A1.1: Zur Kennzeichnung aller Bücher

Seit den 1960er Jahren werden alle Bücher mit einer 10–stelligen *International Standard Book Number* versehen. Die letzte Ziffer dieser sog. **ISBN–10–Angabe** berechnet sich dabei entsprechend folgender Regel:

$$z_{10} = \left(\sum_{i=1}^{9} \; i \cdot z_i \right) \mod 11 .$$

Seit 2007 ist zusätzlich die Angabe entsprechend des Standards **ISBN–13** verpflichtend, wobei die Prüfziffer z_{13} sich dann wie folgt ergibt:

$$z_{13} = 10 - \left(\sum_{i=1}^{12} \; z_i \cdot 3^{(i+1) \mod 2} \right) \mod 10 .$$

Nebenstehend sind einige beispielhafte ISBN angegeben. Hierauf beziehen sich die folgenden Fragen.

Hinweis: Die Aufgabe gehört zum Themengebiet von **Kapitel 1.1.**

Fragebogen zu "A1.1: Zur Kennzeichnung aller Bücher"

a) Um welchen Standard handelt es sich bei Beispiel 1?

- ISBN–10,
- ISBN–13.

b) Entsprechend Beispiel 2 sind zwei Ziffern einer ISBN–13 ausgelöscht. Kann man die ISBN rekonstruieren? Wenn Ja: Geben Sie die ISBN–13 an.

- Ja,
- Nein.

c) Entsprechend Beispiel 3 ist eine Ziffer einer ISBN–13 ausgelöscht. Kann die ISBN rekonstruiert werden? Wenn Ja: Geben Sie die ISBN–13 an.

- Ja,
- Nein.

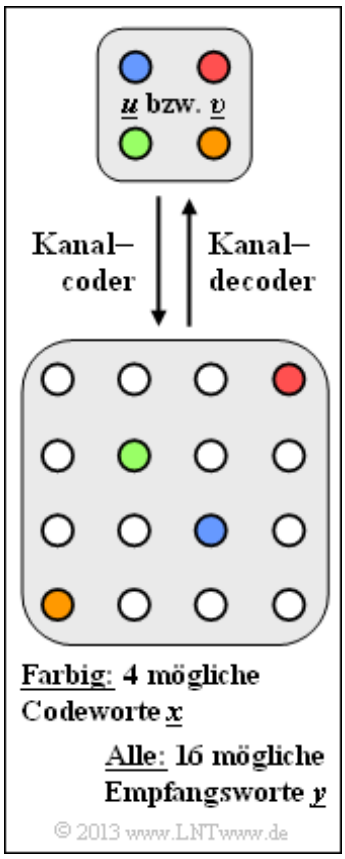
d) Wieviele verschiedene Werte kann die Prüfziffer z_{10} bei ISBN–10 annehmen?

$$\boldsymbol{M} =$$

e) Mitgeteilt als ISBN–10 wird 3–8273–7064–7. Welche Aussage trifft zu?

- Dies ist keine zulässige ISBN.
- Die ISBN könnte richtig sein.
- Die ISBN ist mit Sicherheit richtig.

A1.2: Einfacher binärer Kanalcode



Die Grafik verdeutlicht die hier betrachtete Kanalcodierung C:

- Es gibt vier mögliche Informationsblöcke $\underline{u} = (u_1, u_2, \ \text{...} \ , u_k)$.
- Jeder Informationsblock $\underline{u}$ wird eindeutig (erkennbar an der gleichen Farbe) dem Codewort $\underline{x} = (x_1, x_2, \ \text{...} \ , x_n)$ zugeordnet.
- Aufgrund von Decodierfehlern ($0 \rightarrow 1$, $1 \rightarrow 0$) gibt es mehr als 4, nämlich 16 verschiedene Empfangsworte $\underline{y} = (y_1, y_2, \ \text{...} \ , y_n)$.

Ab Teilaufgabe d) betrachten wir folgende Zuordnung:

$$\underline{u_0} = (0, 0) \leftrightarrow (0, 0, 0, 0) = \underline{x_0}\,,$$
$$\underline{u_1} = (0, 1) \leftrightarrow (0, 1, 0, 1) = \underline{x_1}\,,$$
$$\underline{u_2} = (1, 0) \leftrightarrow (1, 0, 1, 0) = \underline{x_2}\,,$$
$$\underline{u_3} = (1, 1) \leftrightarrow (1, 1, 1, 1) = \underline{x_3}\,.$$

Hinweis: Die hier abgefragten Beschreibungsgrößen wie

- Coderate,
- Hamming–Gewicht,
- Hamming–Distanz, usw.

werden auf **Seite 4** und **Seite 5** von Kapitel 1.1 definiert.

Fragebogen zu "A1.2: Einfacher binärer Kanalcode"

a) Aus wievielen Binärsymbolen besteht ein Informationsblock?

$$k =$$

b) Wie groß ist die Codewortlänge n?

$$n =$$

c) Wie groß ist die Coderate?

$$R =$$

d) Ist der hier vorgegebene Code systematisch?

- ○ Ja,
- ○ Nein.

e) Geben Sie die Hamming–Gewichte aller Codeworte an.

$$w_H(\underline{x}_0) =$$

$$w_H(\underline{x}_1) =$$

$$w_H(\underline{x}_2) =$$

$$w_H(\underline{x}_3) =$$

f) Geben Sie die Hamming–Distanzen zwischen folgenden Codeworten an.

$$d_H(\underline{x}_0, \underline{x}_1) =$$

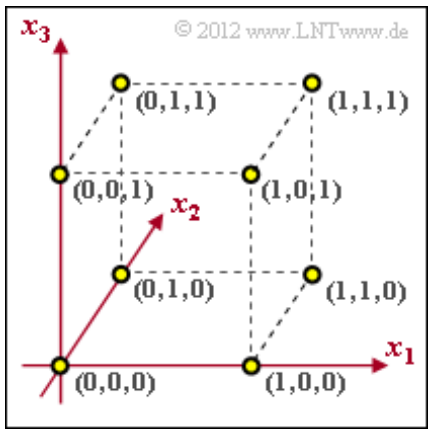
$$d_H(\underline{x}_0, \underline{x}_3) =$$

$$d_H(\underline{x}_1, \underline{x}_2) =$$

g) Wie groß ist die minimale Hamming–Distanz des betrachteten Codes C?

$$d_{min}(C) =$$

Z1.2: 3D–Darstellung von Codes



Codes zur Fehlererkennung bzw. Fehlererkorrektur lassen sich sehr anschaulich im n–dimensionalen Raum darstellen. Wir beschränken uns hier auf binäre Codes der Länge $n = 3$:

$$\underline{x} = (x_1, x_2, x_3) \in \mathrm{GF}(2^3),$$
$$x_i \in \{0, 1\}, \quad i = 1, 2, 3.$$

Allgemein gilt bei der Blockcodierung:

- Das Informationswort $\underline{u} = (u_1, u_2, \ \ldots \ , u_k)$ wird eindeutig in das Codewort $\underline{x} = (x_1, x_2, \ \ldots \ , x_n)$ überführt.
- Die Coderate beträgt $R = k/n$.
- Die Hamming–Distanz $d_H(\underline{x}, \underline{x}')$ zwischen zwei Codeworten $\underline{x} \in C$ und $\underline{x}' \in C$ gibt die Anzahl der Bitpositionen an, in denen sich $\underline{x}$ und $\underline{x}'$ unterscheiden.
- Die Minimaldistanz $d_{min} = \min [d_H(\underline{x}, \underline{x}')]$ ist ein Maß für die Korrekturfähigkeit eines Codes.
- Es können $e = d_{min} - 1$ Fehler erkannt und $t = (d_{min} - 1)/2$ korrigiert werden. Die letzte Aussage gilt allerdings nur für ungerades d_{min}.

Hinweis: Die Aufgabe gehört zum Themengebiet von **Kapitel 1.1.** Zusätzlich werden einige einfache Fragen zu **Kapitel 1.3** vorweg genommen.

Fragebogen zu "Z1.2: 3D–Darstellung von Codes"

a) Welche Aussagen gelten, wenn alle Punkte in GF(2^3) belegt sind?

- ☐ Es gilt die Zuordnung $\underline{u} = (u_1, u_2, u_3) \rightarrow \underline{x} = (x_1, x_2, x_3)$.
- ☐ Es gilt die Identität $\underline{x} = \underline{u}$.
- ☐ Die Coderate ist $R = 1$.
- ☐ Die Minimaldistanz zwischen zwei Codeworten ist $d_{min} = 2$.

b) Welche Aussagen gelten für einen (3, 2, 2)–Blockcode?

- ☐ Code $C_1 = \{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$ ist möglich.
- ☐ Code $C_2 = \{(0, 0, 1), (0, 1, 0), (1, 0, 0), (1, 1, 1)\}$ ist möglich.
- ☐ Code $C_3 = \{(0, 0, 0), (0, 1, 1), (1, 0, 0), (1, 1, 1)\}$ ist möglich.

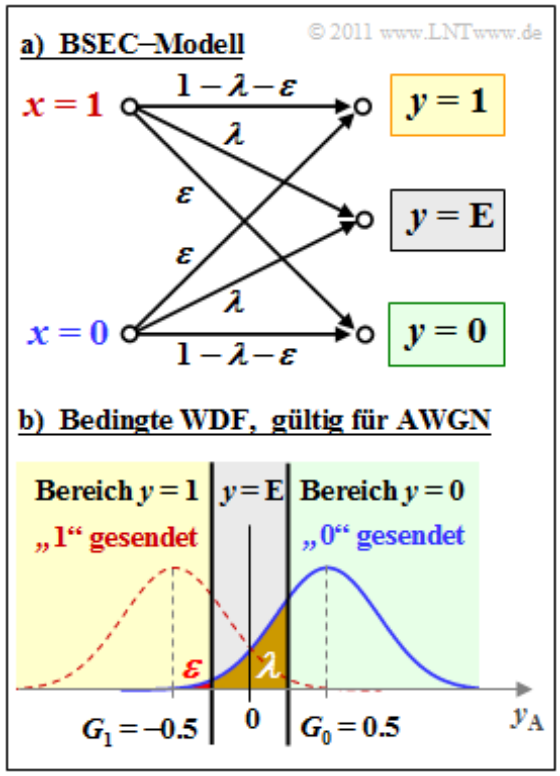
c) Welche Eigenschaften zeigt der in Teilaufgabe b) definierte Code C_1?

- ☐ Ein Bitfehler lässt sich erkennen.
- ☐ Ein Bitfehler kann korrigiert werden.

d) Welche Eigenschaften zeigt der Code $C_4 = \{(0, 0, 0), (1, 1, 1)\}$?

- ☐ Die Coderate beträgt $R = 1/4$.
- ☐ Die Coderate beträgt $R = 1/3$.
- ☐ Ein Bitfehler lässt sich erkennen.
- ☐ Ein Bitfehler kann korrigiert werden.

A1.3: BSC–BEC–BSEC–AWGN



Im Theorieteil zu diesem Kapitel werden die folgenden digitalen Kanalmodelle behandelt:

- **Binary Symmetric Channel** (BSC),
- **Binary Erasure Channel** (BEC),
- **Binary Symm. Error & Erasure Ch.** (BSEC).

Die obere Grafik zeigt das BSEC–Modell. Daraus lassen sich auch die beiden anderen Kanalmodelle ableiten:

- Mit $\lambda = 0$ ergibt sich das BSC–Modell.
- Mit $\varepsilon = 0$ ergibt sich das BEC–Modell.

Die untere Grafik zeigt den Zusammenhang zwischen dem BSEC–Modell und dem analogen AWGN–Kanalmodell. Um Verwechslungen zu vermeiden, bezeichnen wir das (analoge) Ausgangssignal des AWGN–Kanals mit $y_{\rm A}$, wobei mit dem Rauschterm n gilt: $y_{\rm A} = \tilde{x} + n$.

Die Tilde weist auf die bipolare Beschreibung des Digitalsignals hin. Es gilt $\tilde{x} = +1$, falls $x = 0$, und $\tilde{x} = –1$, falls $x = 1$.

Man erkennt die ternäre Ausgangsgröße $y \in \{0, 1, {\rm E}\}$, die sich aus dem AWGN–Modell durch die Unterteilung in drei Bereiche ergibt. Hierzu werden die Entscheiderschwellen G_0 und G_1 benötigt.

$y = {\rm E}$ (*Erasure*) sagt aus, dass die Entscheidung so unsicher ist, dass als Ergebnis weder $y = 0$ noch $y = 1$ gerechtfertigt erscheint. In deutschen Fachbüchern spricht man von einer *Auslöschung*.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 1.2.** Die Streuung des AWGN–Rauschens n wird für die gesamte Aufgabe zu $\sigma = 0.4$ angenommen. Die Wahrscheinlichkeit, dass die Zufallsgröße n größer ist als A oder kleiner als $–A$, ergibt sich mit dem **komplementären Gaußschen Fehlerintegral** ${\rm Q}(x)$ wie folgt:

$$\Pr(n > A) = \Pr(n < -A) = {\rm Q}(A/\sigma).$$

Es folgen noch einige Zahlenwerte der Q–Funktion:

$$\begin{aligned}{\rm Q}(0) &= 50\%\,,\ {\rm Q}(0.5) = 30.85\%\,,\ {\rm Q}(1) = 15.87\%\,,\ {\rm Q}(1.5) = 6.68\%\,,\\ {\rm Q}(2) &= 2.28\%\,,\ {\rm Q}(2.5) = 0.62\%\,,\ {\rm Q}(3) = 0.14\%\,,\ {\rm Q}(3.5) = 0.02\%\,,\ {\rm Q}(4) \approx 0\,.\end{aligned}$$

Bitte beachten Sie weiter: Ausgehend vom AWGN–Kanal ist die Verfälschungswahrscheinlichkeit $\varepsilon = 0$ eigentlich nicht möglich. Für diese Aufgabe behelfen wir uns dadurch, dass alle Wahrscheinlichkeiten in Prozent mit zwei Nachkommastellen angegeben werden sollen. Damit kann $\varepsilon < 0.5 \cdot 10^{–4}$ durch $\varepsilon \approx 0$ angenähert werden.

Fragebogen zu "A1.3: BSC–BEC–BSEC–AWGN"

a) Durch welche Entscheiderschwelle(n) entsteht das BSC–Modell?

- ☐ Eine Entscheiderschwelle bei $G = 0$.
- ☐ Zwei symmetrische Entscheiderschwellen bei $\pm G$.
- ☐ Eine Entscheiderschwelle bei $G_1 = 0$ und eine zweite bei $G_2 = 0.5$.

b) Wie groß ist die BSC–Verfälschungswahrscheinlichkeit ε mit $\sigma = 0.4$?

ε = ____ %

c) Durch welche Entscheiderschwelle(n) entsteht ein BSEC–Modell?

- ☐ Eine Entscheiderschwelle bei $G = 0$.
- ☐ Zwei symmetrische Entscheiderschwellen bei $\pm G$.
- ☐ Eine Entscheiderschwelle bei $G_1 = 0$ und eine zweite bei $G_2 = 0.5$.

d) Welche BSEC–Parameter ergeben sich mit Schwellen bei ±0.2?

ε = ____ %

λ = ____ %

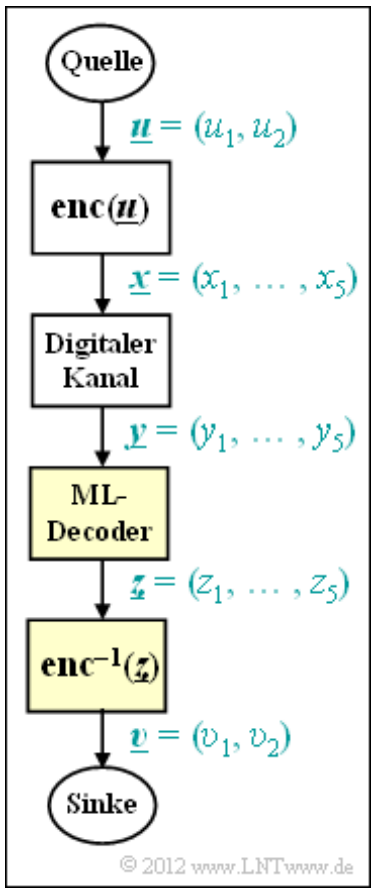
e) Durch welche Entscheiderschwelle(n) entsteht das BEC–Modell? Beachten Sie bitte den letzten Hinweis auf der Angabenseite.

- ☐ Eine Entscheiderschwelle bei $G = 0$.
- ☐ Zwei symmetrische Entscheiderschwellen bei $\pm G$.
- ☐ Eine Entscheiderschwelle bei $G_1 = 0$ und eine zweite bei $G_2 = 0.5$.

f) Berechnen Sie den BEC–Parameter λ für Entscheiderschwellen bei ±0.6.

λ = ____ %

A1.4: Maximum–Likelihood–Entscheidung



Wir betrachten das digitale Übertragungssystem entsprechend der Grafik. Berücksichtigt sind dabei:

- ein systematischer (5, 2)–Blockcode C mit den Codeworten

$$\begin{aligned}\underline{x}_0 &= (0, 0, 0, 0, 0)\,,\\ \underline{x}_1 &= (0, 1, 0, 1, 0)\,,\\ \underline{x}_2 &= (1, 0, 1, 0, 1)\,,\\ \underline{x}_3 &= (1, 1, 1, 1, 1)\,,\end{aligned}$$

- ein digitales (binäres) Kanalmodell, das den Vektor $\underline{x} \in \mathrm{GF}(2^5)$ in den Vektor $\underline{y} \in \mathrm{GF}(2^5)$ verfälscht,
- ein **Maximum–Likelihood–Decoder** mit der Entscheidungsregel

$$\underline{z} = \arg \max_{\underline{x}_i \in C} \Pr(\underline{x}_i \,|\, \underline{y}) = \arg \min_{\underline{x}_i \in C} \, d_{\rm H}(\underline{y}\,,\, \underline{x}_i).$$

In der Gleichung bezeichnet $d_{\rm H}(\underline{y}, \underline{x}_i)$ die **Hamming–Distanz** zwischen Empfangswort $\underline{y}$ und dem (möglicherweise) gesendeten Codewort $\underline{x}_i$.

Hinweis: Die Aufgabe gehört zum **Kapitel 1.2.**

Fragebogen zu "A1.4: Maximum–Likelihood–Entscheidung"

a) Es sei $\underline{y} = (1, 0, 0, 0, 1)$. Welche Entscheidungen erfüllen das ML–Kriterium?

- ☐ $\underline{z} = \underline{x}_0 = (0, 0, 0, 0, 0)$,
- ☐ $\underline{z} = \underline{x}_1 = (0, 1, 0, 1, 0)$,
- ☐ $\underline{z} = \underline{x}_2 = (1, 0, 1, 0, 1)$,
- ☐ $\underline{z} = \underline{x}_3 = (1, 1, 1, 1, 1)$.

b) Es sei $\underline{y} = (0, 0, 0, 1, 0)$. Welche Entscheidungen erfüllen das ML–Kriterium?

- ☐ $\underline{z} = \underline{x}_0 = (0, 0, 0, 0, 0)$,
- ☐ $\underline{z} = \underline{x}_1 = (0, 1, 0, 1, 0)$,
- ☐ $\underline{z} = \underline{x}_2 = (1, 0, 1, 0, 1)$,
- ☐ $\underline{z} = \underline{x}_3 = (1, 1, 1, 1, 1)$.

c) Welche Entscheidung trifft der ML–Decoder für $\underline{y} = (1, 0, 1, 1, 1)$, wenn ihm mitgeteilt wird, dass die beiden letzten Symbole eher unsicher sind?

- ☐ $\underline{z} = \underline{x}_0 = (0, 0, 0, 0, 0)$,
- ☐ $\underline{z} = \underline{x}_1 = (0, 1, 0, 1, 0)$,
- ☐ $\underline{z} = \underline{x}_2 = (1, 0, 1, 0, 1)$,
- ☐ $\underline{z} = \underline{x}_3 = (1, 1, 1, 1, 1)$.

d) Zu welchem Informationswort $\underline{v} = (v_1, v_2)$ führt diese Entscheidung?

$$\boldsymbol{v_1} =$$

$$\boldsymbol{v_2} =$$

A1.5: SPC (5, 4) und BEC–Modell

$\underline{u}_0 = (0, 0, 0, 0)$	$\underline{x}_0 = (0, 0, 0, 0, 0)$
$\underline{u}_1 = (0, 0, 0, 1)$	$\underline{x}_1 = (0, 0, 0, 1, 1)$
$\underline{u}_2 = (0, 0, 1, 0)$	$\underline{x}_2 = (0, 0, 1, 0, 1)$
$\underline{u}_3 = (0, 0, 1, 1)$	$\underline{x}_3 = (0, 0, 1, 1, 0)$
$\underline{u}_4 = (0, 1, 0, 0)$	$\underline{x}_4 = (0, 1, 0, 0, 1)$
$\underline{u}_5 = (0, 1, 0, 1)$	$\underline{x}_5 = (0, 1, 0, 1, 0)$
$\underline{u}_6 = (0, 1, 1, 0)$	$\underline{x}_6 = (0, 1, 1, 0, 0)$
$\underline{u}_7 = (0, 1, 1, 1)$	$\underline{x}_7 = (0, 1, 1, 1, 1)$
$\underline{u}_8 = (1, 0, 0, 0)$	$\underline{x}_8 = (1, 0, 0, 0, 1)$
$\underline{u}_9 = (1, 0, 0, 1)$	$\underline{x}_9 = (1, 0, 0, 1, 0)$
$\underline{u}_{10} = (1, 0, 1, 0)$	$\underline{x}_{10} = (1, 0, 1, 0, 0)$
$\underline{u}_{11} = (1, 0, 1, 1)$	$\underline{x}_{11} = (1, 0, 1, 1, 1)$
$\underline{u}_{12} = (1, 1, 0, 0)$	$\underline{x}_{12} = (1, 1, 0, 0, 0)$
$\underline{u}_{13} = (1, 1, 0, 1)$	$\underline{x}_{13} = (1, 1, 0, 1, 1)$
$\underline{u}_{14} = (1, 1, 1, 0)$	$\underline{x}_{14} = (1, 1, 1, 0, 1)$
$\underline{u}_{15} = (1, 1, 1, 1)$	$\underline{x}_{15} = (1, 1, 1, 1, 0)$

Für diese Aufgabe wird vorausgesetzt:

- Der **Single Parity–check Code** mit $k = 4$ und $n = 5$ ⇒ SPC (5, 4) fügt zu den Informationsbits u_1, ... , u_4 ein Prüfbit p hinzu, so dass in jedem Codewort $\underline{x}$ eine gerade Anzahl von Einsen vorkommt:

$$x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 = 0,$$
$$u_1 \oplus u_2 \oplus u_3 \oplus u_4 \oplus p = 0.$$

- Der **Binary Erasure Channel** (BEC) – mit binären Eingangswerten $x_i \in \{0, 1\}$ und ternärem Ausgang $y_i \in \{0, 1, \text{E}\}$ führt mit Wahrscheinlichkeit $\lambda = 0.1$ zu einer Auslöschung (englisch: *Erasure*), abgekürzt mit „E". Weiterhin gilt $\Pr(y_i = x_i) = 1 - \lambda = 0.9$. Ein echter Übertragungsfehler wird ausgeschlossen:

$$\Pr[(x_i = 0) \cap (y_i = 1)] = \Pr[(x_i = 1) \cap (y_i = 0)] = 0.$$

Der Zusammenhang zwischen dem Informationswort $\underline{u}$ und dem Codewort $\underline{x}$ ist durch die obige Tabelle gegeben. Aus dem Empfangswort $\underline{y}$ wird durch Maximum–Likelihood–Entscheidung der Vektor $\underline{v}$ der Informationsbits an der Sinke gebildet, der möglichst mit dem Informationswort $\underline{u}$ übereinstimmen sollte. Es gelte die folgende Nomenklatur:

$$\underline{u} \in \{\underline{u}_0, \underline{u}_1, \ \cdots \ , \underline{u}_{15}\},$$
$$\underline{v} \in \{\underline{v}_0, \underline{v}_1, \ \cdots \ , \underline{v}_{15}, \underline{E}\}.$$

Das Ergebnis $\underline{v} = \underline{\text{E}}$ = (E, E, E, E) kennzeichnet dabei, dass aufgrund zu vieler Auslöschungen eine Decodierung des Codewortes nicht möglich ist.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 1.2** und das **Kapitel 1.3** des vorliegenden Buches. Die Prüfbits von $\underline{u}_0$, $\underline{u}_4$ und $\underline{u}_{13}$ sollen in der Teilaufgabe (a) ermittelt werden.

Fragebogen zu "A1.5: SPC (5, 4) und BEC–Modell"

a) Wie lautet für die folgenden Informationsworte $\underline{u}$ jeweils das Prüfbit p?

$$\underline{u} = \underline{u}_0\text{:} \quad p = \;$$

$$\underline{u} = \underline{u}_4\text{:} \quad p = \;$$

$$\underline{u} = \underline{u}_{13}\text{:} \quad p = \;$$

b) Es sei $\underline{y}$ = (0, 0, 0, 0, E). Welches Informationswort wurde gesendet?

- ☐ $\underline{u}_0$,
- ☐ $\underline{u}_4$,
- ☐ $\underline{u}_{13}$.

c) Es sei $\underline{y}$ = (0, E, 0, 0, 1). Welches Informationswort wurde gesendet?

- ☐ $\underline{u}_0$,
- ☐ $\underline{u}_4$,
- ☐ $\underline{u}_{13}$.

d) Mit welcher Wahrscheinlichkeit stimmt $\underline{y}$ mit dem Codewort $\underline{x}$ überein?

$$\mathrm{Pr}(\underline{y} = \underline{x}) = \;$$

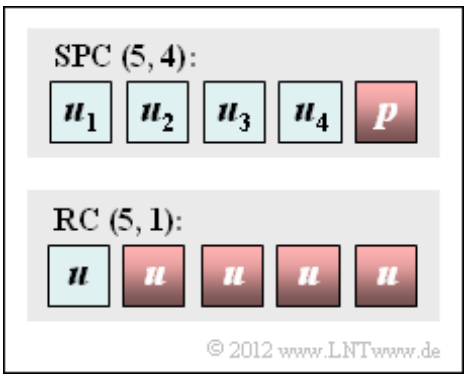
e) Mit welcher Wahrscheinlichkeit stimmen die beiden Vektoren $\underline{u}$ und $\underline{v}$ überein?

$$\mathrm{Pr}(\underline{v} = \underline{u}) = \;$$

f) Wie groß ist die Wahrscheinlichkeit für einen erkannten Fehler?

$$\mathrm{Pr}(\underline{v} = \underline{\mathrm{E}}) = \;$$

Z1.5: SPC (5, 4) vs. RC (5, 1)



Zwischen dem *Single Parity–check Code* und dem *Repetition Code* gleicher Codelänge n besteht eine gewisse Verwandtschaft. Wie im **Kapitel 1.4** noch gezeigt werden wird, handelt es sich um so genannte **duale Codes**.

- Der **Single Parity–check Code** mit $k = 4$ und $n = 5$ ⇒ SPC (5, 4) fügt zu den vier Informationsbits u_1, ... , u_4 ein Prüfbit p hinzu, so dass in jedem Codewort $\underline{x}$ eine gerade Anzahl von Einsen vorkommt:

$$x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 = 0 \quad \Rightarrow \quad u_1 \oplus u_2 \oplus u_3 \oplus u_4 \oplus p = 0 .$$

- Ein jeder **Wiederholungscode** (englisch: *Repetition Code*) ist durch den Codeparameter $k = 1$ charakterisiert. Beim RC (5, 1) lauten die beiden Codeworte (0, 0, 0, 0, 0) und (1, 1, 1, 1, 1).

Die Grafik zeigt die Grundstruktur dieser beiden Codes, die in dieser Aufgabe miteinander verglichen werden sollen.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 1.3** des vorliegenden Buches.

Fragebogen zu "Z1.5: SPC (5, 4) vs. RC (5, 1)"

a) Wie unterscheiden sich SPC (5, 4) und RC (5, 1) hinsichtlich Codeumfang?

SPC (5, 4): $|\boldsymbol{C}| =$

RC (5, 4): $|\boldsymbol{C}| =$

b) Welche der folgenden Codeworte sind beim SPC (5, 4) möglich?

- ☐ (0, 0, 0, 0, 0),
- ☐ (0, 0, 1, 0, 0),
- ☐ (1, 1, 0, 1, 1),
- ☐ (1, 1, 1, 1, 1).

c) Welche der folgenden Codeworte sind beim RC (5, 1) möglich?

- ☐ (0, 0, 0, 0, 0),
- ☐ (0, 0, 1, 0, 0),
- ☐ (1, 1, 0, 1, 1),
- ☐ (1, 1, 1, 1, 1).

d) Wieviele Codefolgen (N) müssen in die ML–Entscheidung einbezogen werden?

SPC (5, 4): $\boldsymbol{N} =$

RC (5, 1): $\boldsymbol{N} =$

e) Wie groß ist die minimale Distanz beider Codes?

SPC (5, 4): $\boldsymbol{d_{min}} =$

RC (5, 1): $\boldsymbol{d_{min}} =$

f) Bis zu wievielen Bitfehlern (e) funktioniert die Fehlererkennung?

SPC (5, 4): $\boldsymbol{e} =$

RC (5, 1): $\boldsymbol{e} =$

g) Bis zu wievielen Bitfehlern (t) funktioniert die Fehlerkorrektur?

SPC (5, 4): $\boldsymbol{t} =$

RC (5, 1): $\boldsymbol{t} =$

A1.6: Zum (7, 4)–Hamming–Code

1962 hat **Richard Wesley Hamming** eine Klasse binärer Blockcodes angegeben, die sich durch die Anzahl m der zugeführten Prüfbits unterscheiden. Die Codewortlänge ist bei diesen Codes stets $n = 2^m - 1$ und das Informationswort besteht aus $k = n - m$ Bit:

$m = 2$: (3, 1) Hamming–Code, ⇒ **RC (3, 1),**

$m = 3$: (7, 4) Hamming–Code,

$m = 4$: (15, 11) Hamming–Code,

$m = 5$: (31, 26) Hamming–Code, usw.

Im Verlaufe dieser Aufgabe gibt es Fragen

- zum Codeumfang $|C|$,
- zur Coderate R, und
- zur minimalen Distanz d_{min}

i	$\underline{u}_i$	$\underline{x}_i$
0	(0, 0, 0, 0)	(0, 0, 0, 0, 0, 0, 0)
1	(0, 0, 0, 1)	(0, 0, 0, 1, 1, 1, 1)
2	(0, 0, 1, 0)	(0, 0, 1, 0, 0, 1, 1)
3	(0, 0, 1, 1)	(0, 0, 1, 1, 1, 0, 0)
4	(0, 1, 0, 0)	(0, 1, 0, 0, 1, 1, 0)
5	(0, 1, 0, 1)	(0, 1, 0, 1, 0, 0, 1)
6	(0, 1, 1, 0)	(0, 1, 1, 0, 1, 0, 1)
7	(0, 1, 1, 1)	(0, 1, 1, 1, 0, 1, 0)
8	(1, 0, 0, 0)	(1, 0, 0, 0, 1, 0, 1)
9	(1, 0, 0, 1)	(1, 0, 0, 1, 0, 1, 0)
10	(1, 0, 1, 0)	(1, 0, 1, 0, 1, 1, 0)
11	(1, 0, 1, 1)	(1, 0, 1, 1, 0, 0, 1)
12	(1, 1, 0, 0)	(1, 1, 0, 0, 0, 1, 1)
13	(1, 1, 0, 1)	(1, 1, 0, 1, 1, 0, 0)
14	(1, 1, 1, 0)	(1, 1, 1, 0, 0, 0, 0)
15	(1, 1, 1, 1)	(1, 1, 1, 1, 1, 1, 1)

dieser Codeklasse. Weiterhin soll geklärt werden, ob der für diese Aufgabe durch seine Codetabelle $\underline{u}_i$ ⇒ $\underline{x}_i$ gegebene (7, 4)–Hamming–Code systematisch ist, und ob es sich um einen so genannten „perfekten Code" handelt. Der Laufindex kann hierbei die Werte $i = 1, \ldots, 2^k = 16$ annehmen.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 1.3.** Genaueres zu den Hamming–Codes finden Sie auf folgenden Seiten:

- **Hamming–Codes (1),**
- **Hamming–Codes (2),**
- **Einige Eigenschaften des (7, 4, 3)–Hamming–Codes.**

Für diesen Hamming–Code wurden andere Prüfgleichungen herangezogen als im **Theorieteil.** Deshalb unterscheiden sich auch die Codetabellen. In der **Aufgabe A1.7,** bei der der gleiche Code verwendet wird, ist das Schaubild der Prüfgleichungen angegeben.

Man spricht von einem perfekten Code, wenn folgende Bedingung erfüllt ist:

$$2^k = \frac{2^n}{\sum_{f=0}^{t} \binom{n}{f}} \quad \Rightarrow \quad 2^m = \sum_{f=0}^{t} \binom{n}{f}.$$

Hierbei bezeichnet t die Anzahl der korrigierbaren Fehler. Bei ungerader Minimaldistanz d_{min} gilt:

$$t = \frac{d_{min} - 1}{2}.$$

Die Interpretation zu dieser Bedingung finden Sie in der Musterlösung zu dieser Aufgabe.

Fragebogen zu "A1.6: Zum (7, 4)–Hamming–Code"

a) Geben Sie die Kenngrößen des gegebenen Codes C an:

$|C| =$

$k =$

$n =$

$R =$

b) Handelt es sich um einen systematischen Code?

- ○ Ja,
- ○ Nein.

c) Wie groß ist die minimale Distanz zwischen zwei beliebigen Codeworten?

$d_{min} =$

d) Wieviele Übertragungsfehler können erkannt (e) bzw. korrigiert (t) werden?

$e =$

$t =$

e) Ist der hier betrachtete Hamming–Code perfekt?

- ○ Ja,
- ○ Nein.

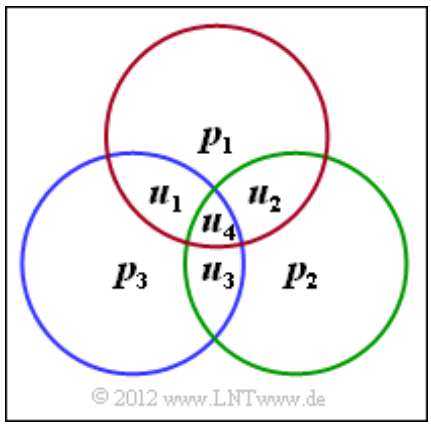
f) Welche Aussagen gelten hinsichtlich eines perfekten Codes?

- ☐ Ein perfekter Code führt stets zu Pr(Blockfehler) = 0.
- ☐ Alle Empfangsworte $\underline{y}$ sind einem gültigen Codewort zuordbar.
- ☐ Bei perfekten Codes ist die minimale Hamming–Distanz ungerade.

g) Welche der nachfolgend genannten Codes sind perfekt?

- ☐ (15,11)–Hamming–Code,
- ☐ (63,57)–Hamming–Code,
- ☐ (3,1)–Repetition Code,
- ☐ (4,1)–Repetition Code,
- ☐ (5,1)–Repetition Code.

A1.7: H und G des (7, 4)–Hamming–Codes



Die Grafik zeigt die Prüfgleichungen des (7, 4, 3)–Hamming–Codes, der bereits in der **Aufgabe A1.6** eingehend betrachtet und anhand der Codetabelle beschrieben wurde.

In dieser Aufgabe wird dieser Code – wie in der Kanalcodierung allgemein üblich – nun durch zwei Matrizen charakterisiert:

- Die Prüfmatrix **H** ist eine Matrix mit $m = n - k$ Zeilen und n Spalten. Sie beschreibt die $m = 3$ Prüfgleichungen, wobei sich die erste Zeile auf die Elemente des roten Kreises und die zweite Zeile auf die des grünen Kreises bezieht. Die letzte Zeile gibt die Modulo–2–Summe des blauen Kreises wieder.
- Eine zweite Beschreibungsmöglichkeit bietet die Generatormatrix **G**, mit k Zeilen und n Spalten. Sie gibt den Zusammenhang zwischen den Informationsworten $\underline{u}$ und den Codeworten $\underline{x}$ an:

$$\underline{x} = \underline{u} \cdot \mathbf{G}.$$

Daraus und aus der Gleichung $\mathbf{H} \cdot \underline{x}^{\rm T} = \mathbf{0}$ kann der Zusammenhang zwischen der Prüfmatrix **H** und der Generatormatrix **G** hergestellt werden:

$$\underline{x}^{\rm T} = \mathbf{G}^{\rm T} \cdot \underline{u}^{\rm T} \quad \Rightarrow \quad \mathbf{H} \cdot \mathbf{G}^{\rm T} \cdot \underline{u}^{\rm T} = \underline{0} \quad \forall\, \underline{u} \in {\rm GF}(2^k)$$

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

Anzumerken ist, dass in diesen Gleichungen $\underline{0}$ einen Zeilenvektor mit k Elementen bezeichnet und $\mathbf{0}$ eine Matrix mit m Zeilen und k Spalten. Alle Elemente von $\underline{0}$ bzw. $\mathbf{0}$ sind identisch 0.

Handelt es sich um einen **systematischen Code,** so können die beiden Beschreibungsgrößen **H** und **G** unter Zuhilfenahme von *Einheitsmatrizen* wie folgt geschrieben werden:

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

P ist dabei eine Matrix mit k Zeilen und m Spalten. Dementsprechend besitzt die transponierte Matrix $\mathbf{P}^{\rm T}$ m Zeilen und k Spalten.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 1.4.**

Fragebogen zu "A1.7: H und G des (7, 4)–Hamming–Codes"

a) Welches Format hat die Prüfmatrix?

H: Spaltenzahl =

H: Zeilenzahl =

b) Welche Aussagen hinsichtlich der Prüfmatrix **H** sind zutreffend?

- ☐ Die erste Zeile lautet: 1101100.
- ☐ Die zweite Zeile lautet: 0111010.
- ☐ Die dritte Zeile lautet: 1011001.

c) Woran erkennt man, dass ein systematischer Code vorliegt?

- ☐ In jeder Zeile gibt es eine gerade Anzahl von Einsen.
- ☐ Am Ende von **H** erkennt man eine Einheitsmatrix.
- ☐ Die mittlere Spalte von **H** ist mit Einsen besetzt.

d) Geben Sie die Generatormatrix **G** an. Welche Aussagen stimmen?

- ☐ Die erste Zeile lautet: 1000101,
- ☐ Die zweite Zeile lautet: 0111010,
- ☐ Die letzte Zeile lautet: 0001111.

e) Welches Codewort $\underline{x}_{11}$ ergibt sich für $\underline{u}_{11} = (1, 0, 1, 1)$?

- ☐ $\underline{x}_{11} = (1, 1, 1, 1, 0, 0, 0)$,
- ☐ $\underline{x}_{11} = (1, 0, 1, 1, 0, 0, 0)$,
- ☐ $\underline{x}_{11} = (1, 0, 1, 1, 0, 0, 1)$.

Z1.7: Klassifizierung von Blockcodes

Code 1:
$\{(0,0,0,0), (0,0,1,1), (0,1,0,1), (0,1,1,0), (1,0,0,1), (1,0,1,0), (1,1,0,0), (1,1,1,1)\}$

Code 2:
$\{(0,0,0,0), (1,1,1,1)\}$

Code 3:
$\{(0,0,0,0), (0,1,1,0), (1,0,0,1), (1,1,1,1)\}$

Code 4:
$\{(0,0,0,0), (0,0,1,1), (1,1,0,0), (1,1,1,1)\}$

Code 5:
$\{(0,0,1,1), (0,1,0,1), (0,1,1,0), (1,0,0,1), (1,0,1,0), (1,1,0,0)\}$

Wir betrachten Blockcodes der Länge $n = 4$:

- den **Single Parity–check Code** SPC (4, 3) mit

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

- den **Wiederholungscode** RC (4, 1) mit der Prüfmatrix

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

- den (4, 2)–Blockcode mit der Generatormatrix

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

- den (4, 2)–Blockcode mit der Generatormatrix

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

- einen weiteren Code mit dem Codeumfang $|C| = 6$.

Diese Codes werden im Folgenden mit Code 1, ... , Code 5 bezeichnet. In der Grafik sind die einzelnen Codes explizit angegegeben.

Bei den Fragen zu diesen Aufgaben geht es um die Begriffe

- **lineare Codes,**
- **systematische Codes,**
- **duale Codes.**

Hinweis: Die Aufgabe gehört zum Themengebiet von **Kapitel 1.4.**

Fragebogen zu "Z1.7: Klassifizierung von Blockcodes"

a) Wie lässt sich Code 5 beschreiben?

- ☐ In jedem Codewort sind genau 2 Nullen enthalten.
- ☐ In jedem Codewort sind genau 2 Einsen enthalten.
- ☐ Nach jeder 0 sind die Symbole 0 und 1 gleichwahrscheinlich.

b) Welche der folgenden Blockcodes sind linear?

- ☐ Code 1,
- ☐ Code 2,
- ☐ Code 3,
- ☐ Code 4,
- ☐ Code 5.

c) Welche der folgenden Blockcodes sind systematisch?

- ☐ Code 1,
- ☐ Code 2,
- ☐ Code 3,
- ☐ Code 4,
- ☐ Code 5.

d) Welche Codepaare sind zueinander dual?

- ☐ Code 1 und Code 2,
- ☐ Code 2 und Code 3,
- ☐ Code 3 und Code 4.

A1.8: Identische Codes

Wir betrachten einen Blockcode C, der durch folgende Generatormatrix beschrieben wird:

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

$\underline{u}_0 = (0, 0, 0)$	$\underline{x}_0 = (0, 0, 0, 0, 0, 0)$
$\underline{u}_1 = (0, 0, 1)$	$\underline{x}_1 = (0, 1, 1, 1, 1, 0)$
$\underline{u}_2 = (0, 1, 0)$	$\underline{x}_2 = (1, 0, 0, 1, 1, 0)$
$\underline{u}_3 = (0, 1, 1)$	$\underline{x}_3 = (1, 1, 1, 0, 0, 0)$
$\underline{u}_4 = (1, 0, 0)$	$\underline{x}_4 = (0, 0, 1, 0, 1, 1)$
$\underline{u}_5 = (1, 0, 1)$	$\underline{x}_5 = (0, 1, 0, 1, 0, 1)$
$\underline{u}_6 = (1, 1, 0)$	$\underline{x}_6 = (1, 0, 1, 1, 0, 1)$
$\underline{u}_7 = (1, 1, 1)$	$\underline{x}_7 = (1, 1, 0, 0, 1, 1)$

Die Zuordnung zwischen den Informationsworten $\underline{u}$ und den Codeworten $\underline{x}$ kann der beiliegenden Tabelle entnommen werden. Man erkennt, dass es sich dabei nicht um einen systematischen Code handelt.

Durch Manipulation der Generatormatrix $\mathbf{G}$ lassen sich daraus identische Codes konstruieren. Darunter versteht man Codes mit gleichen Codeworten, jedoch unterschiedlicher Zuordnung $\underline{u} \rightarrow \underline{x}$. Folgende Operationen sind erlaubt, um einen identischen Code zu erhalten:

- Vertauschen oder Permutieren der Zeilen,
- Multiplizieren aller Zeilen mit einem konstanten Vektor ungleich 0,
- Ersetzen einer Zeile durch eine Linearkombination zwischen dieser Zeile und einer anderen.

Für den in der Teilaufgabe c) gesuchten Code $C_{\rm sys}$ ⇒ Generatormatrix $\mathbf{G}_{\rm sys}$ wird weiter gefordert, dass er systematisch ist.

Hinweis: Die Aufgabe bezieht sich vorwiegend auf die Seite **Systematische Codes** im **Kapitel 1.4.** Bezug genommen wird zudem auf die so genannte *Singleton–Schranke*. Diese besagt, dass die minimale Hamming–Distanz eines (n, k)–Blockcodes nach oben beschränkt ist:

$$d_{\rm min} \le n - k + 1.$$

Fragebogen zu "A1.8: Identische Codes"

a) Geben Sie die Kenngrößen des gegebenen Codes C an.

$$\boldsymbol{n} =$$

$$\boldsymbol{k} =$$

$$|\boldsymbol{C}| =$$

$$\boldsymbol{R} =$$

$$\boldsymbol{m} =$$

$$\boldsymbol{d}_{\rm min} =$$

b) Gibt es einen (6, 3)–Blockcode mit größerer Minimaldistanz?

- ○ Ja.
- ○ Nein.

c) Wie lautet die Generatormatrix $\mathbf{G}_{\rm sys}$ des identischen systematischen Codes?

- ☐ Die 1. Zeile lautet „1 0 1 1 0 1”.
- ☐ Die 2. Zeile lautet „0 1 0 1 0 1”.
- ☐ Die 3. Zeile lautet „0 0 1 0 1 1”.

d) Welche Zuordnungen ergeben sich bei dieser Codierung?

- ☐ $\underline{u} = (0, 0, 0) \Rightarrow \underline{x}_{\rm sys} = (0, 0, 0, 0, 0, 0)$.
- ☐ $\underline{u} = (0, 0, 1) \Rightarrow \underline{x}_{\rm sys} = (0, 0, 1, 0, 0, 1)$.
- ☐ $\underline{u} = (0, 1, 0) \Rightarrow \underline{x}_{\rm sys} = (0, 1, 0, 1, 1, 0)$.

e) Welche Prüfbits hat der systematische Code $\underline{x}_{\rm sys} = (u_1, u_2, u_3, p_1, p_2, p_3)$?

- ☐ $p_1 = u_1 \oplus u_2$,
- ☐ $p_2 = u_2 \oplus u_3$,
- ☐ $p_3 = u_1 \oplus u_3$.

Z1.8: Äquivalente Codes

Info	Code A	Code B
0 0 0	0 0 0 0 0 0	0 0 0 0 0 0
0 0 1	0 0 1 0 1 1	0 1 1 1 1 0
0 1 0	0 1 0 1 0 1	1 0 0 1 1 0
0 1 1	0 1 1 1 1 0	1 1 1 0 0 0
1 0 0	1 0 0 1 1 0	0 0 1 0 1 1
1 0 1	1 0 1 1 0 1	0 1 0 1 0 1
1 1 0	1 1 0 0 1 1	1 0 1 1 0 1
1 1 1	1 1 1 0 0 0	1 1 0 0 1 1

Info	Code C	Code D
0 0 0	0 0 0 0 0 0	0 0 0 0 0 0
0 0 1	0 0 1 1 1 1	0 0 1 0 1 0
0 1 0	0 1 0 0 1 1	0 1 0 1 0 0
0 1 1	0 1 1 0 0 0	0 1 1 1 1 0
1 0 0	1 0 0 1 0 1	1 0 0 1 0 1
1 0 1	1 0 1 0 1 0	1 0 1 1 1 1
1 1 0	1 1 0 1 1 0	1 1 0 0 0 1
1 1 1	1 1 1 0 0 1	1 1 1 0 1 1

In der Grafik sind die Zuordnungen $\underline{u} \rightarrow \underline{x}$ für verschiedene Codes angegeben, die im Folgenden jeweils durch die Generatormatrix **G** und die Prüfmatrix **H** charakterisiert werden:

- **Code A:**

$$\mathbf{G}_{\rm A} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

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

- **Code B:**

$$\mathbf{G}_{\rm B} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

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

- **Code C:**

$$\mathbf{G}_{\rm C} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \qquad \mathbf{H}_{\rm C} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

- **Code D:**

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

In dieser Aufgabe soll untersucht werden, welche dieser Codes bzw. Codepaare

- systematisch sind,
- identisch sind (das heißt: Verschiedene Codes haben gleiche Codeworte),
- äquivalent sind (das heißt: Verschiedene Codes haben gleiche Codeparameter).

Hinweis: Die Aufgabe gehört zum Themengebiet von **Kapitel 1.4.** Anzumerken ist, dass die Angabe einer Prüfmatrix **H** nicht eindeutig ist. Verändert man die Reihenfolge der Prüfgleichungen, so entspricht dies einer Vertauschung von Zeilen.

Fragebogen zu "Z1.8: Äquivalente Codes"

a) Welche der nachfolgend aufgeführten Codes sind systematisch?

- ☐ Code A,
- ☐ Code B,
- ☐ Code C,
- ☐ Code D.

b) Welche der vorgegebenen Codepaare sind identisch?

- ☐ Code A und Code B,
- ☐ Code B und Code C,
- ☐ Code C und Code D.

c) Welche der gegebenen Codepaare sind äquivalent, aber nicht identisch?

- ☐ Code A und Code B,
- ☐ Code B und Code C,
- ☐ Code C und Code D.

d) Wie unterscheiden sich die Generatormatrizen $G_{\rm B}$ und $G_{\rm C}$?

- ☐ Durch verschiedene Linearkombinationen verschiedener Zeilen.
- ☐ Durch zyklische Vertauschung der Zeilen um 1 nach unten.
- ☐ Durch zyklische Vertauschung der Spalten um 1 nach rechts.

e) Bei welchen Codes gilt $\mathbf{H} \cdot \mathbf{G}^{\rm T} = \mathbf{0}$?

- ☐ Code A,
- ☐ Code B,
- ☐ Code C,
- ☐ Code D.

A1.9: Erweiterter Hamming–Code

Es sollen zwei Codes miteinander verglichen werden, deren Codetabellen rechts angegeben sind. Die ersten vier Bit eines jeden Codewortes $\underline{x}$ geben das jeweilige Informationswort $\underline{u}$ wider (schwarze Schrift). Danach folgen $m = n - k$ Prüfbit (rote Schrift).

Codeworte von C_1 Hamming-Code (7, 4)	Codeworte von C_2 HC erweitert auf (8, 4)
(0, 0, 0, 0, 0, 0, 0)	(0, 0, 0, 0, 0, 0, 0, 0)
(0, 0, 0, 1, 1, 1, 1)	(0, 0, 0, 1, 1, 1, 1, 0)
(0, 0, 1, 0, 0, 1, 1)	(0, 0, 1, 0, 0, 1, 1, 1)
(0, 0, 1, 1, 1, 0, 0)	(0, 0, 1, 1, 1, 0, 0, 1)
(0, 1, 0, 0, 1, 1, 0)	(0, 1, 0, 0, 1, 1, 0, 1)
(0, 1, 0, 1, 0, 0, 1)	(0, 1, 0, 1, 0, 0, 1, 1)
(0, 1, 1, 0, 1, 0, 1)	(0, 1, 1, 0, 1, 0, 1, 0)
(0, 1, 1, 1, 0, 1, 0)	(0, 1, 1, 1, 0, 1, 0, 0)
(1, 0, 0, 0, 1, 0, 1)	(1, 0, 0, 0, 1, 0, 1, 1)
(1, 0, 0, 1, 0, 1, 0)	(1, 0, 0, 1, 0, 1, 0, 1)
(1, 0, 1, 0, 1, 1, 0)	(1, 0, 1, 0, 1, 1, 0, 0)
(1, 0, 1, 1, 0, 0, 1)	(1, 0, 1, 1, 0, 0, 1, 0)
(1, 1, 0, 0, 0, 1, 1)	(1, 1, 0, 0, 0, 1, 1, 0)
(1, 1, 0, 1, 1, 0, 0)	(1, 1, 0, 1, 1, 0, 0, 0)
(1, 1, 1, 0, 0, 0, 0)	(1, 1, 1, 0, 0, 0, 0, 1)
(1, 1, 1, 1, 1, 1, 1)	(1, 1, 1, 1, 1, 1, 1, 1)

- Der systematische (7, 4)–Hamming–Code wurde bereits in **Aufgabe A1.6** sowie **Aufgabe A1.7** behandelt. Prüfmatrix und Generatormatrix dieses Codes sind wie folgt gegeben:

$$\mathbf{H}_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

$$\mathbf{G}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

  Im weiteren Verlauf der Aufgabe wird dieser (gelb hinterlegte) Code C_1 genannt.

- Die rechte Spalte in obiger Tabelle gibt einen Blockcode mit den Parametern $n = 8$ und $k = 4$ an, der in der Literatur meist als „erweiteter Hamming–Code" bezeichnet wird. Wir nennen diesen (grün hinterlegten) Code im Folgenden C_2 und bezeichnen dessen Prüfmatrix mit $\mathbf{H}_2$ und die dazugehörige Generatormatrix mit $\mathbf{G}_2$.

Die Fragen zu dieser Aufgabe beziehen sich auf

- die **Coderate,**
- die **minimale Distanz** zwischen zwei Codeworten,
- die **Prüfmatrix** und die **Generatormatrix** des erweiterten (8, 4)–Hamming–Codes.

Hinweis: Die Aufgabe gehört zu **Kapitel 1.4.** Beachten Sie bei der Lösung, dass C_1 und C_2 jeweils **systematische Codes** sind. Die nachfolgende **Aufgabe Z1.9** behandelt die Erweiterung von Codes in etwas allgemeinerer Form.

Fragebogen zu "A1.9: Erweiterter Hamming–Code"

a) Geben Sie die Coderaten von C_1 und C_2 an.

$$\boldsymbol{C_1}\text{:}\quad \boldsymbol{R} =$$

$$\boldsymbol{C_2}\text{:}\quad \boldsymbol{R} =$$

b) Geben Sie die minimalen Distanzen von C_1 und C_2 an.

$$\boldsymbol{C_1}\text{:}\quad \boldsymbol{d_{min}} =$$

$$\boldsymbol{C_2}\text{:}\quad \boldsymbol{d_{min}} =$$

c) Welches Format besitzt die Prüfmatrix von C_2?

$$\mathbf{H_2}\text{:}\quad \textbf{Spaltenzahl} =$$

$$\mathbf{H_2}\text{:}\quad \textbf{Zeilenzahl} =$$

d) Leiten Sie aus der Codetabelle die Gleichung für das Codebit x_8 (= p_4) ab.

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

e) Welche Aussagen gelten für $\mathbf{H}_2$? *Hinweis:* Richtig sind 3 von 4 Antworten.

- ☐ Die erste Zeile lautet: 1 1 0 1 1 0 0 0.
- ☐ Die zweite Zeile lautet: 0 1 1 1 0 1 0 0.
- ☐ Die dritte Zeile lautet: 0 0 0 0 1 1 1 1.
- ☐ Die letzte Zeile lautet: 1 1 1 1 1 1 1 1.

f) Welche Umformung ist für die letzte Zeile von $\mathbf{H}_2$ zulässig?

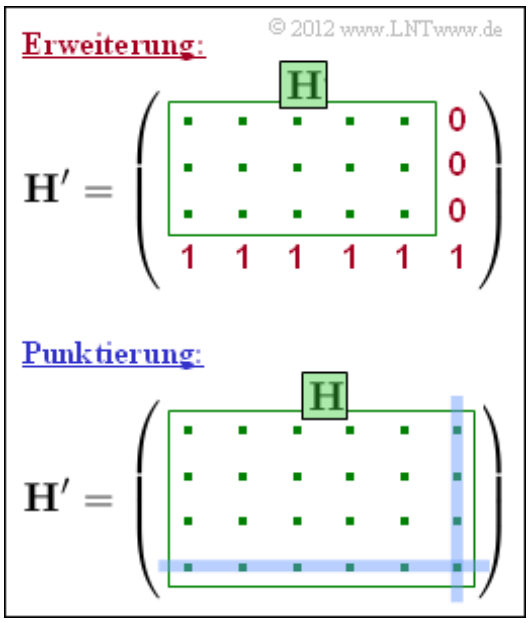
- ☐ 1 1 1 1 1 1 1 1 → 0 0 0 0 0 0 0 0,
- ☐ 1 1 1 1 1 1 1 1 → 1 1 1 0 0 0 0 1,
- ☐ 1 1 1 1 1 1 1 1 → 0 0 1 0 1 0 0 0.

g) Geben Sie die zugehörige Generatormatrix $\mathbf{G}_2$ an. Welche Aussagen treffen zu?

- ☐ $\mathbf{G}_2$ hat gleiches Format wie die Matrix $\mathbf{G}_1$ des (7, 4)–Codes.
- ☐ $\mathbf{G}_2$ beginnt wie $\mathbf{G}_1$ mit einer Diagonalmatrix $\mathbf{I}_4$.

- $\mathbf{G}_2$ hat im betrachteten Beispiel das gleiche Format wie $\mathbf{H}_2$.

Z1.9: Erweiterung – Punktierung



Häufig kennt man einen Code, der für eine Anwendung als geeignet erscheint, dessen Coderate aber nicht exakt mit den Vorgaben übereinstimmt.

Zur Ratenanpassung gibt es verschiedene Möglichkeiten:

- **Erweiterung** (englisch *Extension*): Ausgehend vom (n, k)–Code, dessen Prüfmatrix **H** gegeben ist, erhält man einen (n+1, k)–Code, indem man die Prüfmatrix um eine Zeile und eine Spalte erweitert und die neuen Matrixelemente entsprechend der oberen Grafik mit Nullen und Einsen ergänzt. Man fügt ein neues Prüfbit

$$x_{n+1} = x_1 \oplus x_2 \oplus \ldots \oplus x_n$$

  hinzu und damit auch eine neue Prüfgleichung, die in **H'** berücksichtigt ist.

- **Punktierung** (englisch *Puncturing*): Entsprechend der unteren Abbildung kommt man zu einem (n–1, k)–Code größerer Rate, wenn man auf ein Prüfbit und eine Prüfgleichung verzichtet, was gleichbedeutend damit ist, aus der Prüfmatrix **H** eine Zeile und eine Spalte zu streichen.

- **Verkürzung** (englisch *Shortening*): Verzichtet man anstelle eines Prüfbits auf ein Informationsbit, so ergibt sich ein (n–1, k–1)–Code kleinerer Rate.

In dieser Aufgabe sollen ausgehend von einem (5, 2)–Blockcode

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

folgende Codes konstruiert und analysiert werden:

- ein (6, 2)–Code durch einmalige Erweiterung,
- ein (7, 2)–Code durch nochmalige Erweiterung,
- ein (4, 2)–Code durch Punktierung.

Die Prüfmatrix und die Generatormatrix des systematischen (5, 2)–Codes lauten:

$$\mathbf{H}_{(5,2)} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad \Leftrightarrow \quad \mathbf{G}_{(5,2)} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 1.4.** In der **Aufgabe A1.9** wird beispielhaft gezeigt, wie aus dem (7, 4, 3)–Hamming–Code durch Erweiterung ein (8, 4, 4)–Code entsteht.

Fragebogen zu "Z1.9: Erweiterung – Punktierung"

a) Geben Sie die Kenngrößen des vorgegebenen (5, 2)–Codes an.

(5, 2)–Code: R =

$d_{\rm min}$ =

b) Welche Codeworte besitzt der (6, 2)–Code nach Erweiterung?

☐ (0 0 0 0 0 1), (0 1 0 1 1 0), (1 0 1 1 0 0), (1 1 1 0 1 1).

☐ (0 0 0 0 0 0), (0 1 0 1 1 1), (1 0 1 1 0 1), (1 1 1 0 1 0).

c) Geben Sie die Kenngrößen des erweiterten (6, 2)–Codes an.

(6, 2)–Code: R =

$d_{\rm min}$ =

d) Wie lautet die systematische Generatormatrix des (7, 2)–Codes?

☐ Zeile 1 von **G**: 1, 0, 1, 1, 0, 1, 0.

☐ Zeile 2 von **G**: 0, 1, 0, 1, 1, 1, 0.

e) Geben Sie die Kenngrößen des erweiterten (7, 2)–Codes an.

(7, 2)–Code: R =

$d_{\rm min}$ =

f) Welche Aussagen gelten für den (4, 2)–Code (Punktierung des letzten Prüfbits)?

☐ Die Coderate beträgt nun $R = 2/4 = 0.5$.

☐ $C_{(4,\ 2)} = \{(0, 0, 0, 0),\ (1, 0, 1, 1),\ (0, 1, 0, 1),\ (1, 1, 1, 0)\}$.

☐ Die Minimaldistanz bleibt gegenüber dem (5, 2)–Code gleich.

A1.10: Einige Generatormatrizen

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

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

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

Wir betrachten nun verschiedene Binärcodes einheitlicher Länge n. Alle Codes der Form

$$\underline{x} = (x_1, x_2, \ldots, x_n),$$
$$x_i \in \{0, 1\}, \quad i = 1, \ldots, n$$

lassen sich in einem n–dimensionalen Vektorraum darstellen und interpretieren ⇒ GF(2^n).

Durch eine $k \times n$–Generatormatrix **G** (also eine Matrix mit k Zeilen und n Spalten) ergibt sich ein (n, k)–Code, allerdings nur dann, wenn der Rang (englisch: *Rank*) der Matrix **G** ebenfalls gleich k ist. Weiter gilt:

- Jeder Code C spannt einen k–dimensionalen linearen Untervektorraum des Galoisfeldes GF(2^n) auf.
- Als Basisvektoren dieses Untervektorraums können k unabhängige Codeworte von C verwendet werden. Eine weitere Einschränkung gibt es für die Basisvektoren nicht.
- Die Prüfmatrix **H** spannt ebenfalls einen Untervektorraum von GF(2^n) auf. Dieser hat aber die Dimension $m = n - k$ und ist orthogonal zum Untervektorraum, der auf **G** basiert.
- Bei einem linearen Code gilt $\underline{x} = \underline{u} \cdot \mathbf{G}$, wobei $\underline{u} = (u_1, u_2, \ldots, u_k)$ das Informationswort angibt. Ein systematischer Code liegt vor, wenn $x_1 = u_1, \ldots, x_k = u_k$ gilt.
- Bei einem systematischen Code besteht ein einfacher Zusammenhang zwischen **G** und **H**. Nähere Angaben hierzu finden Sie im **Theorieteil.**

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 1.4.** Für die gesamte Aufgabe gilt $n = 6$. In der Teilaufgabe (d) soll geklärt werden, welche der Matrizen $\mathbf{G}_A$, $\mathbf{G}_B$ bzw. $\mathbf{G}_C$ zu einem (6, 3)–Blockcode mit den nachfolgend aufgeführten Codeworten führen:

$$\mathcal{C}_{(6,3)} = \{ (0,0,0,0,0,0),\ (0,0,1,0,1,1),\ (0,1,0,1,0,1),\ (0,1,1,1,1,0),$$
$$(1,0,0,1,1,0),\ (1,0,1,1,0,1),\ (1,1,0,0,1,1),\ (1,1,1,0,0,0)\}\ .$$

Fragebogen zu "A1.10: Einige Generatormatrizen"

a) Bekannt sind nur die zwei Codeworte (0, 1, 0, 1, 0, 1) und (1, 0, 0, 1, 1, 0) eines linearen Codes. Welche Aussagen sind zutreffend?

- ☐ Es könnte sich um einen (5, 2)–Code handeln.
- ☐ Es könnte sich um einen (6, 2)–Code handeln.
- ☐ Es könnte sich um einen (6, 3)–Code handeln.

b) Wie lauten die Codeworte des linearen (6, 2)–Codes explizit?

- ☐ (0 0 1 0 1 1), (0 1 0 1 0 1), (1 0 0 1 1 0), (1 1 0 0 1 1).
- ☐ (0 0 0 0 0 0), (0 1 0 1 0 1), (1 0 0 1 1 0), (1 1 0 0 1 1).
- ☐ (0 0 0 0 0 0), (0 1 0 1 0 1), (1 0 0 1 1 0), (1 1 1 0 0 0).

c) Welche Aussagen gelten für diesen (6, 2)–Code C?

- ☐ Für alle Codeworte ($i = 1, \ldots, 4$) gilt $\underline{x}_i \in \mathrm{GF}(2^6)$.
- ☐ C ist ein 2–dimensionaler linearer Untervektorraum von $\mathrm{GF}(2^6)$.
- ☐ $\mathbf{G}$ gibt Basisvektoren dieses Untervektorraumes $\mathrm{GF}(2^2)$ an.
- ☐ $\mathbf{G}$ und $\mathbf{H}$ sind jeweils 2×6–Matrizen.

d) Welche der Generatormatrizen (siehe Grafik) führen zu einem (6, 3)–Code?

- ☐ Generatormatrix $\mathbf{G}_\mathrm{A}$,
- ☐ Generatormatrix $\mathbf{G}_\mathrm{B}$,
- ☐ Generatormatrix $\mathbf{G}_\mathrm{C}$.

A1.11: Syndromdecodierung

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

Zur Decodierung eines (7, 4, 3)–Hamming–Codes, der durch seine Prüfmatrix

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

gegeben ist, eignet sich auch die *Syndromdecodierung*. Da alle Hamming–Codes perfekt sind, ergibt sich hiermit ein gleich gutes Ergebnis wie mit der (im allgemeinen Fall) komplizierteren Maximum–Likelihood–Detektion.

Bei der **Syndromdecodierung** geht man wie folgt vor:

- Man bildet aus dem Empfangsvektor $\underline{y}$ das Syndrom (es gilt $m = n - k$):

$$\underline{s} = \underline{y} \cdot \mathbf{H}^{\rm T} \in {\rm GF}(2^m) .$$

- Beim **BSC–Kanal** ist auch das Empfangswort $\underline{y} = \underline{x}$ (Codewort) + $\underline{e}$ (Fehlervektor) ein Element von GF (2^n), und es gilt wegen $\underline{x} \cdot \mathbf{H}^{\rm T} = \underline{0}$ gleichermaßen:

$$\underline{s} = \underline{e} \cdot \mathbf{H}^{\rm T} .$$

- Viele Fehlermuster $\underline{e}$ führen zum gleichen Syndrom $\underline{s}$. Man fasst nun diejenigen Fehlermuster mit dem gleichen Syndrom $\underline{s}_\mu$ zur Nebenklasse Ψ_μ zusammen.

- Als Nebenklassenanführer $\underline{e}_\mu$ bezeichnet man denjenigen Fehlervektor, der innerhalb der Klasse Ψ_μ das geringste Hamming–Gewicht aufweist und dementsprechend am wahrscheinlichsten ist.

Die obige Grafik zeigt die unvollständige Liste der Nebenklassenanführer $\underline{e}_\mu$ für die einzelnen $\underline{s}_\mu$. Die wahrscheinlichsten Fehlervektoren

- $\underline{e}_3$ mit Syndrom $\underline{s}_3 = (0, 1, 1)$,
- $\underline{e}_5$ mit Syndrom $\underline{s}_5 = (1, 0, 1)$,
- $\underline{e}_6$ mit Syndrom $\underline{s}_6 = (1, 1, 0)$,
- $\underline{e}_7$ mit Syndrom $\underline{s}_7 = (1, 1, 1)$

sollen in den Teilaufgaben d) und e) ermittelt werden.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 1.5.** Zugrunde liegt ein Hamming–Code mit den Parametern $n = 7$ und $k = 4 \;\Rightarrow\; m = 3$. Alle Codeworte haben folgendes Format:

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

Die Prüfgleichungen sind auf dem Angabenblatt zur **Aufgabe Z1.11** veranschaulicht, in der genau die gleiche Konstellation betrachtet wird wie in der vorliegenden Aufgabe. Verwenden Sie in der letzten Teilaufgabe (f) den BSC–Parameter $\varepsilon = 0.1$.

Fragebogen zu "A1.11: Syndromdecodierung"

a) Wie viele Empfangsworte (N_0) führen zum Syndrom $\underline{s} = \underline{s}_0 = (0, 0, 0)$?

$$\boldsymbol{N_0} =$$

b) Wie viele Empfangsworte (N_7) führen zum Syndrom $\underline{s} = \underline{s}_7 = (1, 1, 1)$?

$$\boldsymbol{N_7} =$$

c) Welche Eigenschaften weisen alle Nebenklassenanführer $\underline{e}_\mu$ auf?

- ☐ Die letzten 3 Bit von $\underline{e}_\mu$ sind identisch mit $\underline{s}_\mu$.
- ☐ Alle $\underline{e}_\mu$ beinhalten jeweils eine einzige 1.
- ☐ Alle $\underline{e}_\mu$ beinhalten höchstens eine 1.

d) Zu welchem Syndrom $\underline{s}_\mu$ führt der Fehlervektor (1, 0, 0, 0, 0, 0, 0)?

$$\underline{\boldsymbol{e}} = (1, 0, 0, 0, 0, 0, 0): \quad \textbf{Index } \boldsymbol{\mu} =$$

e) Berechnen Sie jeweils das Syndrom $\underline{s}_\mu$ (Eingabe: Index μ) für

$$\underline{\boldsymbol{e}} = (0, 1, 0, 0, 0, 0, 0): \quad \textbf{Index } \boldsymbol{\mu} =$$

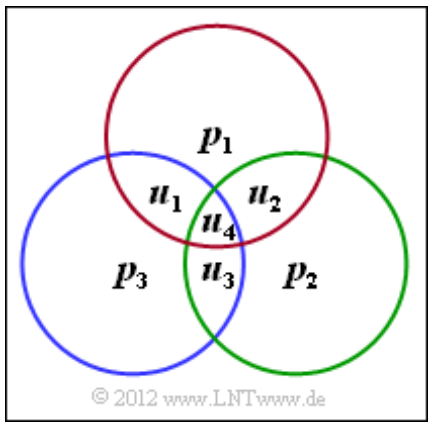
$$\underline{\boldsymbol{e}} = (0, 0, 1, 0, 0, 0, 0): \quad \textbf{Index } \boldsymbol{\mu} =$$

$$\underline{\boldsymbol{e}} = (0, 0, 0, 1, 0, 0, 0): \quad \textbf{Index } \boldsymbol{\mu} =$$

f) Welche Blockfehlerwahrscheinlichkeit ergibt sich für das BSC–Modell mit der Verfälschungswahrscheinlichkeit $\varepsilon = 0.1$?

$$\textbf{Pr(Blockfehler)} =$$

Z1.11: Nochmals Syndromdecodierung



Betrachtet wird die gleiche Konstellation wie in der **Aufgabe A1.11,** nämlich die Decodierung eines (7, 4, 3)–Hamming–Codes mit der Prüfmatrix

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

Dementsprechend lautet das Generatorpolynom:

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

Bei der **Syndromdecodierung** bildet man aus dem Empfangsvektor $\underline{y}$ das Syndrom $\underline{s}$:

$$\underline{s} = \underline{y} \cdot \mathbf{H}^{\rm T} \in {\rm GF}(2^m).$$

Mit diesem Ergebnis lässt sich beim betrachteten Hamming–Code ein jeder Einzelfehler im Codewort korrigieren. Im fehlerfreien Fall gilt $\underline{s} = \underline{s}_0 = (0, 0, 0)$. Aber auch bei 3 Übertragungsfehlern kann sich unter Umständen $\underline{s}_0 = (0, 0, 0)$ ergeben, so dass diese Fehler unerkannt bleiben.

Hinweis: Die Aufgabe bezieht sich auf die im **Kapitel 1.5** behandelte Thematik. Weitere Informationen zur Syndromdecodierung finden Sie im Angabenblatt zur **Aufgabe A1.11.** Die Grafik verdeutlicht die drei Prüfgleichungen entsprechend der Prüfmatrix:

- erste Zeile: rote Gruppierung,
- zweite Zeile: grüne Gruppierung,
- dritte Zeile: blaue Gruppierung.

Fragebogen zu "Z1.11: Nochmals Syndromdecodierung"

a) Handelt es sich um einen systematischen Code?

- ○ Ja,
- ○ Nein.

b) Empfangen wurde $\underline{y} = (1, 0, 0, 1, 0, 1, 0)$. Ist dies ein gültiges Codewort?

- ○ Ja,
- ○ Nein.

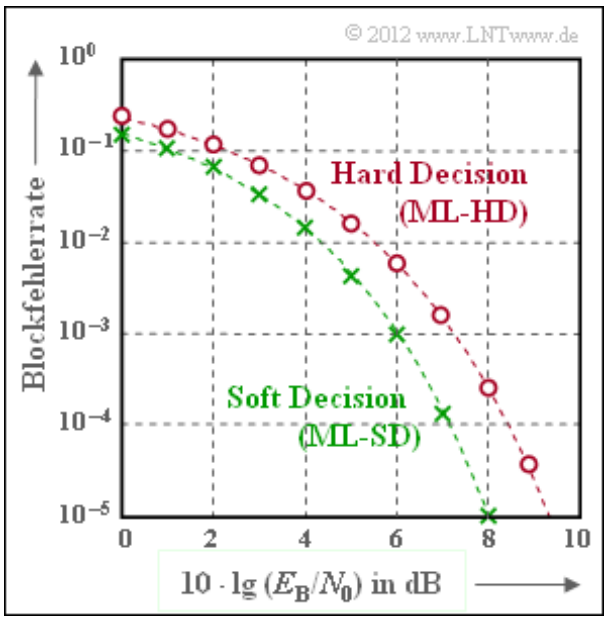
c) Welches Syndrom ergibt sich mit diesem Empfangswort?

- ☐ $\underline{s} = \underline{s}_0 = (0, 0, 0)$,
- ☐ $\underline{s} = \underline{s}_3 = (0, 1, 1)$,
- ☐ $\underline{s} = \underline{s}_7 = (1, 1, 1)$.

d) Welche Empfangsworte führen zum gleichen Syndrom wie in Teilaufgabe (c)?

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

A1.12: Hard / Soft Decision



Die Abbildung zeigt die Blockfehlerwahrscheinlichkeit für den **(7, 4, 3)–Hamming–Code**, wobei für den Empfänger zwei Varianten berücksichtigt sind:

- Bei Maximum–Likelihood–Detektion mit harten Entscheidungen (*Hard Decision*, HD), die im vorliegenden Fall (perfekter Code) auch durch Syndromdecodierung realisiert werden kann, ergibt sich die rote Kurve (Kreismarkierung).
- Der Kanal kann bei *Hard Decision* vereinfacht durch das **BSC–Modell** ersetzt werden. Der Zusammenhang zwischen dem BSC–Parameter ε und dem AWGN–Quotienten E_B/N_0 (in der Grafik verwendet) ist wie folgt gegeben:

$$\varepsilon = \mathrm{Q}\left(\sqrt{2 \cdot R \cdot E_B/N_0}\right) .$$

  Hier bezeichnet Q(x) die *komplementäre Gaußsche Fehlerfunktion* und R die Coderate.

- Die grüne Kurve (Kreuze) zeigt die Blockfehlerwahrscheinlichkeit bei „weichen” Entscheidungen (*Soft Decision*, SD). Dieser Funktionsverlauf lässt sich nicht in geschlossen–mathematischer Form angeben. In der Grafik eingezeichnet ist eine in **[Fri96]** angegebene obere Schranke:

$$\begin{aligned}\mathrm{Pr(Blockfehler)} \le\; & 7 \cdot \mathrm{Q}\left(\sqrt{3 \cdot \frac{2 \cdot R \cdot E_B}{N_0}}\right) + \\ & + 7 \cdot \mathrm{Q}\left(\sqrt{4 \cdot \frac{2 \cdot R \cdot E_B}{N_0}}\right) + \mathrm{Q}\left(\sqrt{7 \cdot \frac{2 \cdot R \cdot E_B}{N_0}}\right) .\end{aligned}$$

  Der jeweils erste Faktor im Argument der Q–Funktion gibt die möglichen Hamming–Distanzen an: $i = 3$, 4 und 7. Die Vorfaktoren berücksichtigen die Vielfachheiten $W_3 = W_4 = 7$ und $W_7 = 1$, und $R = 4/7$ beschreibt die Coderate. Für $10 \cdot \lg E_B/N_0 > 8$ dB ist Pr(Blockfehler) kleiner als 10^{-5}.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 1.5.** Verwenden Sie für numerische Ergebnisse das folgende Berechnungsmodul:

Komplementäre Gaußsche Fehlerfunktion

Fragebogen zu "A1.12: Hard / Soft Decision"

a) Wir betrachten bis einschließlich Teilaufgabe (d) stets *Hard Decision*. Welche Blockfehlerwahrscheinlichkeit besitzt der (7, 4, 3)–Hamming–Code?

$\varepsilon = 0.01$: Pr(Blockfehler) =

$\varepsilon = 0.001$: Pr(Blockfehler) =

b) Wie kann man die Fehlerwahrscheinlichkeit eines Hamming–Codes annähern?

- ☐ Pr(Blockfehler) = $n \cdot (n–1)/2 \cdot \varepsilon^2$.
- ☐ Pr(Blockfehler) = $n \cdot \varepsilon^2$.
- ☐ Pr(Blockfehler) = $n \cdot \varepsilon^n$.

c) Welcher Hamming–Code besitzt die kleinste Blockfehlerwahrscheinlichkeit bei konstantem BSC–Parameter ε?

- ○ der Hamming–Code (3, 1, 3) ⇒ *Repetition Code* (3, 1, 3),
- ○ der Hamming–Code (7, 4, 3),
- ○ der Hamming–Code (15, 11, 3).

d) Welcher numerische Zusammenhang besteht zwischen dem BSC–Parameter ε und dem AWGN–Quotienten E_B/N_0?

$\varepsilon = 0.01$: $10 \cdot \lg E_B/N_0$ = dB

$\varepsilon = 0.001$: $10 \cdot \lg E_B/N_0$ = dB

e) Welcher Gewinn (in dB) ist durch *Soft Decision* (SD) zu erzielen, wenn die Blockfehlerwahrscheinlichkeit den Wert 10^{-5} nicht überschreiten soll?

$10 \cdot \lg G_{SD}$ = dB

Z1.12: Vergleich (7, 4, 3) und (8, 4, 4)

BSC ε	Pr(Blockfehler) (7, 4, 3)-Code	(8, 4, 4)-Code
$3 \cdot 10^{-1}$	$6.71 \cdot 10^{-1}$	$7.45 \cdot 10^{-1}$
10^{-1}	$1.50 \cdot 10^{-1}$	$1.87 \cdot 10^{-1}$
$3 \cdot 10^{-2}$	$1.71 \cdot 10^{-2}$	$2.23 \cdot 10^{-2}$
10^{-2}	$2.03 \cdot 10^{-3}$	???
$3 \cdot 10^{-3}$	$1.87 \cdot 10^{-4}$	$2.49 \cdot 10^{-4}$
10^{-3}	$2.09 \cdot 10^{-5}$	$2.79 \cdot 10^{-5}$

Hinweis: Nur Korrektur von Einzelfehlern

Nun sollen die Blockfehlerwahrscheinlichkeiten

- des (7, 4, 3)–Hamming–Codes und
- des erweiterten (8, 4, 4)–Hamming–Codes

miteinander verglichen werden. Zugrunde gelegt werden

- das **BSC–Kanalmodell** (Parameter ε, insbesondere $\varepsilon = 0.01$ für numerische Ergebnisse),
- die **Syndromdecodierung,** mit der bei beiden Codes eine Maximum–Likelihood–Detektion realisiert wird. Bei richtiger Belegung der Syndromtabelle ergibt sich jeweils die minimale Blockfehlerwahrscheinlichkeit.

Für den (7, 4, 3)–Code wurde in der **Aufgabe A1.12** berechnet:

$$\text{Pr(Blockfehler)} = 1 - (1-\varepsilon)^7 - 7 \cdot \varepsilon \cdot (1-\varepsilon)^6 .$$

Die Zahlenwerte sind in der Spalte 2 der obigen Tabelle angegeben. Es handelt sich um die tatsächlichen Werte, also nicht um die in Aufgabe A1.12 hergeleitete Näherung: $\text{Pr(Blockfehler)} \approx 21 \cdot \varepsilon^2$.

Anzumerken ist, dass aufgrund des BSC–Kanalmodells nur harte Entscheidungen möglich sind. Mit **Soft–Decision** ergeben sich etwas kleinere Blockfehlerwahrscheinlichkeiten.

Nun soll die Blockfehlerwahrscheinlichkeit für den erweiterten (8, 4, 4)–Code ermittelt werden:

- Die Berechnung in Teilaufgabe d) erfolgt unter der Maßgabe, dass wie beim (7, 4, 3)–Code nur die Fehlermuster mit einer einzigen „1" korrigiert werden. In der rechten Spalte obiger Tabelle sind die Ergebnisse eingetragen, bis auf den Wert für $\varepsilon = 0.01$, der explizit berechnet werden soll.
- In der Teilaufgabe e) soll dagegen berücksichtigt werden, dass beim erweitereten (8, 4, 4)–Code Teile der Syndromtabelle noch mit Gewicht–2–Fehlermustern aufgefüllt werden können.

Hinweis: Die Aufgabe bezieht sich auf **Kapitel 1.5.** Von Interesse für die Lösung dieser Aufgabe ist insbesondere die Seite **Verallgemeinerung der Syndromdecodierung (2).**

Fragebogen zu "Z1.12: Vergleich (7, 4, 3) und (8, 4, 4)"

a) Wieviele Einträge beinhalten die jeweiligen Syndromtabellen?

(7, 4, 3)–Code: $N_{\rm ges}$ =

(8, 4, 4)–Code: $N_{\rm ges}$ =

b) Wieviele Gewicht–2–Fehlermuster gibt es insgesamt?

(7, 4, 3)–Code: N_2' =

(8, 4, 4)–Code: N_2' =

c) Wieviele Fehlermuster in den Syndromtabellen beinhalten zwei Einsen?

(7, 4, 3)–Code: N_2 =

(8, 4, 4)–Code: N_2 =

d) Es gelte nun $\varepsilon = 0.01$. Welche Blockfehlerwahrscheinlichkeit ergibt sich für den erweiterten (8, 4, 4)–Code ohne Gewicht–2–Fehlerkorrektur?

Pr(Blockfehler) =

e) Welches Ergebnis erzielt man demgegenüber mit Gewicht–2–Fehlerkorrektur?

Pr(Blockfehler) =

A1.13: BEC–Decodierung

Wir gehen hier von dem **Modell** auf der letzten Theorieseite im Kapitel 1.5 aus (grün hinterlegte BEC–Konfiguration):

- Jedes Informationswort $\underline{u}$ wird blockweise codiert und liefert das Codewort $\underline{x}$. Der Blockcode sei linear und durch seine Prüfmatrix **H** vollständig gegeben.
- Bei der Übertragung werden n_E Bit des Codewortes ausgelöscht ⇒ **Binary Erasure Channel** (BEC). Aus dem Codewort $\underline{x}$ wird somit das Empfangswort $\underline{y}$.
- Ist die Anzahl n_E der Auslöschungen kleiner als die **minimale Distanz** d_{min} des Codes, so gelingt es, aus $\underline{y}$ das Codewort $\underline{z} = \underline{x}$ ohne Fehler zu rekonstruieren, und man erhält so auch das richtige Informationswort $\underline{v} = \underline{u}$.
- Zur Aufgabenbeschreibung betrachten wir beispielhaft das Hamming–Codewort $\underline{x}$ = (0, 1, 0, 1, 1, 0, 0) und das Empfangswort $\underline{y}$ = (0, 1, E, E, 1, 0, 0).

Prüfmatrix des HC (7, 4, 3):

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

Zu den Teilaufgaben (b), (c):

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

$$\underline{z}_K = (1, 1, 0, 1)$$

Zu den Teilaufgaben (d), (e):

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

$$\underline{z}_K = (1, 1, 0, 0)$$

Ausgelöscht wurden somit durch den Kanal das dritte und vierte Bit. Der Codewortfinder hat somit die Aufgabe, den Vektor $\underline{z}_E = (z_3, z_4)$ mit $z_3, z_4 \in \{0, 1\}$ zu bestimmen. Dies geschieht entsprechend der Gleichung

$$\mathbf{H}_E \cdot \underline{z}_E^T = \mathbf{H}_K \cdot \underline{z}_K^T,$$

wobei im vorliegenden Beispiel gilt:

$$\underline{z}_K = (0, 1, 1, 0, 0), \quad \mathbf{H}_K = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{H}_E = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Diese Gleichung liefert zwei Bestimmungsgleichungen für die zu bestimmenden Bits, deren Lösung zum Ergebnis $z_3 = 0$ und $z_4 = 1$ führt.

Hinweis: Die Aufgabe gehört zu **Kapitel 1.5.** Der Algorithmus zur Zuordnung des Empfangswortes $\underline{y}$ zum richtigen Codewort $\underline{z} = \underline{x}$ ist im **Theorieteil** ausführlich beschrieben. Wir möchten nochmals daran erinnern, dass wir bei der BEC–Decodierung den ersten Decoderblock ($\underline{y} \rightarrow \underline{z}$) als *Codewortfinder* bezeichnen, da hier Fehlentscheidungen ausgeschlossen sind. Jedes Empfangswort wird richtig decodiert, oder es kann gar nicht decodiert werden. Beim BSC–Modell lassen sich dagegen Decodierfehler nicht vermeiden. Dementsprechend heißt der entsprechende Block dort *Codewortschätzer*.

Fragebogen zu "A1.13: BEC–Decodierung"

a) Empfangen wurde $\underline{y}$ = (1, E, 0, 1, 0, 0, E). Für welche Sequenz entscheidet sich der Codewortschätzer?

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

b) Welche Konsequenzen ergeben sich aus den roten Eintragungen für $\mathbf{H}_{\rm K}$ und $\underline{z}_{\rm K}$ (siehe Grafik auf der Angabenseite)?

- ☐ Der Erasure–Vektor lautet $\underline{z}_{\rm E} = (z_5, z_6, z_7)$.
- ☐ Das Empfangswort lautet $\underline{y}$ = (1, 1, 0, 1, E, E, E).
- ☐ $\mathbf{H}_{\rm E}$ ist eine 2 x 3–Matrix.
- ☐ $\mathbf{H}_{\rm E}$ ist eine 3 x 3–Matrix.

c) Nun gelte $\underline{y}$ = (1, 1, 0, 1, E, E, E). Welches Codewort wird ausgewählt?

- ☐ $\underline{z}$ = (1, 1, 0, 1, 1, 1, 0),
- ☐ $\underline{z}$ = (1, 1, 0, 1, 0, 0, 1),
- ☐ $\underline{z}$ = (1, 1, 0, 0, 0, 1, 0).
- ☐ Für das vorliegende $\underline{y}$ ist keine eindeutige Decodierung möglich.

d) Welche Konsequenzen ergeben sich aus den grünen Eintragungen für $\mathbf{H}_{\rm K}$ und $\underline{z}_{\rm K}$ (siehe Grafik auf der Angabenseite)?

- ☐ Das Empfangswort lautet $\underline{y}$ = (1, 1, 0, E, 0, E, E).
- ☐ $\mathbf{H}_{\rm K}$ unterscheidet sich gegenüber Teilfrage (b) in der letzten Zeile.
- ☐ $\mathbf{H}_{\rm K}$ unterscheidet sich gegenüber Teilfrage (b) in der letzten Spalte.

e) Nun gelte $\underline{y}$ = (1, 1, 0, E, 0, E, E). Welches Codewort wird ausgewählt?

- ☐ $\underline{z}$ = (1, 1, 0, 1, 1, 1, 0),
- ☐ $\underline{z}$ = (1, 1, 0, 1, 0, 0, 1),
- ☐ $\underline{z}$ = (1, 1, 0, 0, 0, 1, 0).
- ☐ Für das vorliegende $\underline{y}$ ist keine eindeutige Decodierung möglich.

f) Welche Aussagen ergeben sich für die Korrekturfähigkeit beim BEC? $n_{\rm E}$ gibt

dabei Anzahl der Auslöschungen (*Erasures*) an.

- ☐ Für $n_E < d_{min}$ ist stets eine eindeutige Decodierung möglich.
- ☐ Für $n_E = d_{min}$ ist stets eine eindeutige Decodierung möglich.
- ☐ Für $n_E = d_{min}$ ist manchmal eine eindeutige Decodierung möglich.
- ☐ Für $n_E > d_{min}$ ist eine eindeutige Decodierung nie möglich.

Z1.13: Nochmals BEC–Decodierung

Wir betrachten wieder wie in der vorherigen Aufgabe die Decodierung eines **Hamming–Codes** nach der Übertragung über einen Auslöschungskanal ⇒ **Binary Erasure Channel** (abgekürzt BEC).

Der (7, 4, 3)–Hamming–Code wird durch die nebenstehende Codetabelle $\underline{u}_i \rightarrow \underline{x}_i$ vollständig beschrieben, anhand derer alle Lösungen gefunden werden können.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 1.5.** Im Gegensatz zur **Aufgabe A1.13** soll hier die Lösung nicht streng formal, sondern eher intuitiv gefunden werden.

i	$\underline{u}_i$	$\underline{x}_i$
0	(0, 0, 0, 0)	(0, 0, 0, 0, 0, 0, 0)
1	(0, 0, 0, 1)	(0, 0, 0, 1, 1, 1, 1)
2	(0, 0, 1, 0)	(0, 0, 1, 0, 0, 1, 1)
3	(0, 0, 1, 1)	(0, 0, 1, 1, 1, 0, 0)
4	(0, 1, 0, 0)	(0, 1, 0, 0, 1, 1, 0)
5	(0, 1, 0, 1)	(0, 1, 0, 1, 0, 0, 1)
6	(0, 1, 1, 0)	(0, 1, 1, 0, 1, 0, 1)
7	(0, 1, 1, 1)	(0, 1, 1, 1, 0, 1, 0)
8	(1, 0, 0, 0)	(1, 0, 0, 0, 1, 0, 1)
9	(1, 0, 0, 1)	(1, 0, 0, 1, 0, 1, 0)
10	(1, 0, 1, 0)	(1, 0, 1, 0, 1, 1, 0)
11	(1, 0, 1, 1)	(1, 0, 1, 1, 0, 0, 1)
12	(1, 1, 0, 0)	(1, 1, 0, 0, 0, 1, 1)
13	(1, 1, 0, 1)	(1, 1, 0, 1, 1, 0, 0)
14	(1, 1, 1, 0)	(1, 1, 1, 0, 0, 0, 0)
15	(1, 1, 1, 1)	(1, 1, 1, 1, 1, 1, 1)

Fragebogen zu "Z1.13: Nochmals BEC–Decodierung"

a) Wie groß ist die minimale Distanz des vorliegenden Codes?

d_{min} =

b) Ist der Code systematisch?

- ○ JA.
- ○ NEIN.

c) Bis zu wie vielen *Erasures* ist die erfolgreiche Decodierung gewährleistet?

e_{max} =

d) Wie lautet das gesendete Informationswort $\underline{u}$ für $\underline{y}$ = (1, 0, E, E, 0, 1, 0)?

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

e) Welche der nachfolgenden Empfangsworte können decodiert werden?

- ☐ $\underline{y}_A$ = (1, 0, 0, 1, E, E, E),
- ☐ $\underline{y}_B$ = (E, E, 0, E, 0, 1, 0),
- ☐ $\underline{y}_C$ = (E, E, E, 1, 0, 1, 0),
- ☐ $\underline{y}_D$ = (1, 0, E, E, E, E, 0).

A1.14: Bhattacharyya–Schranke für BEC

Wir betrachten in dieser Aufgabe den systematischen (5, 2)–Code mit der 2×5–Generatormatrix

$$\mathbf{G}_{(5,2)} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

der 3 × 5–Prüfmatrix

$$\mathbf{H}_{(5,2)} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

und den $2^k = 4$ Codeworten

$$\underline{x}_0 = (0,0,0,0,0)\,, \quad \underline{x}_1 = (0,1,0,1,1)\,,$$
$$\underline{x}_2 = (1,0,1,1,0)\,, \quad \underline{x}_3 = (1,1,1,0,1)\,.$$

Erasure(s)	Empfangsvektoren
keine	(0, 0, 0, 0, 0)
eines	(5 Möglichkeiten)
zwei	(10 Möglichkeiten)
drei	(0, 0, E, E, E) (0, E, 0, E, E) (0, E, E, 0, E) (0, E, E, E, 0) (E, 0, 0, E, E) (E, 0, E, 0, E) (E, 0, E, E, 0) (E, E, 0, 0, E) (E, E, 0, E, 0) (E, E, E, 0, 0)
vier	(0, E, E, E, E) (E, 0, E, E, E) (E, E, 0, E, E) (E, E, E, 0, E) (E, E, E, E, 0)
fünf	(E, E, E, E, E)

Am Ausgang des digitalen Kanals, der durch das **BEC–Modell** (*Binary Erasure Channel*) mit der Auslöschungswahrscheinlichkeit $\lambda = 0.001$ festgelegt wird, tritt der Empfangsvektor

$$\underline{y} = (y_1, y_2, y_3, y_4, y_5)$$

auf, wobei für $i = 1, \ldots, 5$ gilt: $y_i \in \{0, 1, \text{E}\}$.

Der BEC–Kanal zeichnet sich dadurch aus, dass

- Verfälschungen (0 → 1, 1 → 0) ausgeschlossen sind,
- es aber zu Auslöschungen (0 → E, 1 → E) kommen kann.

Die Grafik zeigt explizit alle möglichen Empfangsvektoren $\underline{y}$ mit drei oder mehr Auslöschungen (englisch: *Erasures*, abgekürzt E) unter der Voraussetzung, dass der Nullvektor (0, 0, 0, 0, 0) gesendet wurde. Bei weniger als drei Auslöschungen liefert bei dem betrachteten (5, 2)–Code der Codewortschätzer immer die richtige Entscheidung: $\underline{z} = \underline{x}$.

Bei drei oder mehr Auslöschungen kann es dagegen zu Fehlentscheidungen kommen. In diesem Fall gilt für die Blockfehlerwahrscheinlichkeit

$$\text{Pr(Blockfehler)} = \text{Pr}(\underline{z} \neq \underline{x}) = \text{Pr}\left\{ [\underline{x}_0 \mapsto \underline{x}_1] \cup [\underline{x}_0 \mapsto \underline{x}_2] \cup [\underline{x}_0 \mapsto \underline{x}_3] \right\}.$$

Das Ereignis $[\underline{x}_0 \to \underline{x}_1]$ sagt nicht unbedingt aus, dass beim betrachteten Empfangsvektor $\underline{y}$ tatsächlich für das Codewort $\underline{x}_1$ entschieden wird, sondern lediglich, dass die Entscheidung für $\underline{x}_1$ aufgrund der Statistik sinnvoller wäre als die Entscheidung für $\underline{x}_0$. Es könnte aber auch für $\underline{x}_2$ oder $\underline{x}_3$ entschieden werden, wenn das **Maximum–Likelihood–Kriterium** hierfür spricht.

Die Berechnung der Blockfehlerwahrscheinlichkeit ist schwierig, da die Ereignisse $[\underline{x}_0 \to \underline{x}_1]$, $[\underline{x}_0 \to \underline{x}_2]$ und $[\underline{x}_0 \to \underline{x}_3]$ nicht notwendigerweise **disjunkt** sind. Eine obere Schranke liefert die **Union Bound:**

$$\text{Pr(Union Bound)} = \text{Pr}[\underline{x}_0 \mapsto \underline{x}_1] + \text{Pr}[\underline{x}_0 \mapsto \underline{x}_2] + \text{Pr}[\underline{x}_0 \mapsto \underline{x}_3] \geq \text{Pr(Blockfehler)}\,.$$

Eine weitere Schranke wurde von Bhattacharyya angegeben:

$$\Pr(\text{Bhattacharyya}) = W(\beta) - 1 \geq \Pr(\text{Union Bound}) \geq \Pr(\text{Blockfehler}),$$

wobei beim *Binary Erasure Channel* $\beta = \lambda$ gilt. $W(X)$ ist die **Gewichtsfunktion,** wobei die Pseudo–Variable X hier durch den Bhattacharyya–Parameter β zu ersetzen ist.

Die Bhattacharyya–Schranke liegt je nach Kanal mehr oder weniger weit oberhalb der *Union Bound*. Ihre Bedeutung liegt darin, dass die Schranke für unterschiedliche Kanäle in gleicher Weise angebbar ist.

Hinweis: Die Aufgabe gehört zum Themengebiet von **Kapitel 1.6.**

Fragebogen zu "A1.14: Bhattacharyya–Schranke für BEC"

a) Wie groß ist die paarweise Fehlerwahrscheinlichkeit zwischen den Codeworten $\underline{x}_0 = (0, 0, 0, 0, 0)$ und $\underline{x}_1 = (0, 1, 0, 1, 1)$?

$$\mathbf{Pr}[\underline{\boldsymbol{x}}_\mathbf{0} \rightarrow \underline{\boldsymbol{x}}_\mathbf{1}] =$$

b) Welche Aussagen stimmen bezüglich $\Pr[\underline{x}_0 \rightarrow \underline{x}_i]$ mit Laufindex $i = 1, \ ... \ , 3$? Hierbei bezeichnet d_H die Hamming–Distanz zwischen $\underline{x}_0$ und $\underline{x}_i$.

- ☐ Es gilt $\Pr[\underline{x}_0 \rightarrow \underline{x}_i] = \lambda^{d_\mathrm{H}} \cdot (1 - \lambda)^{n \, - \, d_\mathrm{H}}$.
- ☐ Es gilt $\Pr[\underline{x}_0 \rightarrow \underline{x}_i] = 1/2 \cdot \lambda^{d_\mathrm{H}}$.
- ☐ $\Pr[\underline{x}_0 \rightarrow \underline{x}_i]$ ist die Verfälschungswahrscheinlichkeit von $\underline{x}_0$ nach $\underline{x}_i$.

c) Wie groß sind die Wahrscheinlichkeiten

$$\mathbf{Pr}[\underline{\boldsymbol{x}}_\mathbf{0} \rightarrow \underline{\boldsymbol{x}}_\mathbf{2}] =$$

$$\mathbf{Pr}[\underline{\boldsymbol{x}}_\mathbf{0} \rightarrow \underline{\boldsymbol{x}}_\mathbf{3}] =$$

d) Geben Sie die *Union Bound* für die Blockfehlerwahrscheinlichkeit an.

$$\mathbf{Pr(Union\ Bound)} =$$

e) Wie lautet im vorliegenden Fall die *Bhattacharyya–Schranke*?

$$\mathbf{Pr(Bhattacharyya)} =$$

A1.15: Distanzspektren

Wir betrachten wie in **Aufgabe A1.9**

- den (7, 4, 3)–Hamming–Code und
- den erweiterten (8, 4, 4)–Hamming–Code.

Die Grafik zeigt die zugehörigen Codetabellen. In der **Aufgabe A1.12** wurde schon die Syndromdecodierung dieser beiden Codes behandelt.

In dieser Aufgabe sollen die Unterschiede hinsichtlich des Distanzspektrums $\{W_i\}$ herausgearbeitet werden.

Für die Laufvariable gilt $i = 0, \ldots, n$:

- Die Integerzahl W_i gibt die Zahl der Codeworte $\underline{x}$ mit dem **Hamming–Gewicht** $\underline{w}_{\rm H}(\underline{x}) = i$ an.
- Bei den hier betrachteten linearen Code bescheibt W_i gleichzeitig die Anzahl der Codeworte mit der **Hamming–Distanz** i vom Nullwort.

Codeworte von C_1 Hamming-Code (7, 4)	Codeworte von C_2 HC erweitert auf (8, 4)
(0, 0, 0, 0, 0, 0, 0)	(0, 0, 0, 0, 0, 0, 0, 0)
(0, 0, 0, 1, 1, 1, 1)	(0, 0, 0, 1, 1, 1, 1, 0)
(0, 0, 1, 0, 0, 1, 1)	(0, 0, 1, 0, 0, 1, 1, 1)
(0, 0, 1, 1, 1, 0, 0)	(0, 0, 1, 1, 1, 0, 0, 1)
(0, 1, 0, 0, 1, 1, 0)	(0, 1, 0, 0, 1, 1, 0, 1)
(0, 1, 0, 1, 0, 0, 1)	(0, 1, 0, 1, 0, 0, 1, 1)
(0, 1, 1, 0, 1, 0, 1)	(0, 1, 1, 0, 1, 0, 1, 0)
(0, 1, 1, 1, 0, 1, 0)	(0, 1, 1, 1, 0, 1, 0, 0)
(1, 0, 0, 0, 1, 0, 1)	(1, 0, 0, 0, 1, 0, 1, 1)
(1, 0, 0, 1, 0, 1, 0)	(1, 0, 0, 1, 0, 1, 0, 1)
(1, 0, 1, 0, 1, 1, 0)	(1, 0, 1, 0, 1, 1, 0, 0)
(1, 0, 1, 1, 0, 0, 1)	(1, 0, 1, 1, 0, 0, 1, 0)
(1, 1, 0, 0, 0, 1, 1)	(1, 1, 0, 0, 0, 1, 1, 0)
(1, 1, 0, 1, 1, 0, 0)	(1, 1, 0, 1, 1, 0, 0, 0)
(1, 1, 1, 0, 0, 0, 0)	(1, 1, 1, 0, 0, 0, 0, 1)
(1, 1, 1, 1, 1, 1, 1)	(1, 1, 1, 1, 1, 1, 1, 1)

- Häufig weist man der Zahlenmenge $\{W_i\}$ einer Pseudo–Funktion zu, die man **Gewichtsfunktion** (englisch: *Weight Enumerator Function*, WEF) nennt:

$$\{W_i\} \quad \Leftrightarrow \quad W(X) = \sum_{i=0}^{n} W_i \cdot X^i = W_0 + W_1 \cdot X + W_2 \cdot X^2 + \ldots + W_n \cdot X^n .$$

Bhattacharyya hat die Pseudo–Funktion $W(X;)$ verwendet, um eine kanalunabhängige (obere) Schranke für die Blockfehlerwahrscheinlichkeit anzugeben:

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

Der so genannte *Bhattacharyya–Parameter* ist dabei wie folgt gegeben:

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

Hinweis: Die Aufgabe bezieht sich auf **Kapitel 1.6,** ebenso wie **Aufgabe A1.14** und **Aufgabe A1.16.** Als Kanäle sollen betrachtet werden:

- das **BSC–Modell** (*Binary Symmetric Channel*),
- das **BEC–Modell** (*Binary Erasure Channel*),
- das **AWGN–Kanalmodell.**

Anzumerken ist, dass die Bhattacharyya–Schranke im allgemeinen sehr pessimistisch ist. Die tatsächliche Blockfehlerwahrscheinlichkeit liegt oft deutlich darunter.

Fragebogen zu "A1.15: Distanzspektren "

a) Geben Sie das Distanzspektrum des (7, 4, 3)–Hamming–Codes an.

(7, 4, 3)–Code: W_0 =

W_3 =

W_4 =

W_7 =

b) Wie lautet die Bhattacharyya–Schranke für das BSC–Modell mit $\varepsilon = 0.01$?

(7, 4, 3)–Code: Pr(Bhattacharyya) =

c) Wie lautet bei gleichem Kanal die Schranke des erweiterten Codes?

(8, 4, 4)–Code: Pr(Bhattacharyya) =

d) Mit welchem BEC–Parameter λ erhält man die genau gleichen Schranken?

λ =

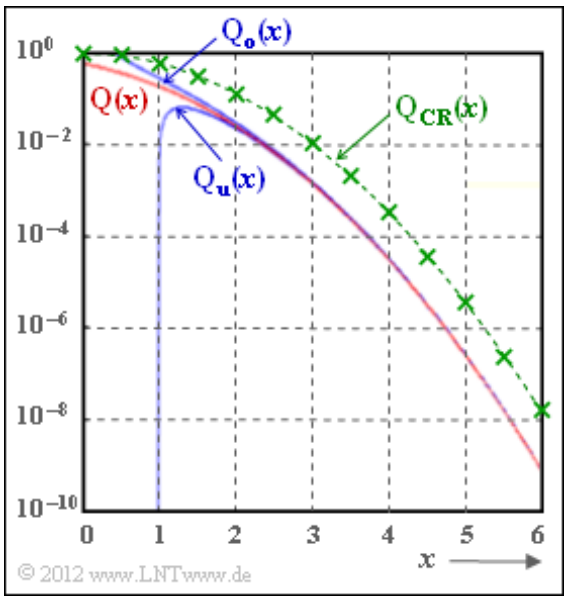
e) Betrachten wir nun das AWGN–Modell. Bestimmen Sie E_B/N_0 in dB derart, dass sich für den (8, 4, 4)–Code die gleiche Bhattacharyya–Schranke ergibt.

(8, 4, 4)–Code: $10 \cdot \lg E_B/N_0$ = dB

f) Ermitteln Sie nun den AWGN–Parameter für den (7, 4, 3)–Hamming–Code.

(7, 4, 3)–Code: $10 \cdot \lg E_B/N_0$ = dB

A1.16: Schranken für AWGN



Wir gehen von der folgenden Konstellation aus:

- ein linearer Blockcode mit der Coderate $R = k/n$ und dem Distanzspektrum $\{W_i\}$, $i = 1, \ldots, n$,
- ein AWGN–Kanal, gekennzeichnet durch „E_B/N_0"

  $\Rightarrow$ umrechenbar in die Rauschleistung σ^2,
- ein Empfänger, basierend auf *Soft Decision* sowie dem *Maximum–Likelihood*–Kriterium.

Unter der für die gesamte Aufgabe gültigen Annahme, dass stets das Nullwort $\underline{x}_1 = (0, 0, \ldots, 0)$ gesendet wird, gilt für die **„paarweise Fehlerwahrscheinlichkeit"** mit einem anderen Codewort $\underline{x}_l$ ($l = 2, \ldots, 2^k$):

$$\Pr[\underline{x}_1 \mapsto \underline{x}_l] = \mathrm{Q}\left(\sqrt{w_\mathrm{H}(\underline{x}_l)/\sigma^2}\right) .$$

Die Herleitung dieser Beziehung finden Sie in **[Liv10].** In dieser Gleichung wurden verwendet:

- die **komplementäre Gaußsche Fehlerfunktion** $\mathrm{Q}(x)$,
- das **Hamming–Gewicht** $w_\mathrm{H}(\underline{x}_l)$ des Codewortes $\underline{x}_l$,
- die AWGN–Rauschleistung $\sigma^2 = (2 \cdot R \cdot E_B/N_0)^{-1}$.

Damit lassen sich verschiedene Schranken für die Blockfehlerwahrscheinlichkeit angeben:

- die sogenannte **Union Bound:**

$$p_1 = \sum_{l=2}^{2^k} \Pr[\underline{x}_1 \mapsto \underline{x}_l] = \sum_{l=2}^{2^k} \mathrm{Q}\left(\sqrt{w_\mathrm{H}(\underline{x}_l)/\sigma^2}\right) ,$$

- die so genannte **Truncated Union Bound** (TUB):

$$p_2 = W_{d_\mathrm{min}} \cdot \mathrm{Q}\left(\sqrt{d_\mathrm{min}/\sigma^2}\right) ,$$

- die **Bhattacharyya–Schranke:**

$$p_3 = W(\beta) - 1 , \text{ mit } \beta = \exp\left[-1/(2\sigma^2)\right] .$$

  In diesem Fall ist das Distanzspektrum $\{W_i\}$ durch die Gewichtsfunktion zu ersetzen:

$$\{W_i\} \quad \Leftrightarrow \quad W(X) = \sum_{i=0}^{n} W_i \cdot X^i = W_0 + W_1 \cdot X + W_2 \cdot X^2 + \ldots + W_n \cdot X^n .$$

  Beim Übergang von der *Union Bound* p_1 zur Schranke p_3 wird unter Anderem die Funktion $\mathrm{Q}(x)$ durch die *Chernoff–Rubin–Schranke* $\mathrm{Q}_\mathrm{CR}(x)$ ersetzt. Beide Funktionen sind in obigerer Grafik dargestellt (rote bzw. grüne Kurve).

In der **Aufgabe Z1.16** wird der Zusammenhang zwischen diesen Funktionen numerisch ausgewertet und

Bezug genommen zu den Schranken $Q_o(x)$ und $Q_u(x)$, die in obiger Grafik ebenfalls eingezeichnet sind.

Hinweis: Die Aufgabe gehört zum **Kapitel 1.6.** Weiter verweisen wir auf folgendes Flash–Modul:

Komplimentäre Gaußsche Fehlerfunktion (Dateigröße: 235 kB)

Fragebogen zu "A1.16: Schranken für AWGN"

a) Welche Gleichung gilt für die *Union Bound*?

- ☐ p_1 = Summe (über $l = 2, \ldots, 2^k$) $W_l \cdot \mathrm{Q}[(l/\sigma^2)^{0.5}]$,
- ☐ p_1 = Summe (über $i = 1, \ldots, n$) $W_i \cdot \mathrm{Q}[(i/\sigma^2)^{0.5}]$.

b) Geben Sie die *Union Bound* für den (8, 4, 4)–Code und $\sigma = 1$, $\sigma = 0.5$ an.

(8, 4, 4)–Code, $\sigma = 1$: p_1 =

$\sigma = 0.5$: p_1 =

c) Was liefert die *Truncated Union Bound* bei gleichen Randbedingungen?

(8, 4, 4)–Code, $\sigma = 1$: p_2 =

$\sigma = 0.5$: p_2 =

d) Welche Aussage gilt immer (für alle Konstellationen)?

- ☐ Die Blockfehlerwahrscheinlichkeit ist nie größer als p_1.
- ☐ Die Blockfehlerwahrscheinlichkeit ist nie größer als p_2.

e) Wie kommt man von p_1 zur Bhattacharyya–Schranke p_3? Dadurch, dass man

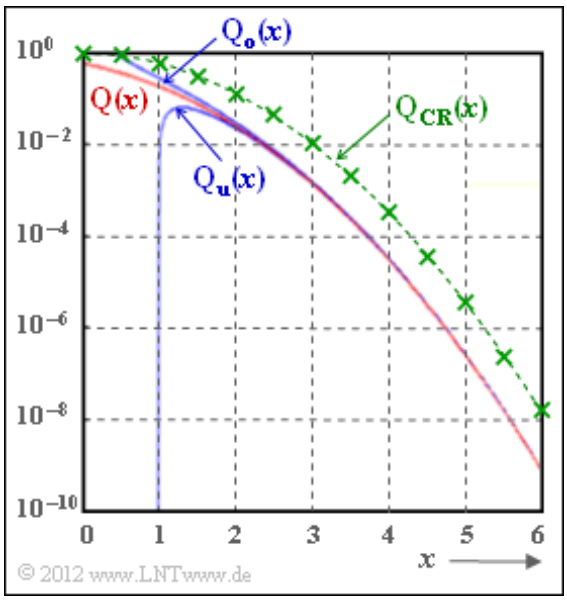
- ☐ die Fehlerfunktion $\mathrm{Q}(x)$ durch die Funktion $\mathrm{Q}_{\mathrm{CR}}(x)$ ersetzt,
- ☐ den Bhattacharyya–Parameter $\beta = 1/\sigma$ setzt,
- ☐ statt $\{W_i\}$ die Gewichtsfunktion $W(X)$ verwendet.

f) Geben Sie die Bhattacharyya–Schranke für $\sigma = 1$ und $\sigma = 0.5$ an.

(8, 4, 4)–Code, $\sigma = 1$: p_3 =

$\sigma = 0.5$: p_3 =

Z1.16: Schranken für Q(*x*)



Die Wahrscheinlichkeit, dass eine Gaußsche Zufallsgröße n mit Streuung σ → Varianz σ^2 betragsmäßig größer ist als ein Wert A, ist gleich

$$\Pr(n > A) = \Pr(n < -A) = \mathrm{Q}(A/\sigma).$$

Hierbei verwendet ist eine der wichtigsten Funktionen für die Nachrichtentechnik (in der Grafik rot eingezeichnet): die **Komplementäre Gaußsche Fehlerfunktion**

$$\mathrm{Q}(x) = \frac{1}{\sqrt{2\pi}} \int_{x}^{+\infty} \mathrm{e}^{-u^2/2}\,\mathrm{d}u\,.$$

$\mathrm{Q}(x)$ ist eine monoton fallende Funktion mit $\mathrm{Q}(0) = 0.5$. Für große Werte von x tendiert $\mathrm{Q}(x)$ gegen Null.

Das Integral der Q–Funktion ist analytisch nicht lösbar und wird meist in Tabellenform angegeben. Aus der Literatur bekannt sind aber handhabbare Näherungslösungen bzw. Schranken für positive x–Werte:

- die obere Schranke (obere blaue Kurve in nebenstehender Grafik, nur gültig für $x > 0$):

$$\mathrm{Q_o}(x) = \frac{1}{\sqrt{2\pi} \cdot x} \cdot \mathrm{e}^{-x^2/2} \;\geq\; \mathrm{Q}(x),$$

- die untere Schranke (untere blaue Kurve in der Grafik, nur gültig für $x > 1$):

$$\mathrm{Q_u}(x) = \frac{1 - 1/x^2}{\sqrt{2\pi} \cdot x} \cdot \mathrm{e}^{-x^2/2} \;\leq\; \mathrm{Q}(x),$$

- die Chernoff–Rubin–Schranke (grüne Kurve in der Grafik, gezeichnet für $K = 1$):

$$\mathrm{Q_{CR}}(x) = K \cdot \mathrm{e}^{-x^2/2} \;\geq\; \mathrm{Q}(x).$$

In der Aufgabe ist zu untersuchen, in wie weit diese Schranken als Näherungen für $\mathrm{Q}(x)$ herangezogen werden können und welche Verfälschungen sich dadurch ergeben.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 1.6** dieses Buches sowie auf das **Kapitel 3.5** im Buch „Stochastische Signaltheorie". Die Aufgabe bietet auch einige wichtige Hinweise zur Lösung der **Aufgabe A1.16,** in der die Funktion $\mathrm{Q_{CR}}(x)$ zur Herleitung der **Bhattacharyya–Schranke** für den AWGN–Kanal benötigt wird. Weiter verweisen wir auf das folgende Interaktionsmodul:

Komplementäre Gaußsche Fehlerfunktion

Fragebogen zu "Z1.16: Schranken für Q(*x*)"

a) Welche Werte liefern die obere und die untere Schranke für $x = 4$?

$$\mathbf{Q_o(\mathit{x} = 4)} =$$

$$\mathbf{Q_u(\mathit{x} = 4)} =$$

b) Welche Aussagen gelten für die Funktionen $Q_o(x)$ und $Q_u(x)$?

- ☐ Für $x \geq 2$ sind die beiden Schranken brauchbar.
- ☐ Für $x < 1$ ist $Q_u(x)$ unbrauchbar (wegen $Q_u(x) < 0$).
- ☐ Für $x < 1$ ist $Q_o(x)$ unbrauchbar (wegen $Q_o(x) > 1$).

c) Um welchen Faktor liegt die Chernoff–Rubin–Schranke oberhalb von $Q_o(x)$?

$$\mathbf{Q_{CR}(\mathit{x})/Q_o(\mathit{x})}: \quad \mathbf{\mathit{x} = 2} =$$

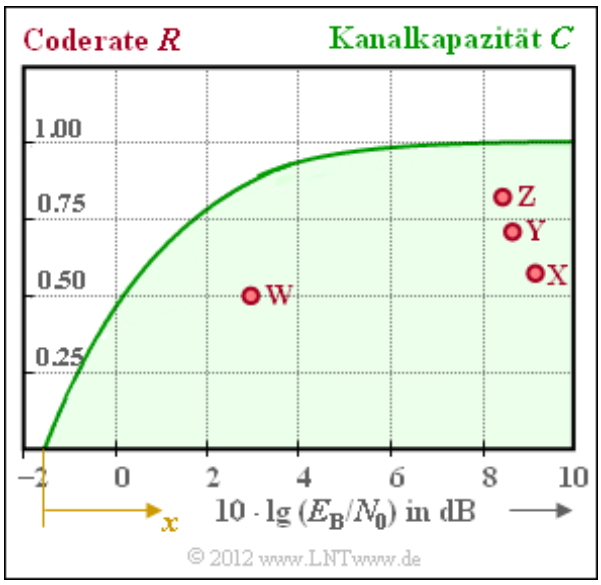
$$\mathbf{\mathit{x} = 4} =$$

$$\mathbf{\mathit{x} = 6} =$$

d) Bestimmen Sie K derart, dass $K \cdot Q_{CR}(x)$ möglichst nahe bei $Q(x)$ liegt und gleichzeitig im gesamten Bereich $Q(x) \leq K \cdot Q_{CR}(x)$ eingehalten wird.

$$\mathbf{\mathit{K}} =$$

A1.17: Coderate vs. E_B/N_0



Die Grafik zeigt maximal zulässige Coderaten $R < C$ gemäß Shannons **Kanalcodierungstheorem:**

- Die grüne Grenzkurve gibt die Kanalkapazität C für den AWGN–Kanal unter der Voraussetzung eines binären Eingangssignals („BPSK") an.
- In **Aufgabe Z1.17** wird hierfür eine einfache Näherung angegeben. Mit der zweiten Abszisse

$$x = \frac{1.6\,\text{dB} + 10 \cdot \lg E_B/N_0}{1\,\text{dB}}$$

ergibt sich näherungsweise:

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

- Gilt $R < C$, so kann ein Code gefunden werden, der bei unendlich langen Blöcken ($n \to \infty$) zur Fehlerwahrscheinlichkeit 0 führt. Wie dieser Code aussieht, ist durch das Kanalcodierungstheorem nicht festgelegt und spielt für diese Aufgabe auch keine Rolle.

In die Grafik eingezeichnet sind die Kenngrößen etablierter Codiersysteme. Die roten Punkte **X**, **Y** und **Z** markieren drei Hamming–Codes unterschiedlicher Codelängen, nämlich mit $n = 7$, $n = 15$ und $n = 31$. Das Codiersystem **W** ist durch die Kenngrößen $R = 0.5$ und $10 \cdot \lg E_B/N_0 = 3$ dB gekennzeichnet.

Hinweis: Die Aufgabe gehört zum Themengebiet von **Kapitel 1.7.** Die informationstheoretische Grenze „Kanalkapazität" bezieht sich auf die Fehlerwahrscheinlichkeit 0. Die eingezeichneten Punkte realer Übertragungssysteme ergeben sich dagegen unter der Annahme BER = 10^{-5}.

Fragebogen zu "A1.17: Coderate vs. E_B/N_0"

a) Welche der roten Punkte gehören zu welchem Hamming–Code? *Hinweis:* Die Grafik wurde für BER = 10^{-5} erstellt.

- ☐ **X** bezeichnet den (7, 4, 3)–Hamming–Code.
- ☐ **Y** bezeichnet den (15, 11, 3)–Hamming–Code.
- ☐ **Z** bezeichnet den (31, 15, 3)–Hamming–Code.

b) In welche Richtung werden sich die Punkte **X**, **Y** und **Z** verschieben, wenn die Grafik für BER = 10^{-10} erstellt werden soll?

- ☐ Nach links,
- ☐ nach rechts,
- ☐ nach oben.

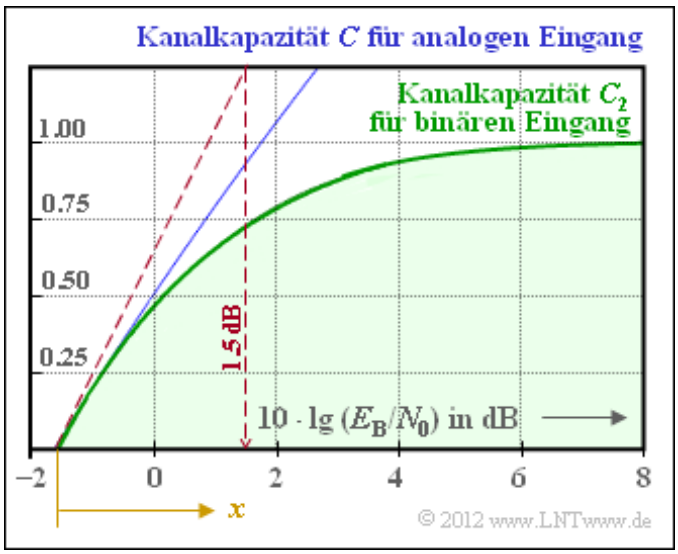
c) Bis zu welcher Coderate R_{max} könnte man ein System mit gleichem E_B/N_0 wie System **W** betreiben?

$$\boldsymbol{E_B/N_0 = 3\ \text{dB}:\quad R_{max}} =$$

d) Um welchen Faktor A könnte die Sendeleistung von System **W** entsprechend der Kanalkapazitätskurve C herabgesetzt werden?

$$\boldsymbol{R = 0.5:\quad A\ \text{(größer 1!)}} =$$

Z1.17: BPSK–Kanalkapazität



Gemäß dem **Kanalcodierungstheorem** lassen sich Binärsignale über den **AWGN–Kanal** dann und nur dann fehlerfrei übertragen, wenn

- man einen Kanalcode der Rate $R = k/n$ verwendet,
- die Blocklänge n dieses Codes sehr groß gewählt wird $\Rightarrow \; n \to \infty$,
- die Rate R kleiner ist als die für binären Eingang gültige Kanalkapazität C_2,
- wobei die BPSK–Kanalkapazität C_2 vom AWGN–Quotienten E_B/N_0 abhängt.

Der zulässige Bereich für die Coderate R ist in der Grafik grün hinterlegt. Die Grenzkurve C_2, gültig für binäre Eingangssignale (daher der Index 2) und manchmal auch als BPSK–Kanalkapazität bezeichnet, ist allerdings nicht in mathematisch–geschlossener Form angebbar, sondern das Ergebnis eines Integrals, das nur numerisch ausgewertet werden kann.

Als blaue Kurve ist die Kanalkapazität C eingetragen, wenn man beliebige reelle Eingangssignale zulässt. Bei mehrstufigen Signalen kann die Rate durchaus auch Werte $R > 1$ annehmen. Für eine Gaußverteilung ergibt sich für eine gegebene Rate R das kleinstmögliche $(E_B/N_0)_{min}$ gemäß der Gleichung

$$(E_B/N_0)_{\rm min} = \frac{2^{2R} - 1}{2R}.$$

Im Umkehrschluss ist die Rate R für den gegebenen AWGN–Quotienten E_B/N_0 nach oben begrenzt. Die gerade noch zulässige Coderate R_{max} bei gegebenem Kanal (E_B/N_0 = const.) bezeichnen wir als die Kanalkapazität C. Für $E_B/N_0 = 1 \;\Rightarrow\; 10 \cdot \lg E_B/N_0 = 0$ dB erhält man beispielsweise $C = 0.5$. Das heißt: Auch bei bestmöglicher Amplitudenverteilung des reellen Eingangssignals darf die Coderate den Wert $R = 0.5$ nicht überschreiten. Bei binärem Eingang ergibt sich ein etwas kleinerer Wert gemäß C_2.

In dieser Aufgabe soll versucht werden, den grafisch vorgegebenen Verlauf der Kanalkapazität C_2 durch eine Exponentialfunktion anzunähern:

- Verwenden Sie für die Abszisse die Hilfsvariable (siehe Grafik)

$$x = \frac{x_0 + 10 \cdot \lg\, E_B/N_0}{1\,\text{dB}}.$$

  Das heißt: x ist ohne Einheit; auf die Pseudo–Einheit „dB” wird verzichtet.

- Berücksichtigen Sie, dass für ein kleines E_B/N_0 die Näherung $C_2 \approx C$ gültig ist (siehe Grafik), woraus der Parameter x_0 bestimmt werden kann.

- Setzen Sie für $C_2' = 1 - \exp(-a \cdot x)$ an und bestimmen Sie den Parameter a aus der gestrichelt eingezeichneten Tangente derart, dass $C_2' \approx C_2$ gilt.

Hinweis: Die Aufgabe behandelt das Thema von **Kapitel 1.7** und ergänzt die **Aufgabe A1.17.** Auf die Pseudo–Einheit „bit/Kanalzugriff" der Kanalkapazität wird in diesen Aufgaben verzichtet.

Fragebogen zu "Z1.17: BPSK–Kanalkapazität"

a) Berechnen Sie aus dem Grenzwert für $C \to 0$ den Kurvenparameter x_0?

$$\boldsymbol{x_0} = \quad \text{dB}$$

b) Approximieren Sie $C_2(x)$ durch $C_2'(x) = 1 - \exp(-a \cdot x)$. Wie groß ist a?

$$\boldsymbol{a} =$$

c) Welche Kanalkapazität C_2' ergibt sich nach dieser Näherung für $E_B = N_0$?

$$\boldsymbol{E_B = N_0\text{: } C_2'} =$$

d) Berechnen Sie auch die Kanalkapazitätsnäherung für folgende Werte:

$$\boldsymbol{10 \cdot \lg E_B/N_0 = 2\ \text{dB}\text{: } C_2'} =$$

$$\boldsymbol{10 \cdot \lg E_B/N_0 = 4\ \text{dB}\text{: } C_2'} =$$

$$\boldsymbol{10 \cdot \lg E_B/N_0 = 6\ \text{dB}\text{: } C_2'} =$$