

Diskrete Strukturen, SS 06

Scheinklausur**Bearbeitungszeit:** 120 Minuten.**Zugelassene Hilfsmittel:** Ein beliebig beschriebenes Blatt DIN A4 und ein nichtprogrammierbarer Taschenrechner.

Es sind insgesamt 36 Punkte erreichbar.

Ist ein **Kasten** bei einer Frage, so bitte die Antwort in den Kasten. Die für diese Antwort benötigten Rechnungen gehen diesenfalls in die Bewertung nicht ein. Eine falsche Antwort gibt 0 Punkte (aber keine negativen Punkte).Bitte zu jeder Bearbeitung einer Frage **ohne Kasten** deutlich die Aufgabennummer angeben.

Wer mehr Papier benötigt, bitte melden.

Aufgabe 1**(1+2+2+1 Punkte)**

- (1) Auf wieviele Arten kann man 4 Kugeln aus 4 Kugeln ziehen, wenn man jeweils wieder zurücklegt und nicht auf die Reihenfolge achtet?
- (2) Bestimme die Ordnung des Elements $((1, 3, 2) \circ (1, 4, 3) \circ (1, 3))^2$ von \mathcal{S}_4 .
- (3) Seien 5 verschiedene Briefe in 5 verschiedene Briefumschläge zu stecken. Wieviele Möglichkeiten gibt es, keinen Brief in den richtigen Umschlag zu stecken? (Hinweis: Permutationen, Fixpunkte.)
- (4) Bestimme $\mu(91)$.

Aufgabe 2**(6 Punkte)**Bestimme das Polynom $f(X) \in \mathbf{F}_2[X]$ von Grad < 6 , welches folgenden Kongruenzen genügt, und trage es hier ein: . (Hinweis: Euklid.)

$$\begin{aligned} f(X) &\equiv_X 1 \\ f(X) &\equiv_{X^2+X+1} 1 \\ f(X) &\equiv_{X^3+X+1} X^2 \end{aligned}$$

Aufgabe 3**(4+2 Punkte)**Sei $m \geq 1$. Sei A_m die Menge der Abbildungen von $\{1, \dots, 6\}$ nach $\{1, \dots, m\}$. Wir interpretieren A_m als die Menge der Perlenfärbungen der 6 Perlen einer Kette mit m möglichen Farben. Auf A_m operiere dementsprechend die Gruppe

$$G := \langle a := (1, 2, 3, 4, 5, 6), b := (2, 6)(3, 5) \rangle \leq \mathcal{S}_6$$

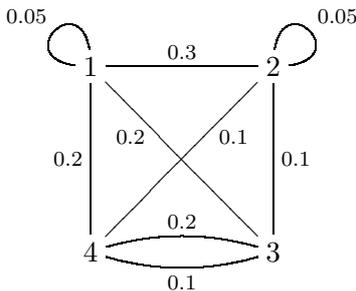
via $(g \cdot f)(x) := f(g^{-1}x)$, wobei $f \in A_m$, $g \in G$ und $x \in \{1, \dots, 6\}$. Zwei Perlenfärbungen f und f' sind bis auf Perlenkettenbewegung als gleich anzusehen, falls sie in derselben G -Bahn von A_m liegen.

- (1) Liste alle Elemente von G auf. (Hinweis: Eine Betrachtung von ${}^b a$ kann helfen.)

- (2) Bestimme die Anzahl der G -Bahnen auf A_3 , d.h. die Anzahl der auch nach Perlenkettenbewegung verschiedenen Perlenfärbungen mit 3 Farben.

Aufgabe 4**(2 Punkte)**

Betrachte folgenden bewerteten Graphen \mathcal{G} .



Bestimme einen minimalen aufspannenden Teilgraphen. Trage diesen mit Farbe in \mathcal{G} ein.

Aufgabe 5**(2+2 Punkte)**

Sei C der lineare Code über \mathbf{F}_2 mit der Erzeugermatrix $\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Sei C' der lineare Code über \mathbf{F}_2 mit der Erzeugermatrix $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.

(1) Bestimme eine Erzeugermatrix von $(C|C')$.

(2) Bestimme den Minimalabstand von $(C|C')$.

Aufgabe 6**(2+1 Punkte)**

Sei $f(X) = X^4 + X + \omega \in \mathbf{F}_4[X]$. Sei C der zyklische Code der Länge 15 mit Erzeugerpolynom $f(X)$. Betrachte \mathbf{F}_4 als Teilkörper von \mathbf{F}_{16} vermöge $\omega \mapsto \gamma^5 = \gamma^2 + \gamma$.

(1) Bestimme alle Nullstellen von $f(X)$ in \mathbf{F}_{16} unter Verwendung der Tatsache, daß γ^9 und γ^{13} als Nullstellen bekannt sind.

(2) Bestimme den designierten Minimalabstand von C , d.h. die mittels aufeinanderfolgender Potenzen einer primitiven 15-ten Einheitswurzel als Nullstellen von $f(X)$ bestimmbare untere Schranke für $d(C)$.

Aufgabe 7**(4+2 Punkte)**

Sei C der Hammingcode mit den Parametern $q = 8$ und $r = 2$ in Standardbezeichnung.

(1) Bestimme eine Prüfmatrix und eine Erzeugermatrix von C .

(2) Vergleiche die Dimension von C mit der Singleton-Schranke im vorliegenden Fall, d.h. für Länge und Minimalabstand wie C .

Aufgabe 8**(3 Punkte)**

Zeige oder widerlege die folgende Aussage.

Sei G eine endliche Gruppe. Ist p eine Primzahl, ist $k \geq 1$, und ist p^k ein Teiler von $|G|$, so gibt es in G ein Element von Ordnung p^k .

Lösung zur Scheinklausur

Aufgabe 1

- (1) Wir haben $\binom{4+4-1}{4-1} = 35$ Möglichkeiten.
- (2) Wir erhalten $((1, 3, 2) \circ (1, 4, 3) \circ (1, 3))^2 = (1, 3, 4, 2)^2 = (1, 4)(2, 3)$, und dieses Element hat Ordnung 2.
- (3) Wir müssen die Anzahl der fixpunktfreien Permutationen in \mathcal{S}_5 bestimmen. Diese ergibt sich zu

$$5! \cdot \sum_{i=0}^5 \frac{(-1)^i}{i!} = 5! \left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} \right) = 44.$$

- (4) Da $91 = 7 \cdot 13$ in eine gerade Zahl paarweise verschiedener Primfaktoren zerfällt, ist $\mu(91) = 1$.

Aufgabe 2

Wir kürzen $u(X) := X$, $v(X) := X^2 + X + 1$ und $w(X) := X^3 + X + 1$ ab. Zwischenergebnisse sind

$$\begin{aligned} 1 &= u(X) \cdot (X^4 + X^3) && + && v(X)w(X) \cdot 1 \\ 1 &= v(X) \cdot (X^3 + X^2 + X + 1) && + && u(X)w(X) \cdot X \\ 1 &= w(X) \cdot (X + 1) && + && u(X)v(X) \cdot X \end{aligned}$$

Somit erfüllt

$$\tilde{f}(X) := 1 \cdot v(X)w(X) \cdot 1 + 1 \cdot u(X)w(X) \cdot X + X^2 \cdot u(X)v(X) \cdot X = X^6 + X^5 + X^3 + X^2 + 1$$

die verlangten Kongruenzen. Polynomdivision durch $u(X)v(X)w(X)$ liefert dann die Lösung

$$f(X) = X^3 + X^2 + X + 1,$$

die die Gradbedingung erfüllt.

Aufgabe 3

- (1) Es ist ${}^b a = (1, 6, 5, 4, 3, 2) = a^{-1} = a^5$. Also ist jedes Element von G von der Form $a^i b^j$ mit $0 \leq i \leq 5$ und $0 \leq j \leq 1$.

Somit wird

$$\begin{aligned} G &= \{a^0, a^1, a^2, a^3, a^4, a^5, a^0b, a^1b, a^2b, a^3b, a^4b, a^5b\} \\ &= \{\text{id}, (1, 2, 3, 4, 5, 6), (1, 3, 5)(2, 4, 6), (1, 4)(2, 5)(3, 6), (1, 5, 3)(2, 6, 4), (1, 6, 5, 4, 3, 2), \\ &\quad (2, 6)(3, 5), (1, 2)(3, 6)(4, 5), (1, 3)(4, 6), (1, 4)(2, 3)(5, 6), (1, 5)(2, 4), (1, 6)(2, 5)(3, 4)\}. \end{aligned}$$

Man kann auch einen Baum erstellen. Der Aufwand dafür ist etwas größer.

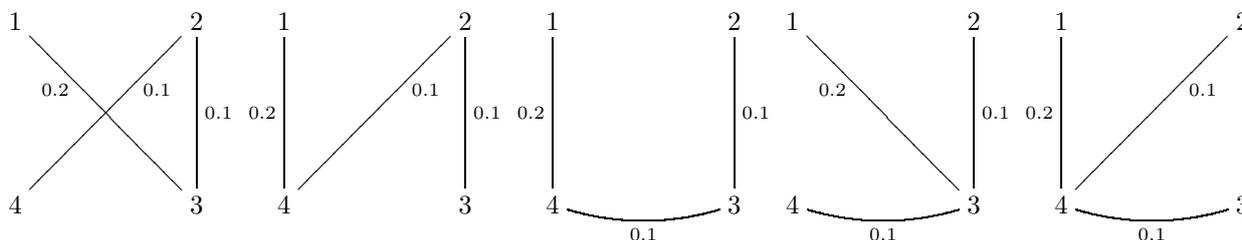
- (2) Nach dem Lemma von Burnside ergibt sich die Anzahl der Bahnen von G auf A_m zu

$$\frac{1}{12} \left(\underbrace{1 \cdot m^6}_{\text{zu id}} + \underbrace{2 \cdot m^1}_{\text{zu } (1, 2, 3, 4, 5, 6) \text{ etc.}} + \underbrace{2 \cdot m^2}_{\text{zu } (1, 3, 5)(2, 4, 6) \text{ etc.}} + \underbrace{4 \cdot m^3}_{\text{zu } (1, 4)(2, 5)(3, 6) \text{ etc.}} + \underbrace{3 \cdot m^4}_{\text{zu } (2, 6)(3, 5) \text{ etc.}} \right).$$

Insbesondere ergibt sich die gefragte Anzahl der Bahnen von G auf A_3 zu 92.

Aufgabe 4

Minimale aufspannende Teilgraphen sind die folgenden.



Verlangt war, einen von diesen anzugeben.

Aufgabe 5

- (1) Eine Erzeugermatrix von $(C|C')$ ist gegeben durch

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

- (2) Der Minimalabstand ist gegeben durch $d((C|C')) = \min\{2d(C), d(C')\}$. Wir erkennen direkt, daß $d(C) = 1$ und $d(C') = 2$. Also ist $d((C|C')) = \min\{2, 2\} = 2$.

Den Minimalabstand aus einer Prüfmatrix für $(C|C')$ abzulesen, ist möglich, aber aufwendiger.

Aufgabe 6

- (1) Es sind mit γ^9 und γ^{13} auch $(\gamma^9)^4 = \gamma^{36} = \gamma^6$ und $(\gamma^{13})^4 = \gamma^{52} = \gamma^7$ Nullstellen von $f(X)$. Wegen $\deg f = 4$ ist die Menge der Nullstellen von $f(X)$ in \mathbf{F}_{16} damit zu $\{\gamma^6, \gamma^7, \gamma^9, \gamma^{13}\}$ bekannt.
- (2) Es ist γ eine primitive 15-Einheitswurzel (da $\gamma^3 \neq 1$ und $\gamma^5 = \gamma^2 + \gamma \neq 1$), und deren 2 aufeinanderfolgende Potenzen γ^6, γ^7 sind Nullstellen von $f(X)$. Also beträgt der designierte Minimalabstand $2 + 1 = 3$.

Aufgabe 7

- (1) Die Prüfmatrix ist nur bis auf eine Permutation der Zeilen bestimmt. Wir können geschickterweise folgende nehmen.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & \beta^0 \\ 1 & \beta^1 \\ 1 & \beta^2 \\ 1 & \beta^3 \\ 1 & \beta^4 \\ 1 & \beta^5 \\ 1 & \beta^6 \end{pmatrix}$$

Denn dann liefern die Erzeugnisse der Zeilen gerade alle eindimensionalen Teilräume von $\mathbf{F}_8^{1 \times 2}$. Dazugehörend erhalten wir die Prüfmatrix

$$\begin{pmatrix} 1 & \beta^0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & \beta^1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \beta^2 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & \beta^3 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & \beta^4 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & \beta^5 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & \beta^6 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- (2) Die Länge von C beträgt $N = 9$, der Minimalabstand $d = 3$ (wie bei allen Hammingcodes). Die Singleton-Schranke besagt nun, daß die Dimension von C nicht über $N - d + 1 = 7$ liegen sollte. Nun ist die Dimension von C gerade $k = 7$, d.h. die Singleton-Schranke wird angenommen.

Aufgabe 8

Die Aussage ist falsch. Z.B. ist 2^3 ein Teiler von $|\mathcal{S}_4|$, ohne daß \mathcal{S}_4 ein Element der Ordnung 2^3 enthält. In der Tat müßte es hierzu ein Element in \mathcal{S}_4 geben, welches in Zykeldarstellung einen Zykel der Länge 8 aufweist, was wegen $8 > 4$ nicht möglich ist.