ZUNAME: .....

VORNAME: .....

MAT. NR.: .....

Prüfung 389.153
Musterlösung B
Datenkommunikation

Institute of Telecommunications
Görtz, Goiser, Hlawatsch, Matz, Mecklenbräuker, Rupp, Zseby
TU-Wien 18.6.2014

Bitte beachten Sie:

- Die Dauer dieser Klausur beträgt **zwei Zeitstunden**.
- **Mobiltelefone** müssen während der Prüfung **ausgeschaltet** sein und dürfen **nicht auf dem Tisch** liegen!
- Bitte legen Sie Ihren **Studierendenausweis auf Ihrem Tisch** zur Überprüfung bereit.
- Es sind (außer Schreibwerkzeugen) **keine Hilfsmittel** erlaubt, auch keine Taschenrechner!
- Bitte verwenden Sie einen **permanent färbenden, nicht-roten Stift**.
- Die Beispiele sind ausschließlich auf den Seiten dieser Angabe auszuarbeiten. **Mitgebrachte Zusatzblätter werden ignoriert!**
- Sofern weitere Leerseiten zur Bearbeitung der Beispiele benötigt werden, sind diese bei der Klausuraufsicht erhältlich.
- Bitte bearbeiten Sie ***nicht*** **mehr als ein Beispiel auf einem Blatt**.
- Bitte kennzeichnen Sie auf **jeder Seite** eindeutig, welche **Aufgabe** und welcher **Unterpunkt** behandelt wird.
- Schreiben Sie auf **jedes Blatt** Ihren **Namen** und Ihre **Matrikelnummer**!
- Diese **Angabe *muss*, mit Ihrem Namen und Ihrer Matrikelnummer beschriftet,** bei der Klausuraufsicht **abgegeben werden**. **Sie dürfen diese Angabe *nicht* mitnehmen!**
- Sofern Sie nicht wollen, dass Ihre Bearbeitung eines Beispiels gewertet wird, streichen Sie die entsprechenden Seiten klar ersichtlich durch.
- Eine **lesbare Schrift und übersichtliche Darstellung** ist eine Voraussetzung für die positive Beurteilung der Arbeit!
- Bitte **bleiben Sie bei Klausurende** so lange **auf Ihrem Platz**, bis alle Klausuren eingesammelt sind und die Klausuraufsicht die Freigabe zum Verlassen der Hörsaals erteilt.
- Sofern Sie während der Klausur zur Toilette müssen, melden Sie sich bitte rechtzeitig bei der Klausuraufsicht. Bitte **verlassen Sie nicht ohne Rücksprache mit der Klausuraufsicht den Hörsaal**.
- Sofern Sie vor dem Klausurende gehen wollen, tun Sie dies bitte **nicht in den letzten 15min** vor dem Ende der Klausur. Melden Sie sich bevor Sie gehen bei der Klausuraufsicht und geben Sie Ihre Angabe ab.

Aufgabe:	1	2	3	4	5	Summe
Punkte (max.):	20	20	20	20	20	100
Punkte:						

Aufgabe 1: (20 Punkte)

Ihr Handy-Akku kann 3600mAh speichern. Tägliche Nutzung verringert die Akkuladung um 50%. Zu kurzes Aufladen kurz vor Ende des Tages gibt dem Akku täglich nur 200mAh dazu. Wir gehen davon aus, dass der Akku am Ende des Tages $k = 0$ vollständig geladen ist.

(a) (4 Punkte) Stellen Sie eine rekursive, zeitdiskrete Gleichung im Zeitbereich für den Ladezustand $y(k), k \geq 0$, des Akkus am Ende des Tages auf, gerade nachdem die tägliche Aufladung abgeschlossen ist.

(b) (4 Punkte) Geben Sie die zugehörige Z-Transformierte an.

(c) (4 Punkte) Geben Sie einen Signalflussgraphen dazu an.

Berechnen Sie nun folgende Aufgaben:

(d) (4 Punkte) Nach wie viel Tagen sinkt die Ladung am Ende des Tages unter die Hälfte?

(e) (4 Punkte) Kann sie unter 5% sinken? Erklären Sie dies.

(a) Zeitreihe:

k	$y(k)$
0	3600
1	1800+ 200 =2000
2	1000 + 200 = 1200
3	600 + 200 = 800
4	400 + 200 = 600
5	300 + 200 = 500
6	250 + 200 = 450
7	225 + 200 = 425
8	212.5 + 200 = 412.5
	...
∞	400

Differenzengleichung:

$$\begin{aligned} y(k) &= \frac{1}{2}y(k-1) + 3600\delta(k) + 200\,U(k-1) \\ &= \frac{1}{2}y(k-1) + 3400\delta(k) + 200\,U(k) \end{aligned}$$

mit dem Anfangswert $y(-1) = 0$, dem zeitdiskreten Impuls $\delta(k)$ und dem Sprung $U(k)$.

(b) Z-Transformierte aus Transformation der Differenzengleichung:

$$Y(z) = \frac{1}{2}z^{-1}Y(z) + 3400 + 200\,\frac{z}{z-1}$$

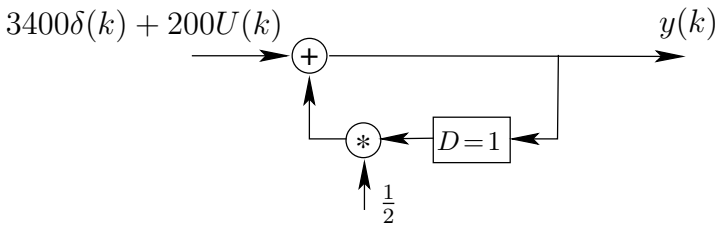
Die Z-Transformierte kann auch zur analytischen Lösung verwendet werden (*nicht* Teil der geforderten Lösung der Aufgabe):

$$
\begin{aligned}
Y(z)(1-\frac{1}{2}z^{-1}) &= 3400 + 200\,\frac{z}{z-1} \\
Y(z) &= 3400\frac{z}{z-\frac{1}{2}} + 200\frac{z^2}{(z-1)(z-\frac{1}{2})} \\
&= 3400\frac{z}{z-\frac{1}{2}} + 200\frac{z^2-\frac{3}{2}z+\frac{1}{2}+\frac{3}{2}z-\frac{1}{2}}{(z-1)(z-\frac{1}{2})} \\
&= 3400\frac{z}{z-\frac{1}{2}} \;+\; 200 \;+\; 200\frac{\frac{3}{2}z-\frac{1}{2}}{(z-1)(z-\frac{1}{2})} \\
&= 3400\frac{z}{z-\frac{1}{2}} \;+\; 200 \;+\; 200\frac{2}{z-1} - 200\frac{1}{2}\frac{1}{z-\frac{1}{2}} \\
&= 3400\frac{z}{z-\frac{1}{2}} \;+\; 200 \;+\; 400z^{-1}\frac{z}{z-1} - 100z^{-1}\frac{z}{z-\frac{1}{2}}
\end{aligned}
$$

Die analytische Lösung lautet daher

$$
\begin{aligned}
\frac{y(k)}{100} &= 34\left(\frac{1}{2}\right)^k U(k) \;+\; 2\delta(k) \;-\; 1\left(\frac{1}{2}\right)^{k-1} U(k-1) + 4\,U(k-1) \\
&= 34\left(\frac{1}{2}\right)^k U(k) + 2\delta(k) - \left(1\left(\frac{1}{2}\right)^{k-1} U(k) - 1\left(\frac{1}{2}\right)^{-1}\delta(k)\right) + (4\,U(k) - 4\delta(k)) \\
&= 34\left(\frac{1}{2}\right)^k U(k) \;+\; 2\delta(k) - \left(1\left(\frac{1}{2}\right)^{k-1} U(k) - 2\delta(k)\right) + (4\,U(k) - 4\delta(k)) \\
&= 32\left(\frac{1}{2}\right)^k U(k) \;+\; 4\,U(k) \qquad \Rightarrow \quad y(k) = 3200\left(\frac{1}{2}\right)^k U(k) \;+\; 400\,U(k)
\end{aligned}
$$

(c) Signalflussgraph:



(d) Bei $k = 2$ (siehe Tabelle) ist die Ladung kleiner als $3600/2 = 1800$.

(e) Aus Tabelle ersichtlich: Zeitreihe konvergiert, d.h. es gibt eine Konstante $y[\infty]$. Daher für $k \to \infty$: $y[\infty] = \frac{1}{2}y[\infty] + 200$ direkt aus der Differenzengleichung. Der Wert der Konstanten ist damit

$$y(\infty)(1 - 1/2) = 200 \quad \Rightarrow \quad y(\infty) = 400\,.$$

Da $400 > 180$ kann der Ladezustand nicht unter 5% sinken.

Aufgabe 2: (20 Punkte)

Eindimensionale Betrachtung: Von einem satellitengestützten Positionsbestimmungssystem ist folgendes bekannt: (1) Das Satellitensignal wird aus dem Generatorpolynom $p(x) = x^4 + x + 1$ erzeugt, (2) die Pulsform der Chips sind NRZ-Pulse, (3) die Chiprate beträgt 1 Mchip/s, (4) die Synchronisationsgenauigkeit liegt unter 3% der Chipdauer.

(a) (4 Punkte) Zeichnen Sie die Schieberegisterrealisierung des Generatorpolynoms.

(b) (4 Punkte) Bestimmen Sie die binäre Folge.

(c) (4 Punkte) Bestimmen Sie die periodische Autokorrelationsfunktion der Folge.

(d) (4 Punkte) Ist die Autokorrelationsfunktion geeignet zur Positionsbestimmung? Wenn ja, warum?

(e) (4 Punkte) Welche eindimensionale Genauigkeit der Ortsbestimmung kann, unter der Annahme von idealen Ausbreitungsverhältnissen, erreicht werden?

Hinweis: Der NRZ (no-return-to-zero) Puls entspricht einer rechteckigen Kurvenform.

(a) Durch null setzen des Generatorpolynom folgt die Schieberegisterrealisierung:

$$p(x) = x^4 + x + 1 = 0 \mapsto 1 = x^4 + x$$

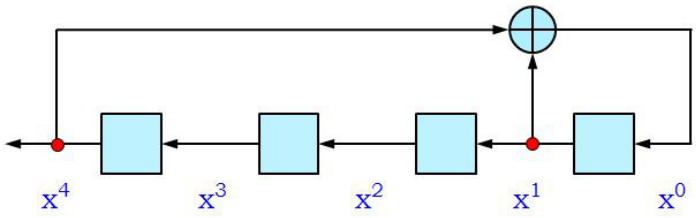


Abbildung 1: Schieberegisterrealisierung des Generatorpolynoms $p(x) = x^4 + x + 1$.

(b) Füttert man das Schieberegister mit dem Anfangszustand [0001] und bestimmt alle weiteren Zustände so erhält man die Tabelle in Abbildung 2. Aus dieser Tabelle entnimmt man die Periode $L = 15$ und die Folge am Ausgang des Schieberegisters $\overrightarrow{c} = [000111101011001]$

(c) Da es sich um eine Folge maximaler Länge $L = 2^n - 1 = 2^4 - 1 = 15$ handelt entspricht diese Folge einer PN-Folge, deren AKF zweiwertig ist, siehe Abbildung 3.

(d) Die AKF ist geeignet zur genauen Positionsbestimmung durch die Anwendung des Prinzips der Laufzeitmessung. Da über die hohe Zeitauflösung (Dirac-ähnlich) eine genaue Ortsbestimmung über die Lichtgeschwindigkeit gegeben ist.

(e) Mit der Chiprate (1 Mchip/s) und der Synchronisationsgenauigkeit folgt die räumliche Genauigkeit: Die Chipdauer, als Kehrwert der Chiprate, beträgt 1 μs. Mit der zeitlichen Synchronisation auf 3 % der Chipdauer ergibt sich eine zeitliche Auflösung von 0,03 μs. Daraus folgt eine entfernungsabhängige Genauigkeit (1-dim) von (plus/minus):

$$\Delta r = c \cdot \Delta T = 3 \cdot 10^8 \cdot 10^{-6} \cdot 0.03 = 9m$$

Takt	Register	Ausgang
0	**0001**	0
1	0011	0
2	0111	0
3	1111	1
4	1110	1
5	1101	1
6	1010	1
7	0101	0
8	1011	1
9	0110	0
10	1100	1
11	1001	1
12	0010	0
13	0100	0
14	1000	1
15	**0001**	0

Abbildung 2: Schieberegisterzustände für Generatorpolynom $p(x) = x^4 + x + 1$.

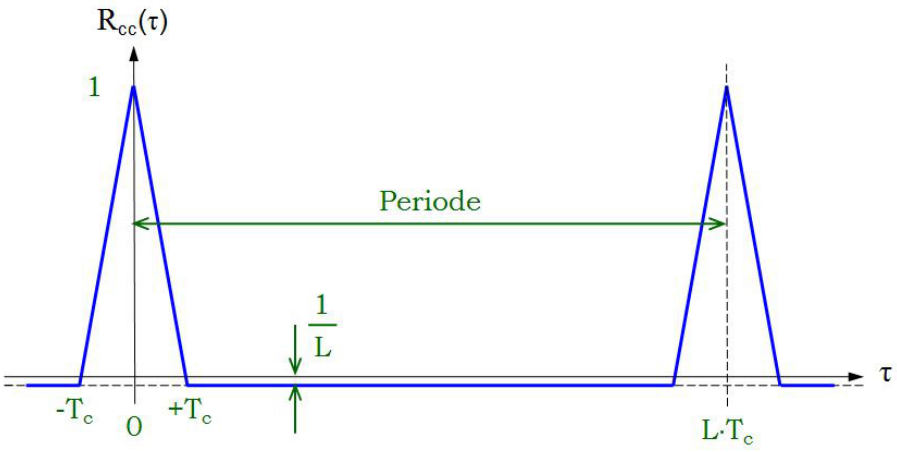


Abbildung 3: AKF einer m-Folge.

Aufgabe 3: (20 Punkte)

Betrachten Sie folgende gedächtnislose diskrete Quelle:

U	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8
$P(U)$	1/4	1/4	1/8	1/8	1/16	1/16	1/16	1/16

(a) (3 Punkte) Gibt es für diese Quelle einen präfixfreien binären Code mit Codewortlängen $w_1 = 1$, $w_2 = 3$, $w_3 = w_4 = w_5 = w_6 = w_7 = w_8 = 4$? Begründen Sie Ihre Antwort.

(b) (7 Punkte) Entwerfen Sie einen binären Huffman-Code für die gegebene Quelle.

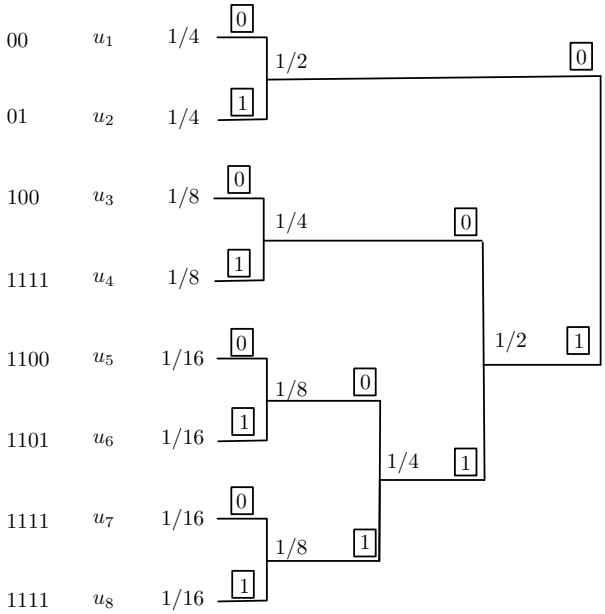
(c) (8 Punkte) Vergleichen Sie die mittlere Codewortlänge Ihres Huffman-Codes mit der Entropie der Quelle (in bit).

(d) (2 Punkte) Wieviele Bits benötigt man bei einem binären Code konstanter Länge?

U	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8
$P(U)$	1/4	1/4	1/8	1/8	1/16	1/16	1/16	1/16
$-\log_2 P(U)$	2	2	3	3	4	4	4	4
$-P(U)\log_2 P(U)$	4/8	4/8	3/8	3/8	2/8	2/8	2/8	2/8

(a) Ja, da Kraftsche Ungleichung erfüllt: $\sum_{i=1}^{8} 2^{-w_i} = 2^{-1} + 2^{-3} + 6 \cdot 2^{-4} = 1 \leq 1$.

(b)



(c)

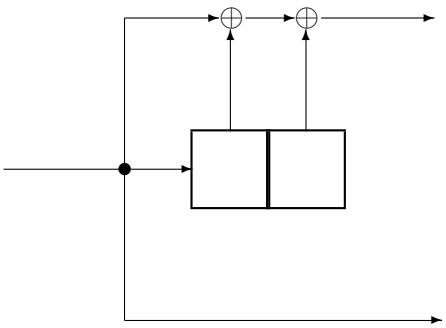
$E[W] = \sum_{i=1}^{8} w_i\, p_i = 2{\cdot}1/4{+}2{\cdot}1/4{+}3{\cdot}1/8{+}3{\cdot}1/8{+}4{\cdot}1/16{+}4{\cdot}1/16{+}4{\cdot}1/16{+}4{\cdot}1/16 = \frac{11}{4} = 2\frac{3}{4} = 2.75$

$H(U) = -\sum_{i=1}^{8} P(u_i) \log_2 P(u_i) = \frac{22}{8} = 2\frac{3}{4} = 2.75\,\text{bit}$

(d) $\log_2(L) = \log_2(8) = 3\,\text{bit}$

Aufgabe 4: (20 Punkte)

Gegeben sei der folgende Faltungscodierer:



(a) (4 Punkte) Wieviele verschiedene innere Zustände hat dieser Codierer?

(b) (4 Punkte) Zeichnen Sie das Zustandsdiagramm!

(c) (4 Punkte) Bestimmen Sie die Codesequenz, die sich aus der Informationssequenz 01000 11 ergibt.

(d) (4 Punkte) Zeichnen Sie das Trellisdiagramm dieses Codierers.

(e) (4 Punkte) Es wurde die fehlerhafte Sequenz 1010 1010 1010 1001 empfangen. Decodieren Sie mit dem Viterbi-Algorithmus.

Musterlösung, siehe Anhang

Aufgabe 5: (20 Punkte)

Alice möchte über das RSA Verfahren mit Bob verschlüsselt kommunizieren. Dazu denkt sie sich 2 Primzahlen $p = 11, q = 3$ aus und berechnet $n = p \cdot q = 33$

Anmerkung: In der Aufgabe soll nur die *reine RSA Trapdoorfunktion* angewendet werden (ohne die in der Praxis verwendete Hashfunktion)

(a) (2 Punkte) Berechnen Sie $\varphi(n)$, die Anzahl der Zahlen $(1 \leq x \leq n)$, die teilerfremd zu n sind (Formel und Berechnung)

(b) (4 Punkte) Alice wählt als öffentlichen Schlüssel e=7. Und bestimmt den geheimen Schlüssel d=3. In welcher Beziehung müssen die Zahlen e und d stehen, damit das RSA Verfahren funktioniert? (Formel)

(c) (4 Punkte) Kreuzen Sie an (x) welche Zahlen Alice öffentlich bekannt gibt, damit das RSA Verfahren angewendet werden kann.

Zahl	p	q	e	d	n	$\varphi(n)$
öffentlich?						

(d) (6 Punkte) Bob möchte die Nachricht $m = 6$ verschlüsselt an Alice senden. Wie berechnet er die verschlüsselte Nachricht c? (Formel und Berechnung)

Hinweis: $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$

(e) (4 Punkte) Alice möchte für die Nachricht m=2 eine Signatur erstellen. Berechnen Sie den Wert der Signatur *sig*. (Formel und Berechnung)

(a)

$$\varphi(n) = (p-1) \cdot (q-1) = 10 \cdot 2 = 20$$

(b)

$$e \cdot d \equiv 1 \mod \varphi(n)$$

(c)

Zahl	p	q	e	d	n	$\varphi(n)$
öffentlich?	-	-	x	-	x	-

(d)

$$\begin{aligned} c = m^e \bmod n &= 6^7 \bmod 33 \\ &= ((6^2 \bmod 33) \cdot (6^2 \bmod 33) \cdot (6^2 \bmod 33) \cdot (6 \bmod 33)) \bmod 33 \\ &= (3 \cdot 3 \cdot 3 \cdot 6) \bmod 33 \\ &= ((3 \bmod 33) \cdot (54 \bmod 33)) \bmod 33 \\ &= (3 \cdot 21) \bmod 33 \\ &= 63 \bmod 33 \\ &= 30 \end{aligned}$$

(e)

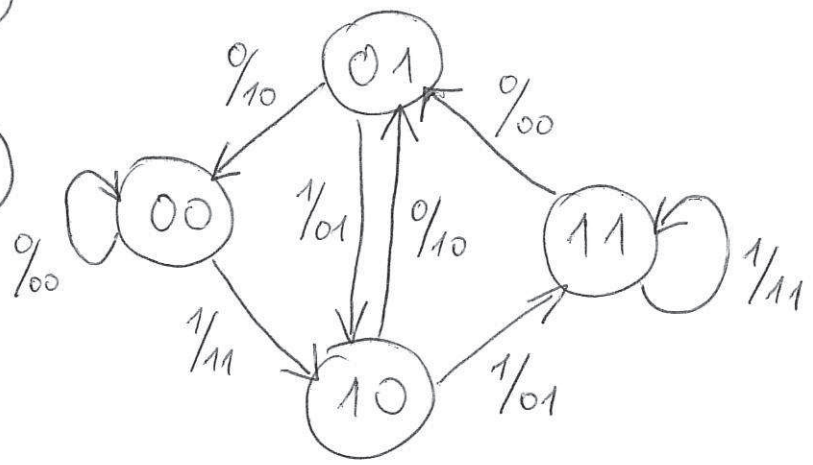
$$c = m^d \bmod n = 2^3 \bmod 33 = 8$$

B

Zuname:..... Matrikelnummer:.....

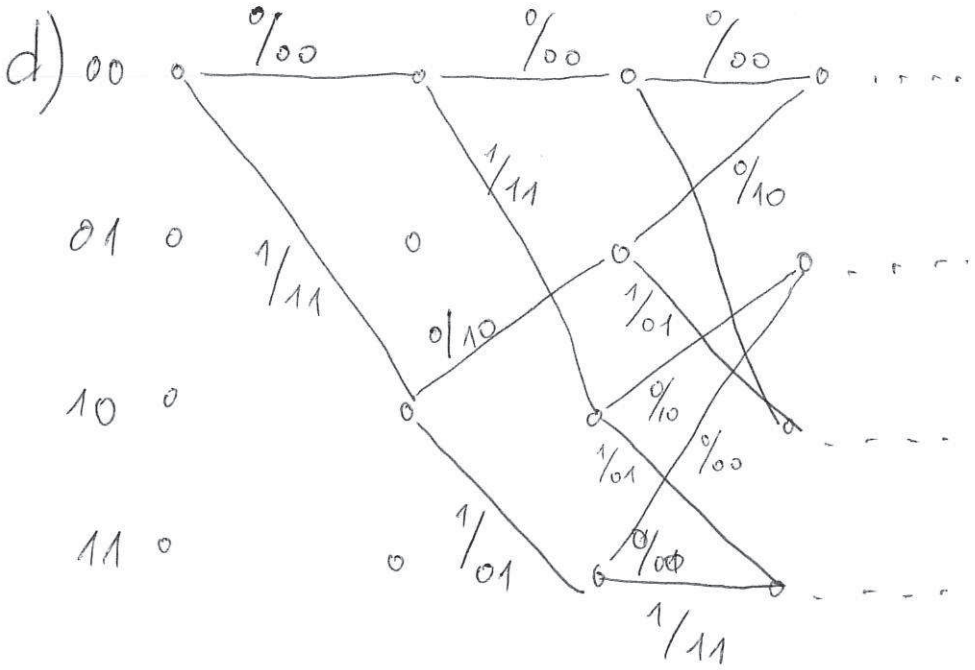
a) vier

b)



c) 00 11 10 10 00 11 01

d)

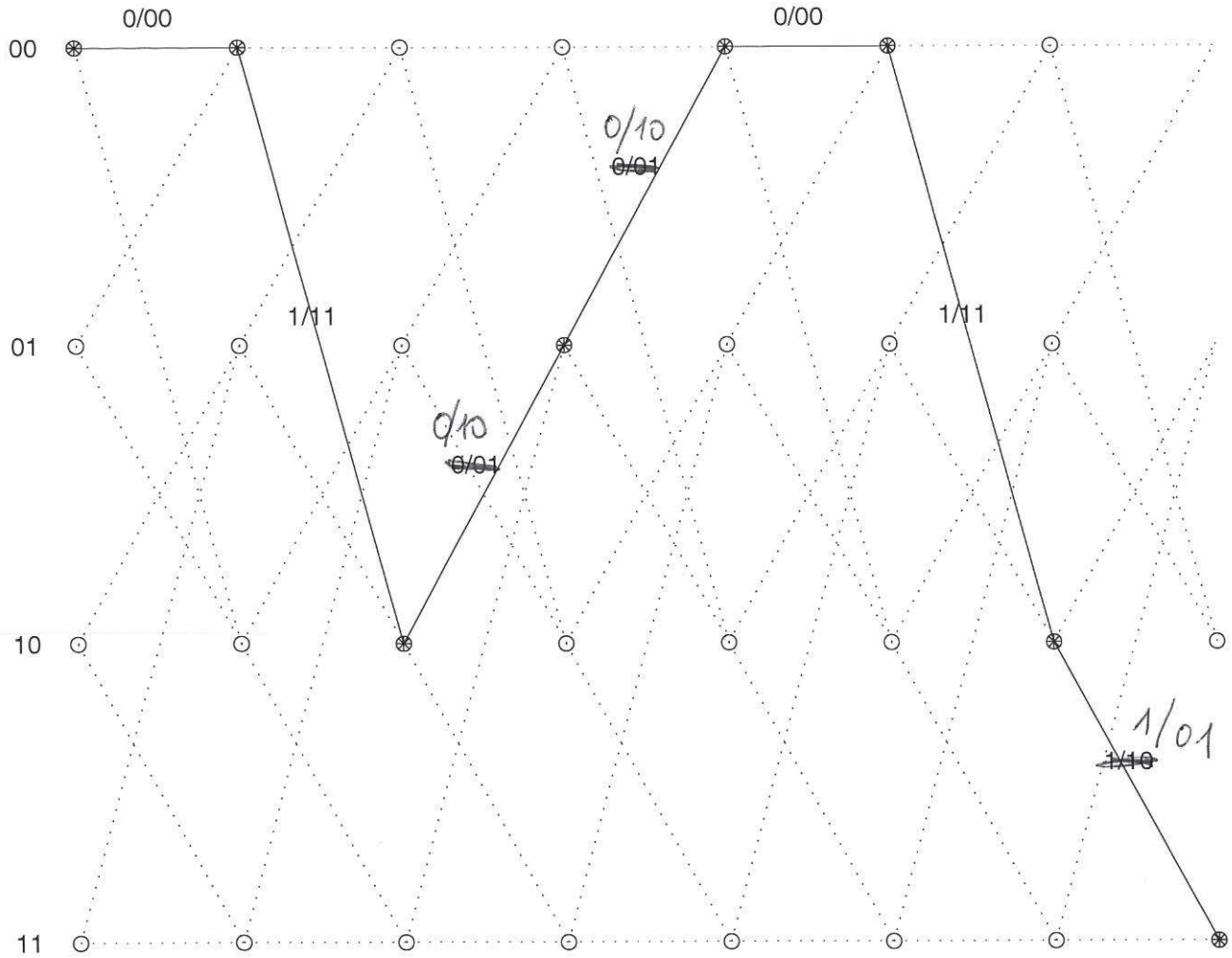


e) 10010011

(B)

c) input: 01000 11

output: 00 11 10 10 00 11 01

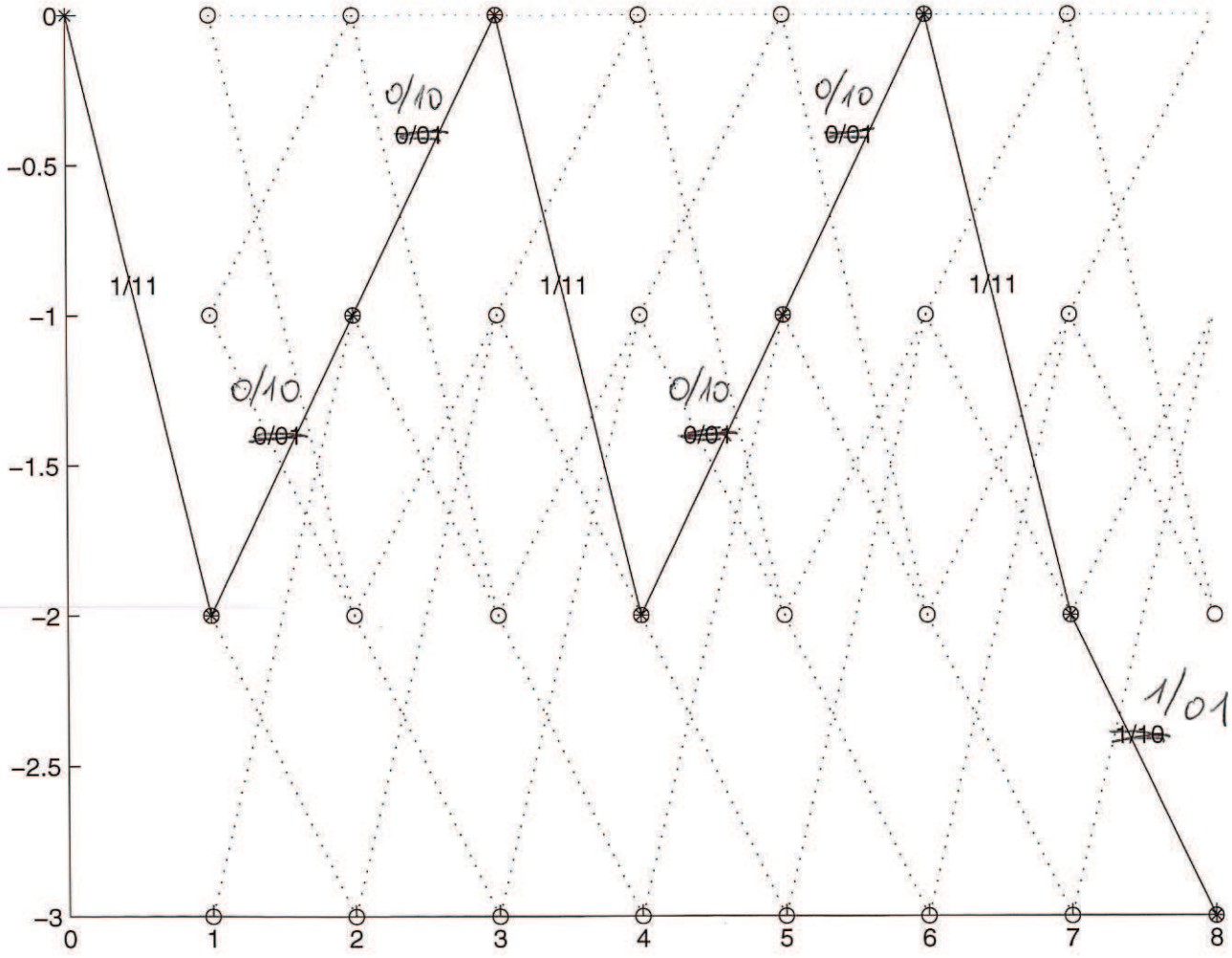


B

e) fehlerhafte Sequenz: ~~1~~ 1 0 ~~1~~ 0 1 0 1 0 ~~1~~ 0 0 1

Codesequenz : 1 1 1 0 1 0 1 1 1 0 1 0 1 1 0 1

minimum Hamming distanz = 3



decodierte Infobits: 1 0 0 1 0 0 1 1