \oplus 1 = 0,$$
$$u_1 \oplus u_3 \oplus u_4 \oplus p_3 = 1 \oplus 0 \oplus 1 \oplus 0 = 0.$$

Richtig ist dementsprechend die Antwort JA.

c) Es gilt $\underline{s} = \underline{y} \cdot \mathbf{H}^{\rm T}$:

$$\underline{s} = \begin{pmatrix}1 & 0 & 0 & 1 & 0 & 1 & 0\end{pmatrix} \cdot \begin{pmatrix}1 & 0 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}0 & 0 & 0\end{pmatrix} = \underline{s}_0 \;\Rightarrow\; \underline{\text{Antwort 1}}\,.$$

d) Man könnte nun für jedes $\underline{y}$ die Gleichung $\underline{y} \cdot \mathbf{H}^{\rm T} = (0, 0, 0)$ überprüfen. Hier soll nun das Ergebnis auf anderem Wege gewonnen werden:

- $\underline{y} = (1, 1, 0, 1, 0, 1, 0)$ unterscheidet sich von $\underline{y} = (1, 0, 0, 1, 0, 1, 0)$ im Bit u_2, das nur in den beiden ersten Prüfgleichungen verwendet wird, nicht jedoch in der letzten $\Rightarrow$ $\underline{s} = \underline{s}_6 = (1, 1, 0)$.
- Wendet man die Prüfgleichungen auf $\underline{y} = (0, 1, 0, 1, 0, 0, 1)$ an, so erhält man $\underline{s} = \underline{s}_0 = (0, 0, 0)$, wie die folgende Rechnung belegt:

  $$u_1 \oplus u_2 \oplus u_4 \oplus p_1 = 0 \oplus 1 \oplus 1 \oplus 0 = 0,$$
  $$u_2 \oplus u_3 \oplus u_4 \oplus p_2 = 1 \oplus 0 \oplus 1 \oplus 0 = 0,$$
  $$u_1 \oplus u_3 \oplus u_4 \oplus p_3 = 0 \oplus 0 \oplus 1 \oplus 1 = 0.$$

- Zum gleichen Ergebnis kommt man mit dem Empfangsvektor $\underline{y} = (0, 1, 1, 0, 1, 0, 1)$, der sich vom Vektor (1, 0, 0, 1, 0, 1, 0) in allen 7 Bitpositionen unterscheidet:

  $$u_1 \oplus u_2 \oplus u_4 \oplus p_1 = 0 \oplus 1 \oplus 0 \oplus 1 = 0,$$
  $$u_2 \oplus u_3 \oplus u_4 \oplus p_2 = 1 \oplus 1 \oplus 0 \oplus 0 = 0,$$
  $$u_1 \oplus u_3 \oplus u_4 \oplus p_3 = 0 \oplus 1 \oplus 0 \oplus 1 = 0.$$

Richtig sind also die Antworten 2 und 3.

Musterlösung zur Aufgabe A1.12

a) Jeder Hamming–Code ist perfekt und weist eine minimale Distanz von $d_{\rm min} = 3$ auf. Deshalb kann ein Bitfehler im Codewort korrigiert werden, während zwei Bitfehler stets zu einer Fehlentscheidung des Codewortes führen ⇒ Parameter $t = 1$. Damit ergibt sich für die Blockfehlerwahrscheinlichkeit:

$$\begin{aligned}\rm Pr(Blockfehler) &= 1 - Pr(kein\ Blockfehler) - Pr(ein\ Blockfehler) = \\ &= 1 - (1-\varepsilon)^7 - 7\cdot\varepsilon\cdot(1-\varepsilon)^6 .\end{aligned}$$

$$\begin{aligned}\varepsilon = 0.01:\ \ \rm Pr(Blockfehler) &= 1 - 0.99^7 - 7\cdot 0.01\cdot 0.99^6 = \\ &= 1 - 0.932065 - 0.065904 \approx \underline{2.03\cdot 10^{-3}},\\ \varepsilon = 0.001:\ \ \rm Pr(Blockfehler) &= 1 - 0.999^7 - 7\cdot 0.001\cdot 0.999^6 = \\ &= 1 - 0.993021 - 0.006958 \approx \underline{2.09\cdot 10^{-5}}.\end{aligned}$$

b) Ein jeder $(n, k, 3)$ Hamming–Code kann nur einen Bitfehler korrigieren. Damit gilt allgemein für den BSC–Kanal mit der Codewortlänge n:

$$\begin{aligned}\rm Pr(Blockfehler) &= 1 - (1-\varepsilon)^n - n\cdot\varepsilon\cdot(1-\varepsilon)^{n-1} = \\ &= 1 - \left[1 - \binom{n}{1}\cdot\varepsilon + \binom{n}{2}\cdot\varepsilon^2 - \ldots\right] - \\ &\quad - \left[n\cdot\varepsilon\cdot\left(1 - \binom{n-1}{1}\cdot\varepsilon + \binom{n-1}{2}\cdot\varepsilon^2 - \ldots\right)\right].\end{aligned}$$

Bei Vernachlässigung aller Terme mit ε^3, ε^4, ... erhält man:

$$\begin{aligned}\rm Pr(Blockfehler) &= n\cdot\varepsilon - \binom{n}{2}\cdot\varepsilon^2 - n\cdot\varepsilon + n\cdot\varepsilon\binom{n-1}{1}\cdot\varepsilon + \ldots = \\ &= -1/2\cdot n\cdot(n-1)\cdot\varepsilon^2 + n\cdot(n-1)\cdot\varepsilon^2 = n\cdot(n-1)/2\cdot\varepsilon^2.\end{aligned}$$

⇒ Richtig ist <u>Lösungsvorschlag 1</u>. Für den (7, 4, 3)–Hamming–Code ergibt sich somit:

$$\rm Pr(Blockfehler) \le \begin{cases} 2.1\cdot 10^{-3} & \text{für } \varepsilon = 10^{-2} \\ 2.1\cdot 10^{-5} & \text{für } \varepsilon = 10^{-3} \end{cases}.$$

Durch Vergleich mit dem Ergebnis der Teilaufgabe (a) erkennt man die Gültigkeit dieser Näherung. Diese ist um so besser, je kleiner die BSC–Verfälschungswahrscheinlichkeit ε ist.

c) Die Ergebnisse der Teilaufgabe b) lassen sich wie folgt zusammenfassen:

$$\rm Pr(Blockfehler) = \begin{cases} 3\cdot\varepsilon^2 & \text{für } n = 3 \\ 21\cdot\varepsilon^2 & \text{für } n = 7 \\ 105\cdot\varepsilon^2 & \text{für } n = 15 \end{cases}.$$

Richtig ist <u>Antwort 1</u>. Die geringste Blockfehlerwahrscheinlichkeit besitzt natürlich der Hamming–Code mit der geringsten Rate $R = 1/3$, also mit der größten relativen Redundanz.

d) Bei *Hard Decision* gilt mit der komplementären Gaußschen Fehlerfunktion $\rm Q(x)$:

$$\varepsilon = \rm Q\left(\sqrt{2\cdot R\cdot E_B/N_0}\right) \quad\Rightarrow\quad E_B/N_0 = \frac{[\rm Q^{-1}(\varepsilon)]^2}{2R}$$

$$\Rightarrow\quad 10\cdot\lg E_B/N_0 = 20\cdot\lg\left[\rm Q^{-1}(\varepsilon)\right] - 10\cdot\lg(2R).$$

Daraus erhält man mit $\varepsilon = 0.01 \Rightarrow Q^{-1}(\varepsilon) = 2.33$:

$$10 \cdot \lg E_{\rm B}/N_0 = 20 \cdot \lg (2.33) - 10 \cdot \lg (8/7) = 7.35\,{\rm dB} - 0.58\,{\rm dB} \approx \underline{6.77\,{\rm dB}}.$$

In analoger Weise ergibt sich für $\varepsilon = 0.001 \Rightarrow Q^{-1}(\varepsilon) \approx 3.09$.

$$10 \cdot \lg E_{\rm B}/N_0 = 20 \cdot \lg (3.09) - 0.58\,{\rm dB} \approx \underline{9.22\,{\rm dB}}.$$

e) Wir beziehen uns auf die Blockfehlerwahrscheinlichkeit 10^{-5}. Nach dem Ergebnis der Teilaufgabe b) darf dann die BSC–Verfälschungswahrscheinlichkeit nicht größer sein als

$$\varepsilon = \sqrt{\frac{10^{-5}}{21}} = 6.9 \cdot 10^{-4} \quad \Rightarrow \quad Q^{-1}(\varepsilon) = 3.2 \quad \Rightarrow \quad 10 \cdot \lg E_{\rm B}/N_0 = 9.52\,{\rm dB}.$$

Mit *Soft Decision* genügen laut Angabe 8 dB $\Rightarrow$ $10 \cdot \lg G_{\rm SD} = \underline{1.52\ {\rm dB}}$.

Musterlösung zur Zusatzaufgabe Z1.12

a) Die Größe der Syndromtabelle ist allgemein $N_{\rm ges} = 2^m$; $m = n - k$ gibt die Anzahl der Prüfbits an.

- Beim (7, 4, 3)–Hamming–Code ist $m = n - k = 3$ $\Rightarrow$ die Länge der Tabelle ist $N_{\rm ges} \underline{= 8}$.
- Die Syndromtabelle des (8, 4, 4)–Codes ist doppelt so groß: $N_{\rm ges} = 2^4 \underline{= 16}$.

b) Allgemein gilt für die Anzahl der Einträge mit Gewicht–2–Fehlermustern: N_2' = „n über 2”. Daraus ergeben sich die Zahlenwerte

- $N_2' \underline{= 21}$ für $n = 7$ $\Rightarrow$ (7, 4, 3)–Code,
- $N_2' \underline{= 28}$ für $n = 8$ $\Rightarrow$ (8, 4, 4)–Code.

c) Beim (7, 4, 3)–Hamming–Code ist die Syndromtabelle gefüllt mit einem Eintrag für den fehlerfreien Fall ($N_0 = 1$) und $n = 7$ Einträge mit Gewicht–1–Fehlermustern ($N_1 = 7$). Damit ist die Anzahl der Einträge mit Gewicht–2–Fehlermustern gleich

$$N_2 = N_{\rm ges} - N_0 - N_1 \underline{= 0}.$$

Dagegen gilt für den erweiterten (8, 4, 4)–Hamming–Code:

$$N_0 = 1, \quad N_1 = 8 \quad \Rightarrow \quad N_2 = N_{\rm ges} - N_0 - N_1 \underline{= 7}.$$

d) Analog zur **Musterlösung** der Aufgabe A1.12 (a) und (b) erhält man hier:

$$\begin{aligned}{\rm Pr(Blockfehler)} &= 1 - (1-\varepsilon)^8 - 8 \cdot \varepsilon \cdot (1-\varepsilon)^7 = \\ &= 1 - 0.922745 - 0.074655 \underline{= 2.69 \cdot 10^{-3}}.\end{aligned}$$

In der Tabelle sind für diesen Fall und für verschiedene BSC–Parameter ε die Ergebnisse in der grün hinterlegten Spalte eingetragen. Gegenüber dem (7, 4, 3)–Code ergibt sich stets eine Verschlechterung.

BSC–Wert ε	(7, 4, 3)-Code	(8, 4, 4)-Code		
	Pr(Blockfehler)	Pr(≥ 2 Fehler)	„Verbesserung“	Pr(Blockfehler)
$3 \cdot 10^{-1}$	$6.71 \cdot 10^{-1}$	$7.45 \cdot 10^{-1}$	$7.41 \cdot 10^{-2}$	$6.71 \cdot 10^{-1}$
10^{-1}	$1.50 \cdot 10^{-1}$	$1.87 \cdot 10^{-1}$	$3.72 \cdot 10^{-2}$	$1.50 \cdot 10^{-1}$
$3 \cdot 10^{-2}$	$1.71 \cdot 10^{-2}$	$2.23 \cdot 10^{-2}$	$5.25 \cdot 10^{-3}$	$1.71 \cdot 10^{-2}$
10^{-2}	$2.03 \cdot 10^{-3}$	$2.69 \cdot 10^{-3}$	$6.59 \cdot 10^{-4}$	$2.03 \cdot 10^{-3}$
$3 \cdot 10^{-3}$	$1.87 \cdot 10^{-4}$	$2.49 \cdot 10^{-4}$	$6.19 \cdot 10^{-5}$	$1.87 \cdot 10^{-4}$
10^{-3}	$2.09 \cdot 10^{-5}$	$2.79 \cdot 10^{-5}$	$6.96 \cdot 10^{-6}$	$2.09 \cdot 10^{-5}$

e) Bei bestmöglicher Korrektur (gefüllte Syndromtabelle) werden auch sieben Gewicht–2–Fehlermuster korrigiert. Damit vermindert sich die Blockfehlerwahrscheinlichkeit um

$${\rm Pr(Gewicht-2-Fehlermuster\ wird\ korrigiert)} = 7 \cdot \varepsilon^2 \cdot (1-\varepsilon)^6.$$

Für $\varepsilon = 0.01$ macht diese „Verbesserung” etwa $0.66 \cdot 10^{-3}$ aus. Die Blockfehlerwahrscheinlichkeit ergibt sich somit zu

$${\rm Pr(Blockfehler)} = 2.69 \cdot 10^{-3} - 0.66 \cdot 10^{-3} \underline{= 2.03 \cdot 10^{-3}}.$$

In der obigen Tabelle ist diese Rechnung für verschiedene BSC–Parameter ε durchgeführt. Man erkennt:

Die Blockfehlerwahrscheinlichkeit des erweiterten (8, 4, 4)–Hamming–Codes (siehe letzte Spalte) stimmt exakt mit der des (7, 4, 3)–Hamming–Codes (Spalte 2) überein. Die Korrektur von 25% der Gewicht–2–Fehlermuster gleicht genau die Tatsache aus, dass beim (8, 4, 4)–Code Fehlermuster mit mehr als einem Fehler (Spalte 3) wahrscheinlicher sind als beim (7, 4, 3)–Code (Spalte 2).

Musterlösung zur Aufgabe A1.13

a) Der Empfangsvektor lautet $\underline{y}$ = (1, E, 0, 1, 0, 0, E). Ausgelöscht wurden also die Codesymbole an den Positionen 2 und 7. Ausgehend von der vorgegebenen Prüfmatrix

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

des Hammingcodes erhält man für Vektor und Matrix hinsichtlich

- aller **korrekt übertragenen Codesymbole** (Index K), die dem Codewortfinder bekannt sind:

$$\underline{z}_{\rm K} = (1, 0, 1, 0, 0)\,, \quad \mathbf{H}_{\rm K} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}\,,$$

- hinsichtlich der beiden **ausgelöschten Codesymbole** z_2 und z_7 (Index E), die zu ermitteln sind:

$$\underline{z}_{\rm E} = (z_2, z_7)\,, \quad \mathbf{H}_{\rm E} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}\,.$$

Die Bestimmungsgleichung lautet somit:

$$\mathbf{H}_{\rm E} \cdot \underline{z}_{\rm E}^{\rm T} = \mathbf{H}_{\rm K} \cdot \underline{z}_{\rm K}^{\rm T}$$

$$\Rightarrow \quad \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} z_2 \\ z_7 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}\,.$$

Daraus ergeben sich drei Gleichungen für die beiden Unbekannten z_2 und z_7:

(a) $z_2 = 1$,

(b) $z_2 = 1$,

(c) $z_2 + z_7 = 0 \Rightarrow z_7 = 1$.

Somit liefert der Codewortfinder $\underline{z}$ = (1, 1, 0, 1, 0, 0, 1) ⇒ Lösungsvorschlag 2.

b) Betrachtet man die vorgegebene Matrix $\mathbf{H}_{\rm K}$, so erkennt man, dass diese mit dem ersten vier Spalten der Prüfmatrix $\mathbf{H}$ übereinstimmt. Die Auslöschungen betreffen also die letzten 3 Bit des Empfangswortes ⇒ $\underline{z}_{\rm E} = (z_5, z_6, z_7)$ ⇒ $\underline{y}$ = (1, 1, 0, 1, E, E, E) und die Erasure–Matrix lautet:

$$\mathbf{H}_{\rm E} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\,.$$

Richtig sind demzufolge die Aussagen 1, 2 und 4.

c) Man erhält nach einigen Matrizenmultiplikationen:

$$\mathbf{H}_{\rm K} \cdot \underline{z}_{\rm K}^{\rm T} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},$$

$$\mathbf{H}_{\rm E} \cdot \underline{z}_{\rm E}^{\rm T} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} z_5 \\ z_6 \\ z_7 \end{pmatrix} = \begin{pmatrix} z_5 \\ z_6 \\ z_7 \end{pmatrix}.$$

Durch Gleichsetzen folgt $z_5 = 0$, $z_6 = 0$, $z_7 = 1$ ⇒ Lösungsvorschlag 2.

d) Der Matrizenvergleich zeigt, dass die ersten drei Spalten von $\mathbf{H}$ und $\mathbf{H}_{\rm K}$ identisch sind. Die vierte Spalte von $\mathbf{H}_{\rm K}$ ist gleich der fünften Spalte der Prüfmatrix. Daraus folgt für den Vektor $\underline{z}_{\rm E} = (z_4, z_6, z_7)$ und weiter für den Empfangsvektor $\underline{y} = (1, 1, 0, {\rm E}, 0, {\rm E}, {\rm E})$ ⇒ Lösungsvorschlag 1 und 3.

e) Analog zur Teilaufgabe (c) erhält man nun:

$$\mathbf{H}_{\rm K} \cdot \underline{z}_{\rm K}^{\rm T} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

$$\mathbf{H}_{\rm E} \cdot \underline{z}_{\rm E}^{\rm T} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} z_4 \\ z_6 \\ z_7 \end{pmatrix} = \begin{pmatrix} 0 \\ z_4 + z_6 \\ z_4 + z_7 \end{pmatrix}.$$

Setzt man nun die beiden Spaltenvektoren gleich, so erhält man nur mehr zwei Gleichungen für die drei Unbekannten ⇒ Lösungsvorschlag 4.

Oder anders ausgedrückt: Ist die Anzahl der Auslöschungen des BEC–Kanals größer als der Rang der Matrix $\mathbf{H}_{\rm E}$, so ergibt sich keine eindeutige Lösung des resultierenden Gleichungssystems.

f) Zur Lösung dieser Aufgabe beziehen wir uns wieder auf den systematischen Hamming–Code (7, 4, 3) entsprechend der angegebenen Prüfgleichung und der nachfolgenden Codetabelle. Die Informationsbit sind schwarz dargestellt und die Prüfbit rot. Die minimale Distanz dieses Codes beträgt $d_{\rm min} = 3$.

0000000	0100111	1000101	1100010
0001011	0101100	1001110	1101001
0010110	0110001	1010011	1110100
0011101	0111010	1011000	1111111

Weiter nehmen wir an, dass stets das gelb hinterlegte Codewort $\underline{x} = (1, 1, 0, 1, 0, 0, 1)$ gesendet wurde:

- Ist die Anzahl $n_{\rm E}$ der Auslöschungen kleiner als $d_{\rm min} = 3$, so ist eine Decodierung nach der hier beschriebenen Methode immer möglich ⇒ siehe beispielsweise Teilaufgabe (a) mit $n_{\rm E} = 2$.
- Auch für $n_{\rm E} = d_{\rm min} = 3$ ist manchmal eine Decodierung möglich, wie in Aufgabe (c) gezeigt. In der Codetabelle gibt es nur ein einziges Codewort, das zum Empfangsvektor $\underline{y} = (1, 1, 0, 1, {\rm E}, {\rm E}, {\rm E})$ passen könnte, nämlich das gelb hinterlegte Codewort $\underline{x} = (1, 1, 0, 1, 0, 0, 1)$.
- Dagegen konnte $\underline{y} = (1, 1, 0, {\rm E}, 0, {\rm E}, {\rm E})$ entsprechend Teilaufgabe (d) nicht decodiert werden. In der Codetabelle erkennt man neben $(1, 1, 0, 1, 0, 0, 1)$ mit $(1, 1, 0, 0, 0, 1, 0)$ ein weiteres

Codewort (grün hinterlegt), das durch die $n_E = 3$ gegebenen Auslöschungen zum Empfangswort $\underline{y}$ wird. Dieser Fall, wenn die $n_E = d_{min}$ Auslöschungen genau die d_{min} unterschiedlichen Bit zweier Codeworte betreffen, führt zu einer Matrix $\mathbf{H}_E$ mit einem Rang kleiner als d_{min}.

- Ist $n_E > d_{min}$, so ist die Anzahl $n - n_E$ der nicht ausgelöschten Bit kleiner als die Anzahl k der Informationsbit. In diesem Fall kann das Codewort natürlich nicht decodiert werden.

Das heißt: Zutreffend sind die Aussagen 1, 3 und 4.

Musterlösung zur Zusatzaufgabe Z1.13

a) Betrachtet wird der (7, 4, 3)–Hamming–Code. Dementsprechend ist die minimale Distanz $d_{\rm min} = 3$.

b) Die ersten $k = 4$ Bit eines jeden Codewortes $\underline{x}$ stimmen mit dem Informationswort $\underline{u}$ überein. Richtig ist somit JA.

c) Es können bis zu $e_{\rm max} = d_{\rm min} - 1 = 2$ Bit ausgelöscht sein, damit eine Decodierung mit Sicherheit möglich ist. Jedes Codewort unterscheidet sich von jedem anderen in mindestens drei Bitpositionen. Bei nur zwei Auslöschungen kann deshalb das Codewort in jedem Fall rekonstruiert werden.

d) In der Tabelle auf der Angabenseite findet man ein einziges Codewort, das mit „10" beginnt und mit „010" endet, nämlich $\underline{x} = (1, 0, 0, 1, 0, 1, 0)$. Da es sich um einen systematischen Code handelt, beschreiben die ersten $k = 4$ Bit das Informationswort $\underline{u} = (1, 0, 0, 1) \Rightarrow$ Antwort 2.

e) Richtig sind die Lösungsvorschläge 1 und 2.

- $\underline{y}_{\rm D} = (1, 0, {\rm E}, {\rm E}, {\rm E}, {\rm E}, 0)$ kann nicht decodiert werden, da weniger als $k = 4$ Bit (Anzahl der Informationsbit) ankommen.
- $\underline{y}_{\rm C} = ({\rm E}, {\rm E}, {\rm E}, 1, 0, 1, 0)$ ist ebenfalls nicht decodierbar, da sowohl $\underline{x} = (0, 1, 1, 1, 0, 1, 0)$ als auch $\underline{x} = (1, 0, 0, 1, 0, 1, 0)$ als mögliches Ergebnis in Frage kommen.
- $\underline{y}_{\rm B} = ({\rm E}, {\rm E}, 0, {\rm E}, 0, 1, 0)$ ist dagegen decodierbar, da von allen 16 möglichen Codeworten nur $\underline{x} = (1, 0, 0, 1, 0, 1, 0)$ mit $\underline{y}_{\rm B}$ in den (richtigen) Bitpositionen 3, 5, 6 und 7 übereinstimmt.
- $\underline{y}_{\rm A} = (1, 0, 0, 1, {\rm E}, {\rm E}, {\rm E})$ ist decodierbar. Es fehlen nur die $m = 3$ Prüfbit. Damit liegt das Informationswort $\underline{u} = (1, 0, 0, 1)$ ebenfalls fest (systematischer Code).

Musterlösung zur Aufgabe A1.14

a) Die Codeworte $\underline{x}_0$ und $\underline{x}_1$ unterscheiden sich in Bit 2, 4 und 5. Wird nur einer dieser drei Binärwerte richtig übertragen, ist damit das gesamte Codewort eindeutig bestimmt. Keine Information über das Codewort erhält man bei folgenden Empfangsvektoren (siehe Tabelle auf der Angabenseite):

- $\underline{y}$ = (0, E, 0, E, E) mit Wahrscheinlichkeit $\lambda^3 \cdot (1 - \lambda)^2$,
- $\underline{y}$ = (0, E, E, E, E) mit Wahrscheinlichkeit $\lambda^4 \cdot (1 - \lambda)$,
- $\underline{y}$ = (E, E, 0, E, E) mit Wahrscheinlichkeit $\lambda^4 \cdot (1 - \lambda)$,
- $\underline{y}$ = (E, E, E, E, E) mit Wahrscheinlichkeit λ^5.

Die Wahrscheinlichkeit, dass aufgrund des spezifischen Empfangsvektors $\underline{y}$ das Codewort $\underline{x}_1$ genau so wahrscheinlich ist wie $\underline{x}_0$, ergibt sich zu

$$\Pr\left[\underline{x}_0 \text{ und } \underline{x}_1 \text{ sind gleichwahrscheinlich}\right] = \lambda^3 \cdot (1-\lambda)^2 + 2 \cdot \lambda^4 \cdot (1-\lambda) + \lambda^5 =$$
$$= \lambda^3 \cdot \left[(1-\lambda)^2 + 2 \cdot \lambda \cdot (1-\lambda) + \lambda^2\right] = \lambda^3 .$$

In diesem Fall entscheidet man sich nach dem Zufallsprinzip entweder für $\underline{x}_0$ (wäre richtig) oder für $\underline{x}_1$ (leider falsch), und zwar mit gleicher Wahrscheinlichkeit. Daraus folgt:

$$\Pr[\underline{x}_0 \mapsto \underline{x}_1] = 1/2 \cdot \lambda^3 \underline{= 5 \cdot 10^{-4}}.$$

b) Nach Teilaufgabe (a) ist die Antwort 2 richtig und nicht die Antwort 1. Auch die Aussage 3 ist falsch: $\Pr[\underline{x}_0 \to \underline{x}_1]$ sagt nicht aus, dass mit dieser Wahrscheinlickeit das Codewort $\underline{x}_0$ tatsächlich in das falsche Codewort $\underline{x}_1$ übergeht, sondern nur, dass es mit dieser Wahrscheinlichkeit zu $\underline{x}_1$ übergehen könnte. $\Pr[\underline{x}_0 \to \underline{x}_1]$ beinhaltet auch Konstellationen, bei denen die Entscheidung tatsächlich für $\underline{x}_2$ bzw. $\underline{x}_3$ fällt.

c) Wegen $d_H(\underline{x}_0, \underline{x}_2) = 3$ und $d_H(\underline{x}_0, \underline{x}_3) = 4$ ergibt sich hierfür

$$\Pr[\underline{x}_0 \mapsto \underline{x}_2] = 1/2 \cdot \lambda^3 \underline{= 5 \cdot 10^{-4}}, \quad \Pr[\underline{x}_0 \mapsto \underline{x}_3] = 1/2 \cdot \lambda^4 \underline{= 5 \cdot 10^{-5}}.$$

d) Die Blockfehlerwahrscheinlichkeit ist nie größer (mit einer gewissen Wahrscheinlichkeit eher kleiner) als die so genannte *Union Bound*:

$$\Pr(\text{Union Bound}) = \Pr[\underline{x}_0 \mapsto \underline{x}_1] + \Pr[\underline{x}_0 \mapsto \underline{x}_2] + \Pr[\underline{x}_0 \mapsto \underline{x}_3] =$$
$$= 2 \cdot \lambda^3/2 + \lambda^4/2 = 0.001 + 0.00005 \underline{= 1.05 \cdot 10^{-3}}.$$

e) Allgemein gilt: Pr(Blockfehler) ≤ Pr(Bhattacharyya) = $W(\beta)$ - 1. Für das Distanzspektrum bzw. die Gewichtsfunktion erhält man im vorliegenden Fall:

$$W_0 = 1, \quad W_3 = 2, \quad W_4 = 1 \quad \Rightarrow \quad W(X) = 1 + 2 \cdot X^3 + X^4 .$$

Beim BEC–Kanal gilt zudem $\beta = \lambda$. Daraus folgt als Endergebnis für $\lambda = 0.001$:

$$\Pr(\text{Bhattacharyya}) = 2 \cdot \lambda^3 + \lambda^4 \underline{= 2.1 \cdot 10^{-3}}.$$

Anzumerken ist, dass beim BEC–Modell die *Bhattacharyya–Schranke* stets doppelt so groß ist wie die *Union Bound*, die ja selbst wieder eine obere Schranke für die Blockfehlerwahrscheinlichkeit darstellt.

Musterlösung zur Aufgabe A1.15

a) Durch die Analyse aller Codeworte des (7, 4, 3)–Hamming–Codes erkennt man, dass

- $W_0 = \underline{1}$ Codewort keine Eins beinhaltet (das Nullwort),
- $W_3 = \underline{7}$ Codeworte drei Einsen beinhalten,
- $W_4 = \underline{7}$ Codeworte vier Einsen beinhalten,
- $W_7 = \underline{1}$ Codewort nur aus Einsen besteht.

W_i gibt gleichzeitig die Anzahl der Codeworte an, die sich vom Nullwort in i Bit unterscheiden.

b) Die Bhattacharyya–Schranke lautet:

$$\Pr(\text{Blockfehler}) \le \Pr(\text{Bhattacharyya}) = W(\beta) - 1\,.$$

Die Gewichtsfunktion ist durch die Teilaufgabe a) festgelegt:

$$W(X) = 1 + 7 \cdot X^3 + 7 \cdot X^4 + X^7$$
$$\Rightarrow \quad \Pr(\text{Bhattacharyya}) = 7 \cdot \beta^3 + 7 \cdot \beta^4 + \beta^7\,.$$

Für den Bhattacharyya–Parameter des BSC–Modells gilt:

$$\beta = 2 \cdot \sqrt{\varepsilon \cdot (1-\varepsilon)} = 2 \cdot \sqrt{0.01 \cdot 0.99} = 0.199$$
$$\Rightarrow \quad \Pr(\text{Bhattacharyya}) = 7 \cdot 0.199^3 + 7 \cdot 0.199^4 + 0.199^7 \approx \underline{0.066}\,.$$

Ein Vergleich mit der tatsächlichen Blockfehlerwahrscheinlichkeit, wie in **Aufgabe A1.12** berechnet:

$$\Pr(\text{Blockfehler}) \approx 21 \cdot \varepsilon^2 = 2.1 \cdot 10^{-3}\,,$$

zeigt, dass Bhattacharyya nur eine äußerst grobe Schranke bereitstellt. Im vorliegenden Fall liegt diese Schranke um mehr als den Faktor 30 über dem tatsächlichen Wert.

c) Aus der Codetabelle des (8, 4, 4)–Codes erhält man folgende Ergebnisse:

$$W(X) = 1 + 14 \cdot X^4 + X^8$$
$$\Rightarrow \quad \Pr(\text{Bhattacharyya}) = 14 \cdot \beta^4 + \beta^8 = 14 \cdot 0.199^4 + 0.199^8 \approx \underline{0.022}\,.$$

d) Die Gleichung für den Bhattacharyya–Parameter lautet:

$$\beta = \begin{cases} \lambda & \text{für das BEC – Modell,} \\ 2 \cdot \sqrt{\varepsilon \cdot (1-\varepsilon)} & \text{für das BSC – Modell,} \\ \exp[-R \cdot E_{\rm B}/N_0] & \text{für das AWGN – Modell.} \end{cases}$$

Mit dem BEC–Modell ergibt sich genau die gleiche Schranke, wenn die Auslöschungswahrscheinlichkeit $\lambda = \beta = \underline{0.199}$ beträgt.

e) Entsprechend obiger Gleichung muss gelten:

$$\beta = \exp[-R \cdot E_{\rm B}/N_0] = 0.199 \quad \Rightarrow \quad R \cdot E_{\rm B}/N_0 = 10^{0.199} = 1.58\,.$$

Die Coderate des (8, 4, 4)–Codes ist $R = 0.5$:

$$E_{\rm B}/N_0 = 3.16 \quad \Rightarrow \quad 10 \cdot \lg E_{\rm B}/N_0 \approx \underline{5\,\text{dB}}\,.$$

f) Mit der Coderate $R = 4/7$ erhält man:

$$E_{\rm B}/N_0 = 7/4 \cdot 1.58 = 2.765 \quad \Rightarrow \quad 10 \cdot \lg E_{\rm B}/N_0 \approx \underline{4.417\,\rm dB}.$$

Musterlösung zur Aufgabe A1.16

a) Richtig ist Antwort 2. Das Distanzspektrum $\{W_i\}$ ist definiert für $i = 0, \ldots, n$:

- W_1 gibt an, wie oft das Hamming–Gewicht $w_{\rm H}(\underline{x}_i) = 1$ auftritt.
- W_n gibt an, wie oft das Hamming–Gewicht $w_{\rm H}(\underline{x}_i) = n$ auftritt.

Damit lautet die *Union Bound*:

$$p_1 = \Pr(\text{Union Bound}) = \sum_{i=1}^{n} W_i \cdot {\rm Q}\left(\sqrt{i/\sigma^2}\right) .$$

b) Das Distanzspektrum des (8, 4, 4)–Codes wurde mit $W_0 = 1$, $W_4 = 14$, $W_8 = 1$ angegeben. Somit erhält man für $\boldsymbol{\sigma = 1}$:

$$p_1 = W_4 \cdot {\rm Q}\left(2\right) + W_8 \cdot {\rm Q}\left(2 \cdot \sqrt{2}\right) = 14 \cdot 2.28 \cdot 10^{-2} + 1 \cdot 0.23 \cdot 10^{-2} \approx \underline{0.3215},$$

bzw. für $\boldsymbol{\sigma = 0.5}$:

$$p_1 = 14 \cdot {\rm Q}\left(4\right) + {\rm Q}\left(4 \cdot \sqrt{2}\right) = 14 \cdot 3.17 \cdot 10^{-5} + 1.1 \cdot 10^{-8} \approx \underline{0.444 \cdot 10^{-3}}.$$

c) Mit der Minimaldistanz $d_{\rm min} = 4$ erhält man:

$$\sigma = 1.0: \quad p_2 = W_4 \cdot {\rm Q}\left(2\right) \underline{= 0.3192},$$
$$\sigma = 0.5: \quad p_2 = W_4 \cdot {\rm Q}\left(4\right) \approx p_1 \underline{= 0.444 \cdot 10^{-3}}.$$

d) Richtig ist Antwort 1. Die *Union Bound* – hier mit p_1 bezeichnet – ist in jedem Fall eine obere Schranke für die Blockfehlerwahrscheinlichkeit. Für die Schranke p_2 (*Truncated Union Bound*) trifft das nicht immer zu. Beispielsweise erhält man beim (7, 4, 3)–Hamming–Code $\Rightarrow$ $W_3 = W_4 = 7$, $W_7 = 1$ und der Streuung $\sigma = 1$:

$$p_2 = 7 \cdot {\rm Q}\left(\sqrt{3}\right) = 7 \cdot 4.18 \cdot 10^{-2} \approx 0.293,$$
$$p_1 = p_2 + 7 \cdot {\rm Q}\left(\sqrt{4}\right) + 1 \cdot {\rm Q}\left(\sqrt{7}\right) \approx 0.455 .$$

Die tatsächliche Blockfehlerwahrscheinlichkeit wird wahrscheinlich zwischen $p_2 = 0.293$ und $p_1 = 0.455$ liegen (wurde nicht nachgeprüft). Das heißt: p_2 ist keine obere Schranke.

e) Richtig sind die Lösungsvorschläge 1 und 3, wie die folgende Rechnung für den (8, 4, 4)–Code zeigt:

- Es gilt ${\rm Q}(x) \le {\rm Q_{CR}}(x) = \exp(-x^2/2)$. Damit kann für die *Union Bound*

  $$p_1 = W_4 \cdot {\rm Q}\left(\sqrt{4/\sigma^2}\right) + W_8 \cdot {\rm Q}\left(\sqrt{8/\sigma^2}\right)$$

  eine weitere obere Schranke angegeben werden:

  $$p_1 \le W_4 \cdot \exp\left[-4/(2\sigma^2)\right] + W_8 \cdot \exp\left[-8/(2\sigma^2)\right] .$$

- Mit $\beta = \exp[-1/(2\sigma^2)]$ kann hierfür auch geschrieben werden (das vorgegebene $\beta = 1/\sigma$ ist also falsch):

$$p_1 \le W_4 \cdot \beta^4 + W_8 \cdot \beta^8.$$

- Die Gewichtsfunktion des (8, 4, 4)–Codes lautet:

$$W(X) = 1 + W_4 \cdot X^4 + W_8 \cdot X^8 \quad \Rightarrow \quad W(\beta) - 1 = W_4 \cdot \beta^4 + W_8 \cdot \beta^8$$
$$\Rightarrow \quad p_3 = W(\beta) - 1 \ge p_1 \,.$$

f) Mit $\boldsymbol{\sigma = 1}$ lautet der Bhattacharyya–Parameter $\beta = \exp(-0.5) = 0.6065$ und man erhält damit für die Bhattacharyya–Schranke:

$$p_3 = 14 \cdot \beta^4 + \beta^8 = 14 \cdot 0.135 + 0.018 \underline{= 1.913}.$$

Berücksichtigt man, dass p_3 (eine Schranke für) eine Wahrscheinlichkeit angibt, so ist $p_3 = 1.913$ nur eine triviale Schranke. Für $\boldsymbol{\sigma = 0.5}$ ergibt sich dagegen $\beta = \exp(-2) \approx 0.135$. Dann gilt:

$$p_3 = 14 \cdot \beta^4 + \beta^8 = 14 \cdot 3.35 \cdot 10^{-4} + 1.1 \cdot 10^{-7} \underline{= 4.7 \cdot 10^{-3}}.$$

Ein Vergleich mit der Teilaufgabe b) zeigt, dass im vorliegenden Beispiel die Bhattacharyya–Schranke p_3 um den Faktor $(4.7 \cdot 10^{-3})/(0.44 \cdot 10^{-3}) > 10$ oberhalb der *Union Bound* p_1 liegt. Der Grund für diese große Abweichung ist die Chernoff–Rubin–Schranke, die deutlich oberhalb der Q–Funktion liegt. In der **Aufgabe Z1.16** wird die Abweichung zwischen Q_{CR} und $Q(x)$ auch quantitativ berechnet:

$$Q_{CR}(x)/Q(x) \approx 2.5 \cdot x \quad \Rightarrow \quad Q_{CR}(x = 4)/Q(x = 4) \approx 10 \,.$$

Musterlösung zur Zusatzaufgabe Z1.16

a) Die obere Schranke lautet:

$$Q_o(x) = \frac{1}{\sqrt{2\pi}\cdot x}\cdot e^{-x^2/2} \quad \Rightarrow \quad Q_o(4) = \frac{1}{\sqrt{2\pi}\cdot 4}\cdot e^{-8} \approx \underline{3.346\cdot 10^{-5}}.$$

Die untere Schranke kann wie folgt umgewandelt werden:

$$Q_u(x) = (1 - 1/x^2)\cdot Q_o(x) \quad \Rightarrow \quad Q_u(4) \approx \underline{3.137\cdot 10^{-5}}.$$

Die relativen Abweichungen gegenüber dem „echten" Wert $Q(4) = 3.167 \cdot 10^{-5}$ sind +5% bzw. –1%.

b) Richtig sind <u>Antwort 1 und 2</u>. Für $x = 2$ wird der tatsächliche Funktionswert $Q(x) = 2.275 \cdot 10^{-2}$ begrenzt durch $Q_o(x) = 2.7 \cdot 10^{-2}$ bzw. $Q_u(x) = 2.025 \cdot 10^{-2}$. Die relativen Abweichungen betragen 18.7% bzw. –11%. Die letzte Aussage ist falsch. Erst für $x < 0.37$ gilt $Q_o(x) > 1$.

c) Für den Quotienten aus $Q_{CR}(x)$ und $Q_o(x)$ gilt nach den vorgegebenen Gleichungen:

$$q(x) = \frac{Q_{CR}(x)}{Q_o(x)} = \frac{\exp(-x^2/2)}{\exp(-x^2/2)/(\sqrt{2\pi}\cdot x)} = \sqrt{2\pi}\cdot x$$

$$\Rightarrow \quad q(x) \approx 2.5\cdot x \quad \Rightarrow \quad q(x=2) = 5,\ \ q(x=4) = 10,\ \ q(x=6) = 15\,.$$

Je größer der Abszissenwert x, um so ungenauer wird $Q(x)$ durch $Q_{CR}(x)$ angenähert. Bei Betrachtung der Grafik auf der Angabenseite hat man (hatte ich) den Eindruck, dass $Q_{CR}(x)$ sich aus $Q(x)$ durch Verschieben nach unten bzw. Verschieben nach oben ergibt. Das ist aber nur eine optische Täuschung und entspricht nicht dem Sachverhalt.

d) Mit <u>$K = 0.5$</u> stimmt die neue Schranke $0.5 \cdot Q_{CR}(x)$ für $x = 0$ exakt mit $Q(x = 0) = 0.500$ überein. Für größere Abszissenwerte wird damit auch die Verfälschung $q = 1.25 \cdot x$ nur halb so groß.

Musterlösung zur Aufgabe A1.17

a) Richtig sind alle Lösungsvorschläge. Dies erkennt man bereits an den Raten: **Z** hat eine größere Rate als **Y** und **Y** eine größere Rate als **X**. Da zudem der Hamming–Code (31,15,3) ⇒ Code **Z** die größte Codewortlänge n aufweist, benötigt er trotz größerer Coderate R für BER = 10^{-5} ein geringeres E_B/N_0.

b) Richtig ist die Antwort 2. Für eine kleinere Bitfehlerrate benötigt man stets ein größeres E_B/N_0. Eine vertikale Verschiebung gibt es nicht, da sich auch mit BER = 10^{-10} an den Coderaten nichts ändert.

c) Für den logarithmierten AWGN–Parameter $10 \cdot \lg E_B/N_0 = 3$ dB ergibt sich die vorne angegebene Hilfsgröße $x = 1.6 + 3 = 4.6$. Damit erhält man:

$$R_{\max} = C(x = 4.6) = 1 - \exp(-0.4 \cdot 4.6) \underline{= 0.84}.$$

d) Entsprechend der vorgegebenen Gleichung gilt nun:

$$1 - \exp(-0.4 \cdot x) = 0.5 \quad \Rightarrow \quad x = \frac{-\ln(0.5)}{-0.4} = 1.73$$

$$\Rightarrow \quad 10 \cdot \lg E_B/N_0 = 1.73 - 1.6 = 0.13\,\text{dB}.$$

$10 \cdot \lg E_B/N_0$ könnte demnach um 3 dB – 0.13 dB = 2.87 dB herabgesetzt werden, also um den Faktor

$$A = 10^{0.287} \underline{= 1.94}.$$

Musterlösung zur Zusatzaufgabe Z1.17

a) Im unteren E_B/N_0–Bereich laufen die Kapazitätskurven

- C_2 (gültig für binären Eingang, z.B. BPSK) und
- C (gültig für analogen reellwertigen Eingang)

zusammen. Für eine gegebene Rate R muss E_B/N_0 größer sein als $(2^{2R} – 1)/2R$. Der Grenzübergang für $R \to 0$ liefert die absolute Shannon–Grenze, ab der eine fehlerfreie Übertragung nicht mehr möglich ist:

$$\text{Min}\ [E_B/N_0] = \lim_{R \to 0} \frac{2^{2R} - 1}{2R} = \ln 2 \approx 0.693$$
$$10 \cdot \lg \text{Min}\ [E_B/N_0] \approx -1.6\,\text{dB} \quad \Rightarrow \quad x_0 \underline{= 1.6\,\text{dB}}.$$

b) Aus der Grafik auf der Angabenseite lässt sich die Tangentensteigerung im Nullpunkt abschätzen:

$$\frac{\text{d}C_2}{\text{d}x}(x = 0) = \frac{1.6 + 1.5}{1.25} = 2.48 \quad \Rightarrow \quad a = \frac{1}{2.48} \underline{\approx 0.4}.$$

Damit lautet die Näherung für die BPSK–Kanalkapazität in Abhängigkeit des Abszissenwertes x:

$$C_2' = \begin{cases} 1 - \exp(-0.4 \cdot x) & \text{für } x > 0, \\ 0 & \text{für } x < 0. \end{cases}$$

c) Aus $E_B = N_0$ folgt $10 \cdot \lg (E_B/N_0) = 0$ dB sowie $x = 1.6$:

$$C_2' = 1 - \exp(-0.4 \cdot 1.6) \underline{\approx 0.47}.$$

d) Die entsprechenden Zahlenwerte lauten:

$$10 \cdot \lg E_B/N_0 = 2\,\text{dB}: \quad C_2' = 1 - \exp(-0.4 \cdot 3.6) \underline{\approx 0.76},$$
$$10 \cdot \lg E_B/N_0 = 4\,\text{dB}: \quad C_2' = 1 - \exp(-0.4 \cdot 5.6) \underline{\approx 0.89},$$
$$10 \cdot \lg E_B/N_0 = 6\,\text{dB}: \quad C_2' = 1 - \exp(-0.4 \cdot 7.6) \underline{\approx 0.95}.$$

Die so angenäherten Werte C_2' der Kanalkapazität für binären Eingang sind etwas zu klein. Aus der Grafik können die genaueren Werte C_2 abgelesen werden:

$$10 \cdot \lg E_B/N_0 = 2\,\text{dB}: \quad C_2 \approx 0.78,$$
$$10 \cdot \lg E_B/N_0 = 4\,\text{dB}: \quad C_2 \approx 0.94,$$
$$10 \cdot \lg E_B/N_0 = 6\,\text{dB}: \quad C_2 \approx 0.99.$$

Ab etwa $10 \cdot \lg (E_B/N_0) = 8$ dB gilt innerhalb der Zeichengenauigkeit $C_2' = C_2 = 1$ (bit/Kanalzugriff).