Technische Universität München
Fakultät für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Ernst W. Mayr
Dr. Werner Meixner

Sommersemester 2011
Übungsblatt 3
29. August 2011

Diskrete Strukturen

Abgabetermin: 6. September 2011, 14 Uhr in die **DS Briefkästen**

Hausaufgabe 1 (4 Punkte)

Seien A und B Mengen. Man zeige:

1. Die Mengen $A \setminus B$, $B \setminus A$ und $A \cap B$ sind paarweise disjunkt und es gelten die Gleichungen

$$A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B) = (A \Delta B) \cup (A \cap B)\,.$$

2. Falls A und B endlich sind, dann gilt die Implikation

$$|A \setminus B| \leq |A| - |B| \quad \Longrightarrow \quad B \subseteq A\,.$$

Hausaufgabe 2 (4 Punkte)

Sei M eine 3-elementige Menge, d. h. $|M| = 3$. Sei R eine (beliebige) binäre Relation über M, d. h. $R \subseteq M \times M$.

1. Sei $R_2 = R^0 \cup R^1 \cup R^2$. Zeigen Sie $R^3 \subseteq R_2$!

   Ist R_2 transitiv? Begründung!

2. Geben Sie eine Relation S über einer 4-elementigen Menge M' an, so dass $S_2 = S^0 \cup S^1 \cup S^2$ nicht transitiv ist.

Hausaufgabe 3 (4 Punkte)

Den folgenden aussagenlogischen Ausdruck bezeichnen wir mit F:

$$p \Rightarrow (q \Rightarrow r) \equiv (p \Rightarrow q) \Rightarrow r\,.$$

1. Bestimmen Sie die Semantik von F als boolesche Funktion (Wahrheitsfunktion) durch Angabe der zugehörigen Wahrheitswerttabelle.

2. Konstruieren Sie eine zu F äquivalente konjunktive Normalform.

3. Ist F allgemeingültig? Begründung!

Hausaufgabe 4 (4 Punkte)

Für alle $n \in \mathbb{N}_0$ definieren wir

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n .$$

1. Zeigen Sie mit direktem Beweis für alle $n \in \mathbb{N}$ die Gleichung

$$L_{n+1} = L_n + L_{n-1} .$$

2. Man zeige mit vollständiger Induktion, dass L_n für jedes $n \in \mathbb{N}_0$ eine natürliche Zahl ist.

Hausaufgabe 5 (4 Punkte)

1. Gilt die Mengengleichheit $O(n^2) = O(n^3)$? Beweisen Sie Ihre Aussage!
2. Wahr oder falsch: $2 \cdot 3^n \in O(3 \cdot 2^n)$? Beweisen Sie Ihre Antwort!
3. Sei $2^{O(n)} = \{2^{f(n)};\ f(n) \in O(n)\}$. Gilt $O(2^n) = 2^{O(n)}$? Beweisen Sie Ihre Aussage!

Hinweis: *Auf den Übungsblättern in diesem Semester wird es grundsätzlich die drei Aufgabentypen Vorbereitungsaufgabe, Tutoraufgabe und Hausaufgabe geben. Die als Vorbereitung bezeichneten Aufgaben dienen der häuslichen Vorbereitung der Tutoraufgaben. Tutoraufgaben werden in den Übungsgruppen bearbeitet. Dabei wird die Lösung der Vorbereitungsaufgaben vorausgesetzt. Die Vorbereitungsaufgaben werden in der Zentralübung unterstützt.*

Vorbereitung 1

Wir betrachten prädikatenlogische Formeln mit Prädikaten über dem Universum $\mathbb{R}$.

1. Wir nehmen an, dass für einstellige Prädikate P und Q die folgende Aussage gilt:

   $$(\exists x)[P(x)] \;\; \wedge \;\; (\forall x)[P(x) \Rightarrow Q(x)]$$

   Man zeige, dass dann $(\exists x)[Q(x)]$ folgt.

2. Wir nehmen an, dass für ein 3-stelliges Prädikat P die folgende Aussage F gilt:

   $$(\forall x \; \exists y \; \forall z) \, [P(x,y,z)] \, .$$

   Man leite eine pränexe prädikatenlogische Formel her, die zu $\neg F$ äquivalent ist.

Vorbereitung 2

1. Direkter Beweis:
   Geben Sie für die folgende Aussage einen direkten Beweis an.

   Das arithmetische Mittel $b = \frac{1}{n}\sum_{i=1}^{n} a_i$ von n Zahlen a_i, $1 \leq i \leq n$ bleibt unverändert, falls die Folge der a_i mit beliebig vielen $b's$ erweitert wird, d. h.

   $$b = \frac{1}{n}\sum_{i=1}^{n} a_i \;\; = \;\; \frac{1}{n+m}\left(\sum_{i=1}^{n} a_i \; + \; m \cdot b\right) \, .$$

2. Indirekter Beweis:
   Es seien $m, n, k \in \mathbb{N}$ natürliche Zahlen mit $m > n \cdot k$.
   Zeigen Sie: Verteilt man m Hamster auf n Käfige, so befinden sich in mindestens einem Käfig $k+1$ oder mehr Hamster.

   Führen Sie einen indirekten Beweis, indem Sie annehmen, in allen Käfigen würden sich nach einer Verteilung weniger als $k+1$ Hamster befinden.

3. Schubfachprinzip:
   Lassen sich obige Aussagen auch mit dem „Schubfachprinizip“ beweisen?

Vorbereitung 3

1. Man zeige: $(\log n^2)^2 \in o(2^{\ln n})$.

2. Sei $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ mit $a_i \in \mathbb{R}$.
   Man zeige $f(x) = \mathcal{O}(x^n)$.

Vorbereitung 4

Sei $S' = \langle S, \circ \rangle$ eine Halbgruppe. Dann nennen wir ein Element $x \in S$ vertauschbar bezüglich $\circ$, falls gilt $(\forall a \in S)\,[\,a \circ x = x \circ a]$. Es sei $V(S)$ die Menge aller bezüglich $\circ$ vertauschbaren Elemente von S.

1. Zeigen Sie die Abgeschlossenheit von $V(S)$ unter der Verknüpfung $\circ$, d. h.:

$$x, y \in V(S) \Longrightarrow x \circ y \in V(S)\,.$$

2. Nun nehmen wir an, dass S' eine Gruppe mit Einselement 1 ist. Zeigen Sie, dass die Unterhalbgruppe $\langle V(S), \circ_{V(S)} \rangle$ von S' dann ebenfalls eine Gruppe ist.

3. Sei S' wieder eine Gruppe mit Einselement 1.
   Ist $V(S)$ ein Normalteiler von S'? Begründung!

Vorbereitung 5

Sei M eine endliche Menge und $z = (a_0, a_1, \ldots, a_{|M|-1})$ ein $|M|$-Tupel mit paarweise verschiedenen $a_i \in M$. Dann ist die Abbildung $\pi_z : M \to M$ mit $\pi_z(a_i) = a_{(i+1) \bmod |M|}$ ein *Zyklus* der *Länge* $|M|$ mit *Basis* M und *Darstellung* z. Für jeden Zyklus π bezeichne $M(\pi)$ die Basis von π. Man kann π_z als zyklische Nachfolgerbildung in M auffassen.

1. Wie viele Darstellungen besitzt ein Zyklus der Länge 3?
   Welchen Zyklus stellt $z = (4, 1, 3, 2)$ dar und welche Basis hat der Zyklus?
   Welche verschiedenen Darstellungen hat ${\pi_z}^3$? Ist ${\pi_z}^4$ ein Zyklus?

Zyklen ρ, σ heißen *disjunkt*, falls $M(\rho) \cap M(\sigma) = \emptyset$ gilt, d. h., falls deren Basismengen disjunkt sind. Eine Menge Z von paarweise disjunkten Zyklen heißt *Zyklenpartition*. Dabei bildet die Menge der Basismengen $P_Z = \{M(\pi)\,;\, \pi \in Z\}$ eine Mengenpartition der Vereinigung der Basismengen $M(Z) = \bigcup_{\pi \in Z} M(\pi)$. Wir sagen, dass Z eine Zyklenpartition der Menge $M(Z)$ ist.
Sei Z eine Zyklenpartition von $[n]$. Dann ist eine bijektive Abbildung $f_Z : [n] \to [n]$ gegeben für alle $i \in [n]$ durch

$$f_Z(i) = \pi(i), \quad \text{falls} \quad i \in M(\pi) \text{ und } \pi \in Z\,.$$

2. Zyklenpartitionen werden häufig durch eine Folge $z_1 z_2 \ldots z_k$ von Zyklusdarstellungen z_i definiert, wobei die Reihenfolge der z_i in der Folge keine Rolle spielt.

   Sei $Z = (4, 5, 1)(3)(2)$ eine Zyklenpartition.
   Beschreiben Sie die Abbildung f_Z extensional!

3. Eine Funktion f sei gegeben durch die folgende Matrixdarstellung.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 6 & 2 & 7 & 9 & 5 & 4 & 3 \end{pmatrix}.$$

   Berechnen Sie $\{f^i(2) \,|\, i \in \mathbb{N}\}$, $\{f^i(3) \,|\, i \in \mathbb{N}\}$, $\{f^i(5) \,|\, i \in \mathbb{N}\}$!

   Bestimmen Sie eine *Zyklendarstellung von* f, d. h. eine Zyklenpartition Z von $[9]$, so dass $f(i) = f_Z(i)$ für alle $i \in [9]$ gilt!

Vorbereitung 6

Ganze Zahlen $a, b \in \mathbb{Z}$ nennt man kongruent modulo m, mit $m \in \mathbb{N}$, i. Z. $a \equiv b\,(mod\,m)$, falls sich a und b um ein ganzzahliges Vielfaches von m unterscheiden, d. h., falls es ein $k \in \mathbb{Z}$ gibt, so dass $a = b + k \cdot m$ gilt. Diesen Zusammenhang kann man der Definition der Operation $\bmod : \mathbb{Z} \times \mathbb{N} \to \mathbb{Z}$ zugrunde legen: $b = a \bmod m$ gilt genau dann, wenn $a \equiv b\,(mod\,m)$ und gleichzeitig $0 \le b < m$ gilt.
Zeigen Sie für alle $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$:

$$\begin{aligned} a &\equiv a \bmod m\ (mod\,m)\,, & (1)\\ (a+b) \bmod m &= [(a \bmod m) + (b \bmod m)] \bmod m\,, & (2)\\ (a \cdot b) \bmod m &= [(a \bmod m) \cdot (b \bmod m)] \bmod m\,. & (3) \end{aligned}$$

In enger Beziehung zur mod-Operation steht die ganzzahlige Division $a \div m$ zweier Zahlen $a \in \mathbb{Z}, m \in \mathbb{N}$. Es gilt

$$a = (a \div m) \cdot m + (a \bmod m)\,.$$

Berechnen Sie: (i) $5 \div 4$, (ii) $(-5) \div 4$, (iii) $(-x) \div 1$.

Tutoraufgabe 1

Wir betrachten prädikatenlogische Formeln für Prädikate über dem Universum $\mathbb{R}$.

1. Seien P und Q einstellige Prädikate, für die die folgenden Aussagen gelten:

   $$(\exists x)[P(x)] \quad \wedge \quad (\exists x)[P(x) \Rightarrow Q(x)]$$

   Man zeige, dass dann nicht notwendigerweise $(\exists x)[Q(x)]$ gilt.

2. Für Funktionen $f, g : \mathbb{N}_0 \to \mathbb{R}$ wird $f(n) \in \omega(g(n))$ wie folgt definiert:

   $$f(n) \in \omega(g(n)) \quad \Longleftrightarrow \quad (\forall c > 0\, \exists n_0 \in \mathbb{N}\, \forall n \ge n_0)\, [\, |f(n)| > c \cdot g(n) \ge 0\,]\,.$$

   Man leite eine pränexe prädikatenlogische Formel für die Aussage $f(n) \notin \omega(g(n))$ her und zeige die Erfüllbarkeit der erhaltenen Formel mit einem Beispiel.

Tutoraufgabe 2

1. Widerspruchsbeweis:
   Sei S eine endliche Menge und $f : S \to S$. Man zeige durch Widerspruchsbeweis die Implikation

   $$f \text{ surjektiv} \implies f \text{ injektiv}\,.$$

2. Schubfachprinzip:
   Nehmen wir an, dass jeder der 520000 Einwohner von Hannover zwei Namensinitialen besitzt aus einem 26-elementigen Alphabet. Dabei bilden die zwei Initialen einer Person ein (geordnetes) Buchstaben-2-Tupel.

   Zeigen Sie: Es gibt in Hannover 3 Personen mit gleichen Initialen, die am gleichen Tag des Jahres (365 Tage) Geburtstag haben.

Tutoraufgabe 3

Es sei $G = \langle S, \circ, e \rangle$ eine Gruppe mit genau 4 Elementen $e, a, b, c \in S$, in der speziell für a gilt $a^2 = e$ mit dem neutralen Element e.

1. Geben Sie zwei verschiedene Gruppen mit obiger Eigenschaft an, indem Sie die zugehörigen Verknüpfungstabellen konstruieren.

2. Zeigen Sie, dass es keine weiteren Gruppen mit obiger Eigenschaft gibt.

Tutoraufgabe 4

Wir betrachten die folgenden Permutationen p_i der Menge $[6] \subseteq \mathbb{N}$ in Zyklendarstellung und beziehen uns dabei auf die Schreibweisen in Vorbereitungsaufgabe 2.

$$p_1 = (1, 5, 4, 6)\,(2)\,(3)\,, \qquad p_2 = (2, 5, 1)\,(3)\,(4)\,(6)\,,$$
$$p_3 = (3, 5, 2)\,(1)\,(4)\,(6)\,, \qquad p_4 = (4, 5, 3)\,(1)\,(2)\,(6)\,.$$

1. Geben Sie eine Zyklendarstellung der Permutation p an, die durch Komposition der p_i wie folgt definiert ist:
$$p = p_1 \circ p_2 \circ p_3 \circ p_4\,.$$

2. Bestimmen Sie die kleinste Potenz $k > 0$, so dass $(p_1 \circ p_4)^k$ gleich der identischen Abbildung id ist $(\forall x(id(x) = x))$.

Tutoraufgabe 5

Zeigen Sie, dass im Folgenden Algebren $A = \langle S, \circ \rangle$ definiert werden, die bezüglich des binären Operators $\circ$ eine Gruppe bilden.

1. Sei $S = \mathbb{R} \setminus \{-1\}$ und für alle $x, y \in S$
$$x \circ y = x + y + xy.$$

2. Sei $1 < n \in \mathbb{N}$ und $S = Z_n^* = \{p \in \mathbb{Z}_n;\ \mathrm{ggT}(p, n) = 1\}$. $\circ$ sei gleich der Multiplikation ganzer Zahlen modulo n.