G. Nebe, M. Künzer 01.09.2006

Diskrete Strukturen, SS 06

Vordiplomsklausur

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 der 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+2 Punkte)

(1) Auf wieviele Arten kann man 3 Kugeln aus 5 Kugeln ziehen, wenn man jeweils nicht wieder zurücklegt und nicht auf die Reihenfolge achtet? $\boxed{}$

(2) Bestimme die Anzahl der Elemente der Konjugationsklasse von $(1,2)(3,4)(5,6)$ in $\mathcal{S}_8$. $\boxed{}$

(3) Bestimme die Anzahl der surjektiven Abbildungen von $\{1,2,3,4,5\}$ nach $\{1,2,3,4\}$. $\boxed{}$

(4) Bestimme die Anzahl der normierten irreduziblen Polynome von Grad 8 in $\mathbf{F}_3[X]$. $\boxed{}$

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

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

(1) Bestimme die Bahnenlänge $|G \cdot 2|$. $\boxed{}$

(2) Bestimme die Bahnenlänge $|\operatorname{Stab}_G(2) \cdot 1|$. $\boxed{}$

(3) Bestimme die Bahnenlänge $|\operatorname{Stab}_G(1,2) \cdot 4|$. $\boxed{}$

(4) Bestimme $|G|$. $\boxed{}$

Aufgabe 3 (3+1 Punkte)

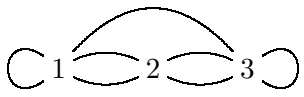
Sei $\mathbf{F}_{32} := \mathbf{F}_2[X]/(X^5 + X^2 + 1)$. Schreibe $\delta := [X]_{X^5+X^2+1}$.

(1) Berechne $(\delta^2+1)^{-1}$ als Linearkombination der Standardbasis $(\delta^0, \delta^1, \delta^2, \delta^3, \delta^4)$ von $\mathbf{F}_{32}$ über $\mathbf{F}_2$. $\boxed{}$ (Hinweis: Euklid.)

(2) Entscheide, ob $\delta^2 + 1$ ein Erzeuger von $\mathbf{F}_{32}^*$ ist. Begründe!

Aufgabe 4 (2 Punkte)

Betrachte folgenden Graphen.



Bestimme die Anzahl seiner Kantenzüge von Länge 2. $\boxed{}$

Aufgabe 5 **(2+1+1 Punkte)**

Wir wollen das RSA-Verfahren anwenden und verwenden dabei die Standardbezeichnungen.
Seien $p = 7$, $q = 11$ und $v = 7$. (Hinweis: Taschenrechner.)

(1) Bestimme e. $\square$

(2) Verschlüssele die Ziffer 5. $\square$

(3) Entschlüssele die Ziffer 2. $\square$

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

Sei C der lineare Code über $\mathbf{F}_4$ mit der Erzeugermatrix $\begin{pmatrix} 1 & 1 & \omega & \omega^2 \\ \omega^2 & 0 & 1 & 1 \end{pmatrix}$.

(1) Bestimme eine Prüfmatrix für C.

(2) Bestimme den Minimalabstand von C.

Aufgabe 7 **(2+1+2+1 Punkte)**

Sei $f(X) = X^3 + X^2 + 1 \in \mathbf{F}_2[X]$. Es ist $g(X) := (X^7 - 1)/f(X) = X^4 + X^3 + X^2 + 1$. Sei C der zyklische Code der Länge 7 mit Erzeugerpolynom $f(X)$.

(1) Bestimme alle Nullstellen von $f(X)$ in $\mathbf{F}_8$. $\square$

(2) Bestimme den designierten Minimalabstand von C.

(3) Bestimme den Minimalabstand $d(C)$ und vergleiche mit dem designierten Minimalabstand von C.

(4) Vergleiche die Dimension von C mit der Hammingschranke im vorliegenden Fall, d.h. für Länge und Minimalabstand wie C.

Aufgabe 8 **(3 Punkte)**

Zeige oder widerlege folgende Aussage.

Sei G eine endliche Gruppe. Seien U und V Untergruppen in G. Sei $|U|$ teilerfremd zu $|V|$, d.h. sei $\mathrm{ggT}(|U|, |V|) = 1$. Es ist $U \cap V = \{1\}$.

G. Nebe, M. Künzer 01.09.2006

Diskrete Strukturen, SS 06

Lösung zur Vordiplomsklausur

Aufgabe 1

(1) Wir haben $\binom{5}{3} = 10$ Möglichkeiten.

(2) Die Konjugationsklasse von $(1,2)(3,4)(5,6)$ in $\mathcal{S}_8$ enthält $\frac{8!}{2^3 \cdot 2! \cdot 3!} = 420$ Elemente.

(3) Die Anzahl der surjektiven Abbildungen von $\{1,2,3,4,5\}$ nach $\{1,2,3,4\}$ ergibt sich zu

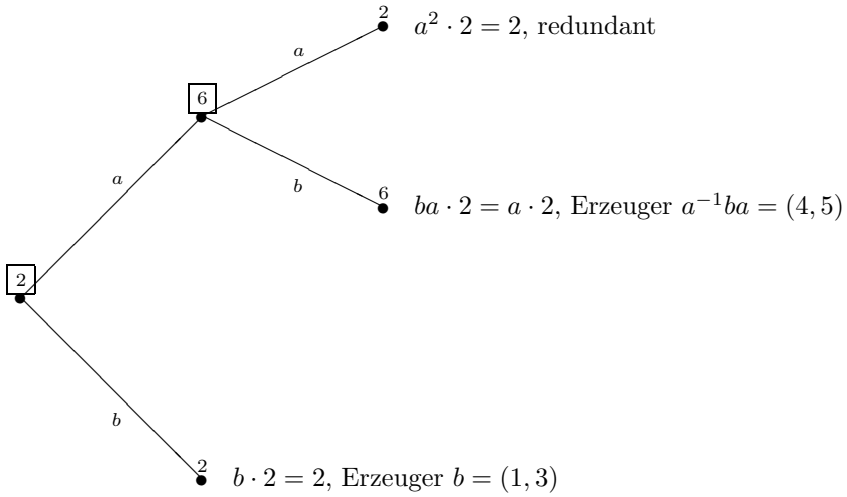
$$\sum_{i=0}^{4} (-1)^i \binom{4}{i} (4-i)^5 \;=\; 1 \cdot 4^5 - 4 \cdot 3^5 + 6 \cdot 2^5 - 4 \cdot 1^5 + 1 \cdot 0^5 \;=\; 240\,.$$

(4) Die Anzahl der normierten irreduziblen Polynome von Grad 8 in $\mathbf{F}_3[X]$ ergibt sich zu

$$\frac{1}{8} \sum_{d|8} 3^d \mu(8/d) \;=\; \frac{1}{8} \left(-3^4 + 3^8\right) \;=\; 810\,.$$

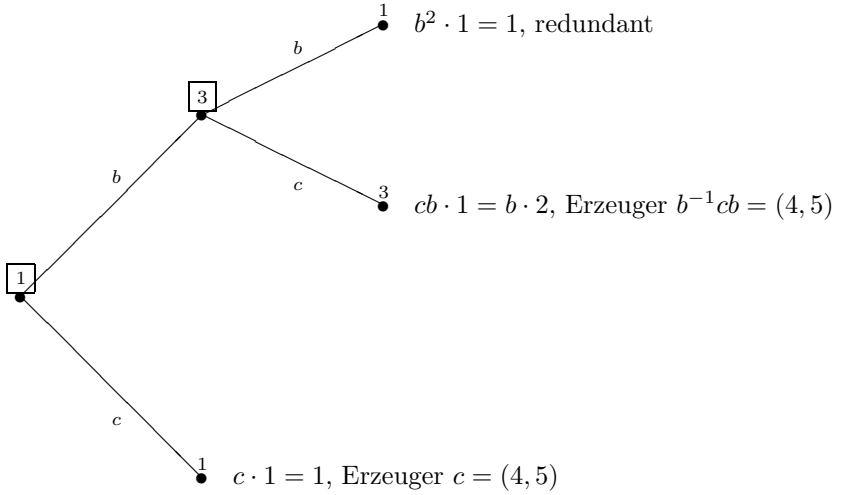
Aufgabe 2

Wir erstellen einen Baum zur Berechnung von $G \cdot 2$ und von $\mathrm{Stab}_G(2)$.



Somit ist $G \cdot 2 = \{2, 6\}$, und $|G \cdot 2| = 2$ (Antwort zu (1)). Ferner ist $\mathrm{Stab}_G(2) = \langle b = (1,3),\ c := (4,5) \rangle$.

Wir erstellen einen Baum zur Berechnung von $\mathrm{Stab}_G(2) \cdot 1$ und von $\mathrm{Stab}_G(1)$.



Somit ist $\mathrm{Stab}_G(2) \cdot 1 = \{1, 3\}$, und $|\mathrm{Stab}_G(2) \cdot 1| = 2$ (Antwort zu (2)). Ferner ist $\mathrm{Stab}_G(1, 2) = \langle c = (4, 5) \rangle$.

Direkt erkennen wir, daß $\mathrm{Stab}_G(1, 2) \cdot 4 = \{4, 5\}$ und $|\mathrm{Stab}_G(1, 2) \cdot 4| = 2$ (Antwort zu (3)).

Insgesamt wird $|G| = \frac{|G|}{|\mathrm{Stab}_G(1)|} \cdot \frac{|\mathrm{Stab}_G(1)|}{|\mathrm{Stab}_G(1,2)|} \cdot |\mathrm{Stab}_G(1, 2)| = |G \cdot 2| \cdot |\mathrm{Stab}_G(2) \cdot 1| \cdot |\mathrm{Stab}_G(1, 2)| = 2 \cdot 2 \cdot 2 = 8$ (Antwort zu (4)).

Aufgabe 3

(1) Mittels des Euklidschen Algorithmus bestimmen wir Polynome $s(X)$ und $t(X)$ so, daß

$$1 \;=\; s(X) \cdot (X^5 + X^2 + 1) + t(X) \cdot (X^2 + 1)\ .$$

Wir erhalten z.B.

$$1 \;=\; X \cdot (X^5 + X^2 + 1) + (X^4 + X^2 + X + 1) \cdot (X^2 + 1)\ .$$

Einsetzen von δ gibt

$$1 \;=\; \delta \cdot (\delta^5 + \delta^2 + 1) + (\delta^4 + \delta^2 + \delta + 1) \cdot (\delta^2 + 1) \;=\; (\delta^4 + \delta^2 + \delta + 1) \cdot (\delta^2 + 1)\ ,$$

und also $(\delta^2 + 1)^{-1} = \delta^4 + \delta^2 + \delta + 1$.

(2) Es ist $\mathbf{F}_{32}^* \simeq C_{31}$. Da 31 prim ist, ist diese Gruppe von jedem Element ungleich 1 erzeugt. Da $\delta^2 + 1 \neq 1$, ist insbesondere $\delta^2 + 1$ ein Erzeuger von $\mathbf{F}_{32}^*$.

Aufgabe 4

Die Inzidenzmatrix unseres Graphen ist $A := \left(\begin{smallmatrix} 1 & 2 & 1 \\ 2 & 0 & 2 \\ 1 & 2 & 1 \end{smallmatrix}\right)$. Der Eintrag an Position (i, j) von A^2 gibt die Anzahl der Kantenzüge der Länge 2 von i nach j. Wir müssen also alle Einträge von A^2 aufaddieren. Da $A^2 = \left(\begin{smallmatrix} 6 & 4 & 6 \\ 4 & 8 & 4 \\ 6 & 4 & 6 \end{smallmatrix}\right)$, erhalten wir 48 Kantenzüge der Länge 2.

Aufgabe 5

(1) Es ist $(11 - 1) \cdot (7 - 1) = 60$. Mittels Euklid ermittelt man, daß $1 = 2 \cdot 60 - 17 \cdot 7$. Das Inverse von $v = 7$ in $\mathbf{Z}/60\mathbf{Z}$ wird also repräsentiert von -17, oder aber, im vorgeschriebenen Intervall, von $e = 43$.

(2) Es ist $5^7 \equiv_{11 \cdot 7} 47$.

(3) Es ist $2^{43} \equiv_{11 \cdot 7} 30$.

Aufgabe 6

(1) Die Erzeugermatrix in Zeilenstufenform ist $\left(\begin{smallmatrix} 1 & 0 & \omega & \omega \\ 0 & 1 & 0 & 1 \end{smallmatrix}\right)$. Dies liefert z.B. die Prüfmatrix $\left(\begin{smallmatrix} \omega & \omega \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

(2) Es gibt in der Prüfmatrix kein linear abhängiges Zeilentupel der Länge 1 (d.h. keine Nullzeile), wohl aber ein linear abhängiges Zeilentupel der Länge 2, bestehend aus der 2-ten und der 4-ten Zeile. Somit erhalten wir den Minimalabstand $d(C) = 2$.

Aufgabe 7

(1) Als Nullstelle ergibt sich durch Probieren zunächst etwa β^3. Daraus erhalten wir die weiteren Nullstellen $(\beta^3)^2 = \beta^6$ und $(\beta^3)^4 = \beta^{12} = \beta^5$. Da $\deg f = 3$ ist, erhalten wir $\{\beta^3, \beta^5, \beta^6\}$ als Nullstellenmenge von $f(X)$. Alternativ hat diese Menge auch die Form $\{\beta + 1, \beta^2 + \beta + 1, \beta^2 + 1\}$.

(2) Es ist β eine primitive 7-te Einheitswurzel (da $\beta \neq 1$). Deren 2 aufeinanderfolgende Potenzen β^5 und β^6 sind Nullstellen von $f(X)$. Also beträgt der designierte Minimalabstand $2 + 1 = 3$.

(3) Eine Prüfmatrix von C ist gegeben durch

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

In dieser ist jedes aus 2 Zeilen bestehende Tupel linear unabhängig, wie eine direkte Prüfung ergibt. Also ist $d(C) \geq 3$. Hierfür kann man alternativ auch das Ergebnis aus (2) heranziehen.

Hingegen ist das aus der 1-ten, der 2-ten und der 4-ten Zeile gebildete Tupel linear abhängig. Also ist auch $d(C) \leq 3$.

Im vorliegenden Fall stimmen also Minimalabstand und designierter Minimalabstand überein.

Alternativ kann man auch mit (2) und der Standarderzeugermatrix arbeiten.

(4) Der Minimalabstand ist $d = d(C) = 3$, die Länge ist $N = 7$. Die Hammingschranke ergibt sich für diese Parameter zu $7 - \log_2(\mathrm{V}_2(7,1)) = 7 - \log_2\left(\binom{7}{0} + \binom{7}{1}\right) = 7 - 3 = 4$. Die Dimension von C ist ebenfalls gleich 4. Die Hammingschranke, die eine obere Schranke für diese Dimension darstellt, wird also angenommen.

Aufgabe 8

Die Aussage ist richtig. Es ist $U \cap V$ eine Untergruppe von U, und folglich $|U \cap V|$ ein Teiler von $|U|$. Genauso ist $U \cap V$ eine Untergruppe von V, und folglich $|U \cap V|$ ein Teiler von $|V|$. Da der größte gemeinsame Teiler von $|U|$ und $|V|$ gleich 1 ist, folgt $|U \cap V| = 1$, und also $U \cap V = \{1\}$.