G. Nebe, M. Künzer 20.03.2007

Diskrete Strukturen, SS 06

Lösung zur Vordiplomsnachklausur

Aufgabe 1

(1) Wir haben $5 \cdot 4 \cdot 3 = 60$ Möglichkeiten.

(2) Es wird

$$\begin{aligned} \big((1,2,3,4) \circ (2,3,5)\big)^4 &= \big((1,2,4)(3,5)\big)^4 \\ &= (1,2,4)^4 \circ (3,5)^4 \\ &= (1,2,4)\,, \end{aligned}$$

und dieses Element hat Ordnung 3.

(3) Die Anzahl der fixpunktfreien Permutationen auf der Menge $\{1,2,\ldots,6\}$ ergibt sich zu

$$6! \cdot \sum_{i=0}^{6} \frac{(-1)^i}{i!} \;=\; 6! \cdot \left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \frac{1}{6!} \right) \;=\; 265\,.$$

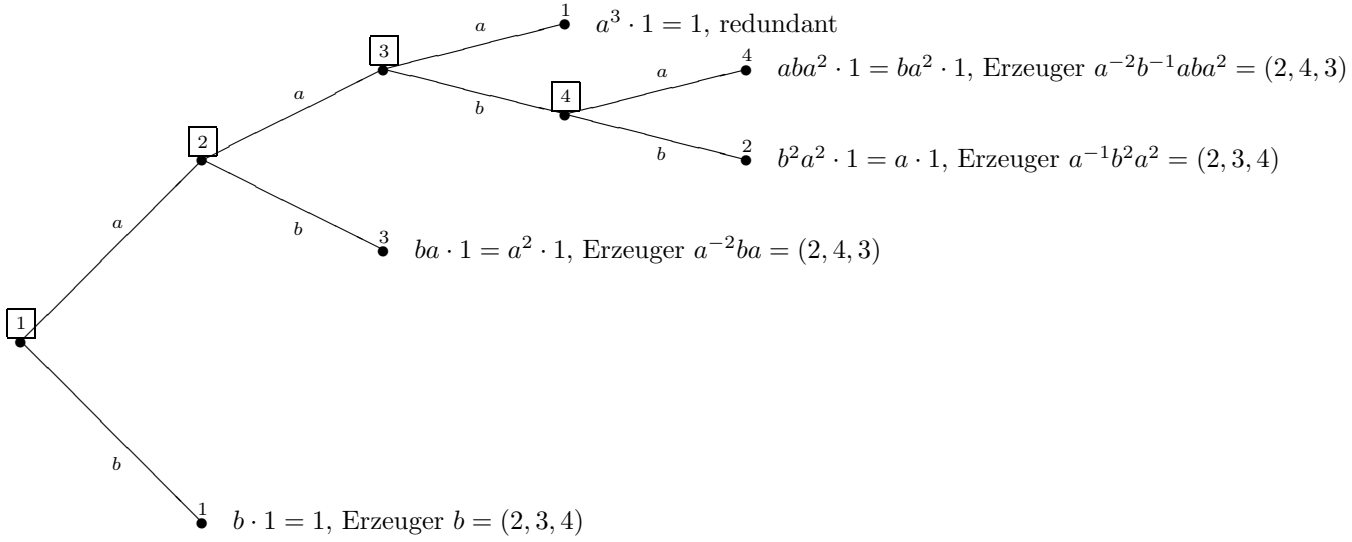
(4) Jedes irreduzible Polynom in $\mathbf{F}_2[X]$ ist normiert. Die Anzahl der irreduziblen Polynome von Grad 12 in $\mathbf{F}_2[X]$ ergibt sich zu

$$\begin{aligned} \tfrac{1}{12} \textstyle\sum_{d|12} 2^d \mu(12/d) &= \tfrac{1}{12} \left(2^2\mu(12/2) + 2^4\mu(12/4) + 2^6\mu(12/6) + 2^{12}\mu(12/12) \right) \\ &= \tfrac{1}{12} \left(4 - 16 - 64 + 4096 \right) \\ &= 335\,. \end{aligned}$$

Hierbei beachten wir, daß der μ-Wert von Zahlen, in welchen eine Primzahl mehr als einfach als Faktor auftritt, wie etwa 4 oder 12, verschwindet.

Aufgabe 2

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



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

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

Insgesamt wird $|G| = \frac{|G|}{|\mathrm{Stab}_G(1)|} \cdot |\,\mathrm{Stab}_G(1)| = |G \cdot 1| \cdot |\,\mathrm{Stab}_G(1)| = 4 \cdot 3 = 12$ (Antwort zu (3)).

Aufgabe 3

(1) Es ist $\mathbf{F}_{7^f}^* \simeq C_{7^f-1}$. Es enthält C_{7^f-1} genau dann eine primitive 20-te Einheitswurzel, wenn 20 ein Teiler von $7^f - 1$ ist, d.h. wenn $7^f \equiv_{20} 1$. Wir müssen also die Ordnung von 7 als Element von $(\mathbf{Z}/20\mathbf{Z})^*$ ermitteln. Wir rechnen

$$\begin{array}{lllllll} 7^2 & = & 49 & \equiv_{20} & 9 & & \\ 7^3 & \equiv_{20} & 9 \cdot 7 & = & 63 & \equiv_{20} & 3 \\ 7^4 & \equiv_{20} & 3 \cdot 7 & = & 21 & \equiv_{20} & 1\,. \end{array}$$

Als Lösung ergibt sich somit $f = 4$.

(2) Das Element $i + 1$ hat Ordnung 8. Da $\mathbf{F}_9 = \langle i+1 \rangle \simeq C_8$, ergibt sich

$$\{x \in \mathbf{F}_9^* \,:\, \langle x \rangle = \mathbf{F}_9^*\} \;=\; \{\iota + 1,\ (\iota+1)^3,\ (\iota+1)^5,\ (\iota+1)^7\} \;=\; \{\iota + 1,\ -\iota + 1,\ -\iota - 1,\ \iota - 1\}\,,$$

wobei letztere Gleichheit unter Beachtung von $(\iota + 1)^2 = -\iota$ am einfachsten zu bestimmen ist.

Aufgabe 4

Die Inzidenzmatrix unseres Graphen ist $\left(\begin{smallmatrix} 1 & 3 \\ 3 & 0 \end{smallmatrix}\right)$. Der Eintrag an Position $(2, 2)$ von A^4 gibt die Anzahl der Kantenzüge von 2 nach 2 der Länge 4. Da $A^4 = (A^2)^2 = \left(\begin{smallmatrix} 10 & 3 \\ 3 & 9 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} * & * \\ * & 90 \end{smallmatrix}\right)$, gibt es 90 solcher Kantenzüge.

Aufgabe 5

(1) Der Euklidsche Algorithmus gibt $56 \cdot 1 - 5 \cdot 11 = 1$. Also ist $z = 56 \cdot 1 = 56$ möglich.

(2) Der Euklidsche Algorithmus gibt $40 \cdot 3 - 7 \cdot 17 = 1$. Also ist $z = 40 \cdot 3 = 120$ möglich.

(3) Der Euklidsche Algorithmus gibt $35 \cdot 3 - 8 \cdot 13 = 1$. Also ist $z = 35 \cdot 3 = 105$ möglich.

(4) Beachte $5 \cdot 7 \cdot 8 = 280$. Sei zunächst $2 \cdot 56 + 1 \cdot 120 + 4 \cdot 105 = 652$ gebildet. Es ist $652 \equiv_{280} 92 = z$.

Aufgabe 6

(1) Die Erzeugermatrix hat die Zeilenstufenform $\left(\begin{smallmatrix} 1 & \omega & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & \omega^2 \end{smallmatrix}\right)$. Dieser entnehmen wir die Prüfmatrix

$$\begin{pmatrix} \omega & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & \omega^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

(2) Da in unserer Prüfmatrix aus (1) je zwei verschiedene Zeilen ein linear unabhängiges, aber die letzten drei Zeilen ein linear abhängiges Tupel bilden, ist der Minimalabstand gleich 3.

Aufgabe 7

(1) Durch Probieren erhalten wir die Nullstelle γ^6. Da $f(X) \in \mathbf{F}_4[X]$, ist mit γ^6 auch $(\gamma^6)^4 = \gamma^{24} = \gamma^9$ eine Nullstelle von $f(X)$. Da $\deg f = 2$, ist die Menge der Nullstellen von $f(X)$ bereits gegeben durch $\{\gamma^6, \gamma^9\} = \{\gamma^3 + \gamma^2, \gamma^3 + \gamma\}$.

(2) Unter den Potenzen von γ^3 sind die beiden aufeinanderfolgenden $(\gamma^3)^2$ und $(\gamma^3)^3$ Nullstellen von $f(X)$. Der designierte Minimalabstand von X ergibt sich also zu $2 + 1 = 3$.

(3) Eine Polynomdivision liefert das Prüfpolynom $g(X) := (X^5 - 1)/f(X) = X^3 + \omega X^2 + \omega X + 1$.

Eine Prüfmatrix von C ist vermöge $g(X)$ gegeben durch

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

In dieser bilden je zwei Zeilen ein linear unabhängiges Tupel. Da die Matrix nur zwei Spalten hat, ist sogar jedes aus drei ihrer Zeilen bestehende Tupel linear abhängig. Dies gibt $d(C) = 3$.

(4) Z.B. die Gestalt der Prüfmatrix liefert $5 - 2 = 3$ als Dimension von C. Für die Hammingschranke bestimmen wir zunächst

$$\mathrm{V}_4(5,1) \;=\; \tbinom{5}{0}(4-1)^0 + \tbinom{5}{1}(4-1)^1 \;=\; 16\,.$$

Somit wird die Hammingschranke zu

$$5 - \log_4\big(\mathrm{V}_4(5,1)\big) \;=\; 5 - \log_4 16 \;=\; 3\,.$$

Ein Vergleich zeigt, daß die Dimension unseres Codes C die Hammingschranke genau erreicht.

Dies ist wegen der Antwort zu (5) auch nicht erstaunlich.

(5) Ja, C ist ein Hammingcode. Zu jeder der Geraden

$$\langle(1\,0)\rangle,\;\; \langle(1\,1)\rangle,\;\; \langle(1\,\omega)\rangle,\;\; \langle(1\,\omega^2)\rangle,\;\; \langle(0\,1)\rangle$$

in $\mathbf{F}_4^{1\times 2}$ gibt es in der in (3) gefundenen Prüfmatrix

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

von C genau eine Zeile, welche in dieser Geraden liegt. Genauer, es liegen

$$(1\,0) \in \langle(1\,0)\rangle,\;\; (\omega\,\omega) \in \langle(1\,1)\rangle,\;\; (1\,\omega) \in \langle(1\,\omega)\rangle,\;\; (\omega\,1) \in \langle(1\,\omega^2)\rangle,\;\; (0\,1) \in \langle(0\,1)\rangle\,.$$

Aufgabe 8

Die Aussage ist falsch. In der Tat liefert der Euklidsche Algorithmus

$$\mathrm{ggT}\big(f(X), f'(X)\big) \;=\; \mathrm{ggT}\big(X^9 + X^7 + X^4 + X^3 + X^2 + X + 1,\, X^8 + X^6 + X^2 + 1\big) \;=\; X^4 + X^2 + 1 \;\neq\; 1\,.$$

Somit enthält $f(X)$ einen irreduziblen Faktor mit Multiplizität größer 1.