Technische Universität München
Fakultät für Informatik
Lehrstuhl für Informatik 7
Softwarezuverlässigkeit u. Theoretische Informatik
Prof. Dr. Javier Esparza
Dr. Werner Meixner

Wintersemester 2008/09
Lösungsblatt 13-Arbeitsblatt
22. Januar 2009

Diskrete Strukturen

Arbeitsblatt 3

(zu Übungsblatt 13)

Hinweis: *Die Lösungen der Vorbereitungsaufgaben von Blatt 13 werden nachfolgend als Arbeitsblatt zur Verfügung gestellt. Es ist unbedingt notwendig, dass dieses Arbeitsblatt vor der Teilnahme an den Tutorübungen intensiv durchgearbeitet wird.*

Vorbereitung 1

Wir betrachten für Graphen $G = (V, E)$ die erweiterte Form des generischen Suchalgorithmus, in der für jeden besuchten Knoten v dessen Vorgänger $pred[v]$, die Suchnummer $n[v]$ und die Suchtiefe $d[v]$ bestimmt werden.

1. Begründen Sie, warum bei Ausführung des Suchalgorithmus die Suchtiefe für einen Knoten nie überschrieben wird.
2. Bei welchen Auswahlstrategien von Elementen aus der „Worklist W“ besteht W stets aus Knoten mit Suchnummern aus einem Abschnitt $[m, n] = [n] \setminus [m-1]$?
3. Ist das Ergebnis der Suchtiefe eines Knotens v bei Anwendung des generischen Suchalgorithmus mit den Strategieen der Breitensuche einerseits oder der Tiefensuche andererseits mit gleichem Startknoten das Gleiche? Begründen Sie Ihre Antwort ggf. mit einem Beispiel!
4. Der Suchalgorithmus werde mit der Strategie der Breitensuche durchgeführt. Nehmen Sie an, dass u vor v aus der Worklist entfernt wird. Geben Sie ein Beispiel an, in dem $d[u] = d[v]$ gilt.

Lösungsvorschlag

Wir beziehen uns auf den folgenden generischen Suchalgorithmus (siehe Vorlesung).

```
Initialisierung;
while die Worklist nicht leer ist:
        wähle einen Knoten v aus der Worklist;
        falls die Menge der unbesuchten Nachbarn von v nicht leer ist:
                wähle einen unbesuchten Nachbarn u von v;
                (mache Arbeitsschritte)
                markiere u als besucht;
                trage u in die Worklist ein.
        andernfalls entferne v aus der Worklist.
```

Bei der Initialisierung werden der Startknoten s (Wurzel) in die Worklist eingetragen und Anfangswerte durch ($\mathsf{n} \leftarrow 1$; $\mathsf{n}[s] \leftarrow 1$; $\mathsf{d}[v] \leftarrow 0$;) definiert.
Die Auswahlstrategie für den Knoten v bestimmt u. A. Breitensuche und Tiefensuche (oder eine Mischform). Die Auswahlstrategie für den Knoten u ist beliebig und wird nicht spezifiziert.
Die erweiterte Form des Suchalgorithmus erhält man, indem man die Arbeitsschritte wie folgt definiert.

$$\mathsf{n} \leftarrow \mathsf{n}{+}1;\ \mathsf{n}[u] \leftarrow \mathsf{n};\ \mathsf{d}[u] \leftarrow \mathsf{d}[v]{+}1;\ \mathsf{pred}[u] \leftarrow v\,.$$

1. Die Berechnung der Suchtiefe wie auch der Suchnummer und des Vorgängers eines Knotens u erfolgt genau dann, wenn er seine Markierung als „besucht“ erhält. Diese Markierung findet nur einmal statt, weil sie erstens unter der Bedingung steht, dass u noch nicht besucht wurde, und zweitens diese Markierung nirgens entfernt wird.

2. Die Suchnummern definieren eine Reihenfolge, in denen die Knoten erstmalig (und gleichzeitig letztmalig) der Worklist hinzugefügt werden.

   Die geforderte Bedingung bedeutet, dass die Worklist stets die Suchnummern lückenlos enthalten muss. Um die Bedingung zu erhalten, darf also stets nur entweder das Element mit der kleinsten oder der größten Nummer der in der Liste vorhandenen Suchnummern entfernt werden. Dem würde eine Mischung aus Breiten- und Tiefensuche entsprechen.

3. Das Beispiel des Kreises C_5 auf den Knoten $[5]$ mit Startknoten $s = 1$ liefert bei Breitensuche $d(4) = 2$.

   Mit Tiefensuche kommt es zunächst auf die Reihenfolge der besuchten Nachbarknoten an. Wenn wir so vorgehen, dass wir $n(1) = 1$, $n(2) = 2$, $n(3) = 3$ und $n(4) = 4$ erhalten, dann ergibt sich $d(4) = 3$.

4. Alle Knoten, die Nachbar des Startknotens s sind, bekommen bei Breitensuche die gleiche Suchtiefe. Offensichtlich aber ist es bei mehreren Nachbarknoten so, dass einer der Knoten vor dem anderen Knoten aus der Workliste entfernt wird, weil zu einem bestimmten Zeitpunkt immer nur ein einziger Knoten entfernt wird.

Vorbereitung 2

Ganze Zahlen $a, b \in \mathbb{Z}$ nennt man kongruent modulo m, mit $m \in \mathbb{N}$, i. Z. $a \equiv b \pmod{m}$, 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. Genau dann wenn $a \equiv b \pmod{m}$ und gleichzeitig $0 \leq b < m$ gilt, dann gilt $b = a \bmod m$. Diesen Zusammenhang kann man der Definition der Operation mod zugrunde legen.
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

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

1. Berechnen Sie: (i) 5 div 6, (ii) (-5) div 6, (iii) x div 1.

2. Zeigen Sie: Für alle $a \in \mathbb{Z}, m \in \mathbb{N}$ gilt

$$(a \pm m)\operatorname{div} m = a \operatorname{div} m \ \pm 1.$$

3. Zeigen Sie, dass für alle ganzen Zahlen $a \in \mathbb{Z}, m, n \in \mathbb{N}$ gilt:

$$(a \cdot n)\ \operatorname{div}(m \cdot n) = a \operatorname{div} m\,.$$

Lösungsvorschlag

1. Wir führen div mithilfe der angegebenen Gleichung auf mod zurück.

   (i) Seien $a = 5$ und $m = 6$. Dann gilt

$$\begin{aligned} (5 \operatorname{div} 6) \cdot 6 &= 5 - (5 \bmod 6) \\ &= 5 - 5 \\ &= 0\,, \quad \text{und es folgt} \\ 5 \operatorname{div} 6 &= 0\,. \end{aligned}$$

   (ii) Seien $a = -5$ und $m = 6$. Dann gilt

$$\begin{aligned} ((-5)\operatorname{div} 6) \cdot 6 &= -5 - ((-5) \bmod 6) \\ &= (-5 - ((-5+6) \bmod 6)) \\ &= (-5 - 1) \\ &= -6\,, \quad \text{und es folgt} \\ (-5)\operatorname{div} 6 &= -1\,. \end{aligned}$$

   (iii) Seien $a = x$ und $m = 1$. Dann gilt

$$\begin{aligned} (x \operatorname{div} 1) \cdot 1 &= x - (x \bmod 1) \\ &= x - 0\,, \quad \text{und es folgt} \\ x \operatorname{div} 1 &= x\,. \end{aligned}$$

2. Es gilt

$$\begin{aligned} ((a \pm m)\operatorname{div} m) \cdot m &= (a \pm m) - (a \pm m) \bmod m \\ &= (a \pm m) - a \bmod m \\ &= (a - a \bmod m) \pm m \\ &= (a \operatorname{div} m)m \pm m\,, \quad \text{und es folgt} \\ (a \pm m)\operatorname{div} m &= a \operatorname{div} m \pm 1\,. \end{aligned}$$

3. Wir zeigen zunächst $(na)\bmod(nm) = n(a \bmod m)$.

   Seien $b = (na)\bmod(nm)$ und $c = (a \bmod m)$. Dann gelten für passende ganze Zahlen $k, l \in \mathbb{Z}$ die Gleichungen $b = na - knm$ und $c = a - lm$. Außerdem gelten die Ungleichungen $0 \leq b < nm$ und $0 \leq c < m$. Daraus folgt

$$\begin{aligned} b - nc &= (na - knm) - n(a - lm) \\ &= (l - k)nm\,. \end{aligned}$$

Aus den beiden Ungleichungen für b und c folgt aber $-mn < b - nc < nm$, d. h. $-mn < (l-k)nm < nm$. Daraus folgt $l-k = 0$, mithin die zu beweisende Gleichung $b = nc$.

Wir rechnen

$$\begin{aligned}((an)\,\mathrm{div}(mn)) \cdot mn &= (an) - (an)\,\mathrm{mod}(mn) \\ &= n(a - a \bmod m) \\ &= n(a\,\mathrm{div}\, m)m\,.\end{aligned}$$

Division durch mn liefert die zu beweisende Gleichung.

Vorbereitung 3

Zeigen Sie für alle $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$:

$$\begin{aligned} a &\equiv a \bmod m \pmod m\,, \\ (a+b) \bmod m &= [(a \bmod m) + (b \bmod m)] \bmod m\,. \end{aligned}$$

Lösungsvorschlag

1. Die Kongruenz modulo m ist definiert durch

$$x \equiv y \pmod b \quad :\Longleftrightarrow \quad (\exists k \in \mathbb{Z})\,[\,x = y + k \cdot b\,]\,.$$

Nach Definition von $(a \bmod b)$ gilt für ein bestimmtes $k \in \mathbb{Z}$

$$a \bmod b = a + k \cdot b\,, \quad \text{d. h.} \quad a = a \bmod b + k' \cdot b\,,$$

mithin

$$a \equiv a \bmod b \pmod b\,.$$

2. Wir setzen nun

$$\begin{aligned} x &:= (a+b) \bmod m\,, \\ y &:= [(a \bmod m) + (b \bmod m)] \bmod m\,. \end{aligned}$$

Es gilt $0 \leq x, y < m$ und

$$\begin{aligned} x &= a + b + k_x \cdot m\,, \\ y &= (a \bmod m) + (b \bmod m) + k_y \cdot m\,, \\ (a \bmod m) &= a + k_a \cdot m\,, \\ (b \bmod m) &= b + k_b \cdot m \end{aligned}$$

für gewisse $k_a, k_b, k_x, k_y \in \mathbb{Z}$. Nun folgt

$$\begin{aligned} y &= a + k_a \cdot m + b + k_b \cdot m + k_y \cdot m \\ &= x - k_x \cdot m + k_a \cdot m + k_b \cdot m + k_y \cdot m \\ &= x + (k_a + k_b + k_y - k_x) \cdot m \\ &= x + k \cdot m\,. \end{aligned}$$

Wegen $0 \leq x, y < m$ folgt $x = y$.

Vorbereitung 4

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

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

$$x \circ y = x + y + xy.$$

2. Sei S gleich der Potenzmenge $\mathcal{P}(X)$ $(= 2^X)$ einer beliebigen Menge X und sei $\circ$ gegeben durch

$$A \circ B = (A \cup B) \setminus (A \cap B).$$

Lösungsvorschlag

1. (a) Zunächst ist zu prüfen, ob durch die Gleichung $x \circ y = x + y + x \cdot y$ tatsächlich eine Abbildung von $S \times S$ in S definiert ist.

   Seien $x, y \in \mathbb{R} \setminus \{-1\}$. Es gilt offenbar $x \circ y \in \mathbb{R}$, denn wir können zeigen, dass $-1 = x + y + x \cdot y$ einen Widerspruch ergibt und deswegen $x, y \in \mathbb{R} \setminus \{-1\}$ gelten muss.

$$\begin{aligned} -1 = x + y + x \cdot y \quad &\Rightarrow \quad -1 - y = x(1 + y) \\ &\Rightarrow \quad x = \frac{-1 - y}{1 + y} \\ &\Rightarrow \quad x = -1\,. \end{aligned}$$

   (b) Wir zeigen die Assoziativität von $\circ$.

$$\begin{aligned} x \circ (y \circ z) &= x + (y \circ z) + x \cdot (y \circ z) \\ &= x + (y + z + y \cdot z) + x \cdot (y + z + y \cdot z) \\ &= x + y + z + y \cdot z + x \cdot y + x \cdot z + x \cdot y \cdot z \\ &= (x + y + x \cdot y) + z + (x + y + x \cdot y) \cdot z \\ &= (x \circ y) + z + (x \circ y) \cdot z \\ &= (x \circ y) \circ z\,. \end{aligned}$$

   (c) $x = 0$ ist das Einselement bezüglich $(x \circ y)$.

$$0 \circ y = 0 + y + 0 \cdot y = y\,.$$

   Das linke Einselement ist offensichtlich auch rechtes Einselement, d. h. Einselement.

   (d) Wir zeigen, dass zu einem Element $x \in S$ das Inverse gegeben ist durch $x^{-1} = -\frac{x}{1+x}$. Es gilt

$$\begin{aligned} x \circ y = 0 \quad &\Leftrightarrow \quad x + y + x \cdot y = 0 \\ &\Leftrightarrow \quad y = -\frac{x}{1 + x}\,. \end{aligned}$$

   Die Existenz eines linken Inversen ist damit bewiesen.

Allein schon aus der offensichtlichen Kommutativität folgt hier, dass jedes linke auch rechtes Inverses ist. Es sei aber bemerkt, dass die Beziehung zwischen linken und rechten Inversen auch ohne Kommutativität ganz allgemein in Gruppen untersucht werden kann. Es genügt, allein die Existenz des linken Inversen nachzuweisen.

Damit ist der Nachweis erbracht, dass G eine kommutative Gruppe ist.

2. Die Mengenoperation, die hier betrachtet wird, nennt man die Bildung der symmetrischen Mengendifferenz. Wir führen zunächst die Bildung der einfachen Mengendifferenz auf die Komplementbildung innerhalb X zurück, d. h. $A \setminus B = A \cap \overline{B}$ mit $\overline{Y} = X \setminus Y$. Dies hat den Vorteil, die De Morganschen Gesetze anwenden zu können.

   Es gilt

$$\begin{aligned} A \circ B &= (A \cup B) \cap (\overline{A \cap B}) \\ &= (A \cup B) \cap (\overline{A} \cup \overline{B}) \\ &= (A \cap \overline{A}) \cup (A \cap \overline{B}) \cup (B \cap \overline{A}) \cup (B \cap \overline{B}) \\ &= (A \cap \overline{B}) \cup (B \cap \overline{A}) \,, \end{aligned}$$

   und folglich

$$\overline{A \circ B} = (A \cap B) \cup (\overline{A} \cap \overline{B}) \,.$$

   (a) Offensichtlich ist durch die Gleichung $A \circ B = (A \cup B) \setminus (A \cap B)$ eine Abbildung von $S \times S$ in S definiert, denn die gesamte Potenzmenge von X ist als Bildbereich der Verknüpfung zugelassen.

   (b) Die Bildung einer mehrfachen symmetrischen Mengendifferenz läßt sich mit drei Mengen A, B, C gut veranschaulichen. Es werden genau jene Elemente erhalten, die entweder in genau einer der Mengen A, B, C sind oder die im Durchschnitt aller 3 Mengen enthalten sind. Dies wird durch folgende Rechnung bestätigt zum Nachweis der Assoziativität:

$$\begin{aligned} (A \circ B) \circ C &= (A \circ B) \cap \overline{C} \,\cup\, (\overline{A \circ B}) \cap C \\ &= [(B \cap \overline{A}) \cup (A \cap \overline{B})] \cap \overline{C} \,\cup\, [(A \cap \overline{B}) \cup (B \cap \overline{A})] \cap C \\ &= (A \cap \overline{B} \cap \overline{C}) \cup (B \cap \overline{A} \cap \overline{C}) \cup (C \cap \overline{A} \cap \overline{B}) \cup (A \cap B \cap C). \end{aligned}$$

   Substituiert man B für A, C für B und A für C, dann erhält man einerseits den Ausdruck $(B \circ C) \circ A$ und andererseits die gleiche Formel wie oben, denn die Formel ist invariant gegenüber der genannten Permutation von Variablen. Also gilt

$$(A \circ B) \circ C = (B \circ C) \circ A = A \circ (B \circ C) \,.$$

   (c) Das Einselement der symmetrischen Mengendifferenz ist offensichtlich die leere Menge.

$$A \circ \emptyset = (A \cup \emptyset) \setminus (A \cap \emptyset) = A \,.$$

   (d) Die Inverse von A ist A selbst. Es gilt

$$A \circ A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset \,.$$

   Damit ist der Nachweis erbracht, dass G eine Gruppe ist.