Diskrete Strukturen

Sommer 2019

Prof. Stefan Lucks, Jannis Bossert
<firstname>.<lastname>(at)uni-weimar.de

Bauhaus-Universität Weimar

January 9, 2020

Aufgabe 1: Isomorphismus

Überprüfen Sie, ob die folgenden Gruppoide Isomorph sind.

a) $(\mathbb{Z}_7^*, \cdot)$ und $(\mathbb{Z}_6, +)$

b) $(\mathbb{Z}_6, +)$ und $(\mathbb{Z}_6, -)$

Hinweis: Beachten Sie dass für einen Generator $g \in \mathbb{Z}_p^*$ bekanntlich gilt: $g^{a+b} \bmod p = (g^a \cdot g^b) \bmod p$.

Aufgabe 1: Isomorphismus

Überprüfen Sie, ob die folgenden Gruppoide Isomorph sind.

a) $(\mathbb{Z}_7^*, \cdot)$ und $(\mathbb{Z}_6, +)$

b) $(\mathbb{Z}_6, +)$ und $(\mathbb{Z}_6, -)$

Hinweis: Beachten Sie dass für einen Generator $g \in \mathbb{Z}_p^*$ bekanntlich gilt: $g^{a+b} \bmod p = (g^a \cdot g^b) \bmod p$.

Gegeben seien Gruppen $(\mathcal{G}, \circ)$ und $(\mathcal{H}, \bullet)$. Beide sind isomorph genau dann wenn eine bijektive Abbildung $f : \mathcal{G} \to \mathcal{H}$ existiert sodass für alle $u, v \in \mathcal{G}$:

$$f(u \circ v) = f(u) \bullet f(v).$$

Implizit muss gelten $|\mathcal{G}| = |\mathcal{H}|$.

Ismorphismus

a) Gesucht ist eine Permutation $\pi : \mathbb{Z}_6 \to \mathbb{Z}_7^*$ sodass $a, b \in \mathbb{Z}_6$: $\pi(a+b) = \pi(a) \cdot \pi(b)$.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Aufgabe 1: Isomorphismus

Für einen Generator $g \in \mathbb{Z}_7^*$ gilt

$$\pi(a) = g^a \bmod 7$$
$$\pi(a+b) = g^{a+b} \bmod 7 = g^a \cdot g^b \bmod 7.$$

Ein Beispielgenerator in $\mathbb{Z}_7^*$ ist 3: $\langle 3 \rangle = \{3, 2, 6, 4, 5, 1\}$.

π	0	1	2	3	4	5
	1	3	2	6	5	1

$\pi(x) \cdot \pi(y)$	0	1	2	3	4	5
0	1	3	2	6	4	5
1	3	2	6	4	5	1
2	2	6	4	5	1	3
3	6	4	5	1	3	2
4	4	5	1	3	2	6
5	5	1	3	2	6	4

Fazit: $(\mathbb{Z}_6, +)$ und $(\mathbb{Z}_7^*, \cdot)$ sind isomorph.

Aufgabe 1: Isomorphismus

b) $(\mathbb{Z}_6, +)$ und $(\mathbb{Z}_6, -)$

Aufgabe 1: Isomorphismus

b) $(\mathbb{Z}_6, +)$ und $(\mathbb{Z}_6, -)$ sind nicht isomorph.

$-$	0	1	2	3	4	5
0	0	5	4	3	2	1
1	1	0	5	4	3	2
2	2	1	0	5	4	3
3	3	2	1	0	5	4
4	4	3	2	1	0	5
5	5	4	3	2	1	0

Für eine Permutation $\pi : \mathbb{Z}_6 \to \mathbb{Z}_6$ mit $\pi(a+b) = \pi(a) - \pi(b)$ muss gelten, dass $\pi(a) \neq \pi(b)$ für alle $a \neq b \in \mathbb{Z}_6$. Es gilt aber dass zwei Werte auf den selben abgebildet werden würden:

$$\pi(2) = \pi(1+1) = \pi(1) - \pi(1) = 0$$
$$\pi(4) = \pi(2+2) = \pi(2) - \pi(2) = 0.$$

Daraus würde folgen dass $\pi(2) = \pi(4)$, was ein Widerspruch ist.

Aufgabe 2: Diffie-Hellman-Schlüsselaustausch

Alice und Bob haben sich mit Hilfe des Diffie-Hellman-Schlüsselaustausches auf einen geheimen Schlüssel K geeinigt. Eve hat im Laufe des Austausches folgende Parameter von der unsicheren Leitung abgehört: $p = 67$, $g = 13$, $A = 64$, $B = 2$. Ermitteln Sie den geheimen Schlüssel K nur mit Hilfe dieser Informationen.

Aufgabe 2: Diffie-Hellman-Schlüsselaustausch

Alice und Bob haben sich mit Hilfe des Diffie-Hellman-Schlüsselaustausches auf einen geheimen Schlüssel K geeinigt. Eve hat im Laufe des Austausches folgende Parameter von der unsicheren Leitung abgehört: $p = 67$, $g = 13$, $A = 64$, $B = 2$. Ermitteln Sie den geheimen Schlüssel K nur mit Hilfe dieser Informationen.

Für den Diffie-Hellman-Schlüsselaustausch gilt:

$$
\begin{aligned}
a, b &\twoheadleftarrow \mathbb{Z}_p^* \\
A &= g^a \bmod p \\
B &= g^b \bmod p \\
K &= A^b \bmod p = B^a \bmod p = g^{ab} \bmod p.
\end{aligned}
$$

Aufgabe 2: Diffie-Hellman-Schlüsselaustausch

Wir erhalten mit Hilfe eines kleinen Pythonskripts die multiplikative Gruppe von $g \in \mathbb{Z}_p^*$:

(1, 13), (2, 35), (3, 53), (4, 19), (5, 46), (6, 62), (7, 2), (8, 26), (9, 3), (10, 39), (11, 38), (12, 25), (13, 57), (14, 4), (15, 52), (16, 6), (17, 11), (18, 9), (19, 50), (20, 47), (21, 8), (22, 37), (23, 12), (24, 22), (25, 18), (26, 33), (27, 27), (28, 16), (29, 7), (30, 24), (31, 44), (32, 36), (33, 66), (34, 54), (35, 32), (36, 14), (37, 48), (38, 21), (39, 5), (40, 65), (41, 41), (42, 64), (43, 28), (44, 29), (45, 42), (46, 10), (47, 63), (48, 15), (49, 61), (50, 56), (51, 58), (52, 17), (53, 20), (54, 59), (55, 30), (56, 55), (57, 45), (58, 49), (59, 34), (60, 40), (61, 51), (62, 60), (63, 43), (64, 23), (65, 31), (66, 1)

Aufgabe 2: Diffie-Hellman-Schlüsselaustausch

Wir erhalten mit Hilfe eines kleinen Pythonskripts die multiplikative Gruppe von $g \in \mathbb{Z}_p^*$:

(1, 13), (2, 35), (3, 53), (4, 19), (5, 46), (6, 62), (7, 2), (8, 26), (9, 3), (10, 39), (11, 38), (12, 25), (13, 57), (14, 4), (15, 52), (16, 6), (17, 11), (18, 9), (19, 50), (20, 47), (21, 8), (22, 37), (23, 12), (24, 22), (25, 18), (26, 33), (27, 27), (28, 16), (29, 7), (30, 24), (31, 44), (32, 36), (33, 66), (34, 54), (35, 32), (36, 14), (37, 48), (38, 21), (39, 5), (40, 65), (41, 41), (42, 64), (43, 28), (44, 29), (45, 42), (46, 10), (47, 63), (48, 15), (49, 61), (50, 56), (51, 58), (52, 17), (53, 20), (54, 59), (55, 30), (56, 55), (57, 45), (58, 49), (59, 34), (60, 40), (61, 51), (62, 60), (63, 43), (64, 23), (65, 31), (66, 1)

Dieser können wir entnehmen das $a = \mathrm{DLog}_{13}(64) = 42$ und $b = \mathrm{DLog}_{13}(2) = 7$. Daraus folgt dass $K = 13^{42 \cdot 7} \bmod 67 \equiv 24$.

Aufgabe 3: Shamir-Secret-Sharing

Um ein Geheimnis $S = p(0)$ eines Polynoms p nicht einer einzelnen Person anzuvertrauen, wurden 3 Paare $(x_i, p(x_i))$ an 3 Personen weitergereicht. Finden Sie an Hand der Wertepaare

$$(a_1, b_1) = (3, 207)$$
$$(a_2, b_2) = (6, 274)$$
$$(a_3, b_3) = (7, 53),$$

mit $a_i, b_i \in \mathbb{Z}_{503}$ das Geheimnis $S = p(0)$ mit Hilfe der Interpolationsformel von Lagrange heraus.

Aufgabe 3: Shamir-Secret-Sharing

Es gilt

$$p(x) = \sum_{i=1}^{n} \left(b_i \cdot \prod_{j \neq i} \frac{x - a_j}{a_i - a_j} \right).$$

Wir zerlegen das Polynom in drei Teilsummanden:

$$p_1(x) = b_1 \frac{x - a_2}{a_1 - a_2} \frac{x - a_3}{a_1 - a_3}$$

$$p_2(x) = b_2 \frac{x - a_1}{a_2 - a_1} \frac{x - a_3}{a_2 - a_3}$$

$$p_3(x) = b_3 \frac{x - a_1}{a_3 - a_1} \frac{x - a_2}{a_3 - a_2}$$

Aufgabe 3: Shamir-Secret-Sharing

Summand 1:

$$
\begin{aligned}
p_1(x) &= b_1 \frac{x - a_2}{a_1 - a_2} \frac{x - a_3}{a_1 - a_3} \\
&= 207 \cdot \frac{x - 6}{-3} \frac{x - 7}{-4} \\
&= 207 \cdot 12^{-1} \cdot (x^2 - 13x + 42).
\end{aligned}
$$

Aufgabe 3: Shamir-Secret-Sharing

Summand 1:

$$
\begin{aligned}
p_1(x) &= b_1 \frac{x - a_2}{a_1 - a_2} \frac{x - a_3}{a_1 - a_3} \\
&= 207 \cdot \frac{x - 6}{-3} \frac{x - 7}{-4} \\
&= 207 \cdot 12^{-1} \cdot (x^2 - 13x + 42).
\end{aligned}
$$

Nebenrechnung: $12^{-1} \bmod 503 \equiv 42$.

Aufgabe 3: Shamir-Secret-Sharing

Summand 1:

$$
\begin{aligned}
p_1(x) &= b_1 \frac{x - a_2}{a_1 - a_2} \frac{x - a_3}{a_1 - a_3} \\
&= 207 \cdot \frac{x - 6}{-3} \frac{x - 7}{-4} \\
&= 207 \cdot 12^{-1} \cdot (x^2 - 13x + 42).
\end{aligned}
$$

Nebenrechnung: $12^{-1} \bmod 503 \equiv 42$.

Also:

$$
\begin{aligned}
&= 207 \cdot 42 \cdot (x^2 - 13x + 42) \bmod 503 \\
&\equiv 143x^2 + 153x + 473.
\end{aligned}
$$

Aufgabe 3: Shamir-Secret-Sharing

Summand 2:

$$
\begin{aligned}
p_2(x) &= b_2 \frac{x - a_1}{a_2 - a_1} \frac{x - a_3}{a_2 - a_3} \\
&= 274 \cdot \frac{x - 3}{3} \frac{x - 7}{-1} \\
&= 274 \cdot (-3)^{-1} \cdot (x^2 - 10x + 21).
\end{aligned}
$$

Aufgabe 3: Shamir-Secret-Sharing

Summand 2:

$$
\begin{aligned}
p_2(x) &= b_2 \frac{x - a_1}{a_2 - a_1} \frac{x - a_3}{a_2 - a_3} \\
&= 274 \cdot \frac{x - 3}{3} \frac{x - 7}{-1} \\
&= 274 \cdot (-3)^{-1} \cdot (x^2 - 10x + 21).
\end{aligned}
$$

Nebenrechnung: $(-3)^{-1} \bmod 503 \equiv 335. \qquad 335 \cdot 274 \bmod 503 = 244.$

Aufgabe 3: Shamir-Secret-Sharing

Summand 2:

$$
\begin{aligned}
p_2(x) &= b_2 \frac{x - a_1}{a_2 - a_1} \frac{x - a_3}{a_2 - a_3} \\
&= 274 \cdot \frac{x - 3}{3} \frac{x - 7}{-1} \\
&= 274 \cdot (-3)^{-1} \cdot (x^2 - 10x + 21).
\end{aligned}
$$

Nebenrechnung: $(-3)^{-1} \bmod 503 \equiv 335. \qquad 335 \cdot 274 \bmod 503 = 244.$

Also:

$$
\begin{aligned}
&= 244 \cdot (x^2 - 10x + 21) \bmod 503 \\
&\equiv 244x^2 + 75x + 94 \bmod 503.
\end{aligned}
$$

Summand 3:

$$\begin{aligned} p_3(x) &= b_3 \frac{x - a_1}{a_3 - a_1} \frac{x - a_2}{a_3 - a_2} \\ &= 53 \cdot \frac{x - 3}{4} \frac{x - 6}{1} \\ &= 53 \cdot 4^{-1}(x^2 - 9x + 18). \end{aligned}$$

Shamir-Secret-Sharing

Summand 3:

$$
\begin{aligned}
p_3(x) &= b_3 \frac{x - a_1}{a_3 - a_1} \frac{x - a_2}{a_3 - a_2} \\
&= 53 \cdot \frac{x - 3}{4} \frac{x - 6}{1} \\
&= 53 \cdot 4^{-1}(x^2 - 9x + 18).
\end{aligned}
$$

Nebenrechnung: $4^{-1} \bmod 503 \equiv 126.$ $\quad 53 \cdot 126 \bmod 503 \equiv 139.$

Shamir-Secret-Sharing

Summand 3:

$$
\begin{aligned}
p_3(x) &= b_3 \frac{x - a_1}{a_3 - a_1} \frac{x - a_2}{a_3 - a_2} \\
&= 53 \cdot \frac{x - 3}{4} \frac{x - 6}{1} \\
&= 53 \cdot 4^{-1}(x^2 - 9x + 18).
\end{aligned}
$$

Nebenrechnung: $4^{-1} \bmod 503 \equiv 126.$ $\quad 53 \cdot 126 \bmod 503 \equiv 139.$

Also:

$$
\begin{aligned}
&\equiv 139 \cdot (x^2 - 9x + 18) \bmod 503 \\
&\equiv (139x^2 + 258x + 490) \bmod 503
\end{aligned}
$$

Aufgabe 3: Shamir-Secret-Sharing

Wir können nun berechnen:

$$\begin{aligned} p(x) &= 143x^2 + 153x + 473 + 244x^2 + 75x + 94 + 139x^2 + 258x + 490 \\ &\equiv 23x^2 + 486x + 51. \end{aligned}$$

Damit gilt

$$p(0) = 51.$$

Probe:

$$\begin{aligned} p(3) &= 23 \cdot 9 + 486 \cdot 3 + 51 \equiv 207 \mod 503 \\ p(6) &= 23 \cdot 36 + 486 \cdot 6 + 51 \equiv 274 \mod 503 \\ p(7) &= 23 \cdot 49 + 486 \cdot 7 + 51 \equiv 53 \mod 503 \end{aligned}$$

Aufgabe 4: Irreduzible Polynome

Betrachten Sie den Körper $\mathbb{Z}_2[X]_{p(\mathtt{x})}$.

a) Zeigen oder widerlegen Sie: $p(\mathtt{x}) = \mathtt{x}^4 + \mathtt{x} + 1$ ist irreduzibel über $\mathbb{Z}_2$.

b) Zeigen oder widerlegen Sie: $p(\mathtt{x}) = \mathtt{x}^4 + \mathtt{x}^3 + \mathtt{x}^2 + 1$ ist irreduzibel über $\mathbb{Z}_2$.

c) Stellen Sie für alle Elemente aus $\mathbb{Z}_2[X]_{p(\mathtt{x})}$ mit $p(\mathtt{x}) = \mathtt{x}^3 + \mathtt{x}^2 + 1$ die Additions- und Multiplikationstabelle auf.

Aufgabe 4: Irreduzible Polynome

Sei n der Grad von $p(\mathtt{x})$. Da die Koeffizienten $a_i \in \mathbb{Z}_2 = \{0, 1\}$ liegen, können wir die Elemente $q \in \mathbb{Z}_2[X]_{p(\mathtt{x})}$ als n-bit-Strings darstellen:

$$q = a_{n-1} \cdot \mathtt{x}^{n-1} + a_{n-2} \cdot \mathtt{x}^{n-2} + \ldots + a_1 \cdot \mathtt{x} + a_0.$$

Beispielsweise können wir $0 = (000)_2 = \mathtt{0}$, $1 = (001)_2 = \mathtt{1}$, $2 = (010)_2 = \mathtt{x}$, $3 = (011)_2 = \mathtt{x} + \mathtt{1}$, $\ldots$, $7 = (111)_2 = (\mathtt{x}^2 + \mathtt{x} + \mathtt{1})$ repräsentieren.

Aufgabe 4: Irreduzible Polynome

a) $p(\mathrm{x})$ ist irreduzibel wenn kein Paar $q(\mathrm{x})$, $r(\mathrm{x})$ existiert mit $p(\mathrm{x}) = q(\mathrm{x}) \cdot r(\mathrm{x})$ und $\deg(q), \deg(r) > 0$.
Es reicht alle Polynome von Grad 1 oder 2 als Kandidaten für $q(\mathrm{x})$ zu überprüfen:

Aufgabe 4: Irreduzible Polynome

a) $p(\mathrm{x})$ ist irreduzibel wenn kein Paar $q(\mathrm{x})$, $r(\mathrm{x})$ existiert mit $p(\mathrm{x}) = q(\mathrm{x}) \cdot r(\mathrm{x})$ und $\deg(q), \deg(r) > 0$.
Es reicht alle Polynome von Grad 1 oder 2 als Kandidaten für $q(\mathrm{x})$ zu überprüfen:

```
10011 / 10 = 1001 Rest 1
10
 00
  00
   10
    1
```

Aufgabe 4: Irreduzible Polynome

a) $p(\mathrm{x})$ ist irreduzibel wenn kein Paar $q(\mathrm{x})$, $r(\mathrm{x})$ existiert mit $p(\mathrm{x}) = q(\mathrm{x}) \cdot r(\mathrm{x})$ und $\deg(q), \deg(r) > 0$.
Es reicht alle Polynome von Grad 1 oder 2 als Kandidaten für $q(\mathrm{x})$ zu überprüfen:

```
10011 / 10 = 1001 Rest 1
10011 / 11 = 1010 Rest 1
10011 / 100 = 100 Rest 11
10011 / 101 = 101 Rest 10
10011 / 110 = 111 Rest 1
10011 / 111 = 110 Rest 1
```

$\rightarrow p(\mathrm{x})$ ist irreduzibel.

Aufgabe 4: Irreduzible Polynome

b) $x^4 + x^3 + x^2 + 1$

Aufgabe 4: Irreduzible Polynome

b) $x^4 + x^3 + x^2 + 1$

Nein: $(x^3 + x + 1) \cdot (x + 1) = x^4 + x^3 + x^2 + 1$

Aufgabe 4: Irreduzible Polynome

c) Stellen Sie für alle Elemente aus $\mathbb{Z}_2[X]_{p(\mathtt{x})}$ mit $p(\mathtt{x}) = \mathtt{x}^3 + \mathtt{x}^2 + 1$ die Additions- und Multiplikationstabelle auf.

Aufgabe 4: Irreduzible Polynome

c) Stellen Sie für alle Elemente aus $\mathbb{Z}_2[X]_{p(\mathrm{x})}$ mit $p(\mathrm{x}) = \mathrm{x}^3 + \mathrm{x}^2 + 1$ die Additions- und Multiplikationstabelle auf.

$+$	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

Aufgabe 4: Irreduzible Polynome

c) Stellen Sie für alle Elemente aus $\mathbb{Z}_2[X]_{p(\mathtt{x})}$ mit $p(\mathtt{x}) = \mathtt{x}^3 + \mathtt{x}^2 + 1$ die Additions- und Multiplikationstabelle auf.

$+$	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

$\cdot$	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	101	111	001	011
011	000	011	110	101	001	010	111	100
100	000	100	101	001	111	011	010	110
101	000	101	111	010	011	110	100	001
110	000	110	001	111	010	100	011	101
111	000	111	011	100	110	001	101	010

Aufgabe 5: Galoiskörper Multiplikation

Berechnen sie folgende Aufgaben im $\mathbb{GF}(2^8)$ zum irreduziblen Polynom $p(x) = x^8 + x^4 + x^3 + x + 1$.

a) $(x^7 + x^6 + x + 1) \cdot (x^2 + 1)$

b) $(x^5 + x^4 + x^2) \cdot (x^2 + 1)$

Wir stellen unsere Polynome als Bitstring dar. Somit wird $p(x)$ zu $(100011011)_2 = (11b)_{16}$. Des weitern repräsentieren wir die Multiplikation in $\mathbb{GF}(2^8)$ mit $\circ$, wobei gilt:

$$f(x) \circ x = i \begin{cases} f(x) \cdot x & \text{,wenn } deg(f(x)) < 7 \\ f(x) \cdot x \oplus p(x) & \text{, sonst} \end{cases}$$

und wo $f(x) \circ x^j$ die j malige Anwendung von $f(x) \circ x$ ist.

Aufgabe 5: Galoiskörper Multiplikation

a)

$$f(x) = (x^7 + x^6 + x + 1) = (11000011)_2$$
$$g(x) = (x^2 + 1) = (101)_2$$

$$\begin{aligned}
(x^7 + x^6 + x + 1) \cdot (x^2 + 1) &= f(x) \cdot x^2 \oplus f(x) \cdot 1 \\
&= (11000011)_2 \cdot (100)_2 \oplus (11000011)_2 \\
&= (11000011 \cdot 10 \oplus 100011011) \circ 10 \oplus 11000011 \\
&= (110000110 \oplus 100011011) \circ 10 \oplus 11000011 \\
&= 10011101 \circ 10 \oplus 11000011 \\
&= 10011101 \cdot 10 \oplus 100011011 \oplus 11000011 \\
&= 100111010 \oplus 100011011 \oplus 11000011 \\
&= 00100001 \oplus 11000011 = 11100010 \\
&= 11100010 = x^7 + x^6 + x^5 + x
\end{aligned}$$

Aufgabe 5: Galoiskörper Multiplikation

b)

$$f(x) = (x^5 + x^4 + x^2) = (00110100)_2$$
$$g(x) = (x^2 + 1) = (101)_2$$

$$\begin{aligned}
(x^5 + x^4 + x^2) \cdot (x^2 + 1) &= f(x) \cdot x^2 \oplus f(x) \cdot 1 \\
&= (00110100)_2 \cdot (100)_2 \oplus (00110100)_2 \\
&= (00110100 \cdot 10) \circ 10 \oplus 00110100 \\
&= 01101000 \circ 10 \oplus 00110100 \\
&= 11010000 \oplus 00110100 \\
&= 11100100 = x^7 + x^6 + x^5 + x^2
\end{aligned}$$

Aufgabe 6: CRC

Implementieren Sie das CRC Verfahren von Folie 203 ff. der Vorlesung in Python3. Ihr Programm soll dabei zwei Parameter entgegen nehmen:

- Das Generatorpolynom P(x) von Grad n
- Eine Empfangene Nachricht der Länge $s + n$ Bit, wobei s variabel ist

Beide Eingaben sollen als Binärstring via Kommandozeilenparameter eingelesen werden. Ihr Programm soll ausgeben, ob ein Fehler bei der Übertragung aufgetreten ist und wenn nein, die entsprechende Nachricht.

Fragen?