6.0 VU Theoretische Informatik **2023W** **28.2.2024**			
Matrikelnummer	Nachname **Lösung**	Vorname	Gruppe **A**

Aufgabe 1

Sei $\mathbb{G}$ die Menge der geraden Zahlen, also $\{0, 2, 4, \dots\}$, und $\mathbb{U}$ die Menge der ungeraden Zahlen, also $\{1, 3, 5, \dots\}$. Wir definieren die Menge M als $M = \mathbb{G} \times \mathbb{U}$, d.h., als die Zahlenpaare bestehend aus einer geraden und einer ungeraden Zahl.

Beweisen Sie auf folgende zwei Arten, dass die Menge M abzählbar unendlich ist.

(a) [**8 Punkte**] Skizzieren Sie eine Aufzählung der Elemente der Menge M. Geben Sie zumindest die ersten 16 Elemente Ihrer Aufzählung an. Zwecks Nachvollziehbarkeit der Aufzählung sollten Sie bei dieser Aufzählung folgendermaßen vorgehen.

- Gliedern Sie die Zahlenpaare in Gruppen und beschreiben Sie kurz (max. 2 Sätze), wie diese Gruppen gebildet werden. Aus dieser Beschreibung soll unmittelbar erkennbar sein, wie sich die Aufzählung der ersten 16 Elemente auf beliebig viele Elemente von M erweitern ließe.

- Geben Sie für jede Gruppe auch die Anzahl der Elemente in dieser Gruppe sowie die Positionen, die die Elemente der Gruppe in der Aufzählung einnehmen, an!

Lösung

Zahlenpaare	Anzahl	Positionen
(0,1)	1	0
(0,3), (2,1), (2,3)	3 $(= 2^2 - 1)$	1, …, 3
(0,5), (2,5), (4,1), (4,3) (4,5)	5 $(= 3^2 - 2^2)$	4, …, 8
(0,7), (2,7), (4,7), (6,1), (6,3) (6,5), (6,7)	7 $(= 4^2 - 3^2)$	9, …, 15
etc.		

Bildung der Gruppen: Die i-te Gruppe (mit $i = 1, 2, 3, \dots$) besteht aus allen Zahlenpaaren, die sich mit den ersten i Elementen von $\mathbb{G}$ und $\mathbb{U}$ aber nicht mit den ersten $i - 1$ Elementen von $\mathbb{G}$ und $\mathbb{U}$ bilden lassen.

Anmerkungen:

- Natürlich gibt es auch andere Möglichkeiten, die Menge M aufzuzählen. Etwa kann man die i-te Gruppe als Menge der Paare (g, u) mit $g + u = 2i - 1$ definieren, wodurch sich $\{(0, 1)\}$, $\{(0, 3), (2, 1)\}$, $\{(0, 5), (2, 3), (4, 1)\}$ etc. ergibt.

- Werden Gruppen mit unendlich vielen Elementen gebildet, etwa $G_1 = \{(0, u) \mid u \in \mathbb{U}\}$, $G_2 = \{(2, u) \mid u \in \mathbb{U}\}$ etc., ergibt sich keine korrekte Aufzählung: Diese Aufzählung kommt nie über die erste Gruppe hinaus.

(b) [**4 Punkte**] Geben Sie eine bijektive Abbildung $f\colon \mathbb{N}^2 \to M$ und ihre Umkehrfunktion $f^{-1}\colon M \to \mathbb{N}^2$ an.

Bemerkung: In der Vorlesung wurde gezeigt, dass die Menge $\mathbb{N}^2$ abzählbar unendlich ist. Indem Sie eine bijektive Abbildung zwischen den Mengen $\mathbb{N}^2$ und M angeben, beweisen Sie wiederum, dass die Menge M abzählbar unendlich ist.

Lösung

$f : \mathbb{N}^2 \to M$ mit $f(n_1, n_2) = (2n_1, 2n_2 + 1)$ für beliebiges Element $(n_1, n_2) \in \mathbb{N}^2$.
$f^{-1} : M \to \mathbb{N}^2$ mit $f^{-1}(n_1, n_2) = (\frac{n_1}{2}, \frac{n_2-1}{2})$ für beliebiges Element $(n_1, n_2) \in M$.

Aufgabe 2

Sei $L_1 = \{a^{2n}b^{4n}c^{7k}a^{2j} \mid n, k, j \geq 0\}$ und $L_2 = \{a^{2n}b^{2k}a^{4k} \mid n, k \geq 0\}$.

(a) [**3 Punkte**] Geben Sie eine kontextfreie Grammatik an, die L_1 erzeugt.

Lösung

$G = (\{S, A, B, C\}, \{a, b, c\}, P, S)$ mit
$P = \{S \to ABC, \quad A \to a^2Ab^4 \mid \varepsilon, \quad B \to c^7B \mid \varepsilon, \quad C \to a^2C \mid \varepsilon\}$

(b) [**5 Punkte**] Zeigen Sie mit Hilfe des Satzes von Chomsky-Schützenberger, dass auch L_2 kontextfrei ist, indem Sie eine geeignete Sprache D_n, eine reguläre Menge R sowie einen geeigneten Homomorphismus h angeben, sodass gilt: $L = h(D_n \cap R)$.
(D_n bezeichnet eine Dyck-Sprache (wohlgeformte Klammerausdrücke) über n verschiedenen Klammerpaaren.)

Lösung

L ist kontextfrei, da $L = h(D_2 \cap R)$, wobei $R = \{(,)\}^*\{[\}^*\{]\}^*$ und
$h : \{(,),[,]\}^* \longrightarrow \{a, b\}^*$ mit $h(() = h()) = a, \quad h([) = b^2, \quad h(]) = a^4$

(c) [**2 Punkte**] Geben Sie $L = L_1 \cap L_2$ an.

Lösung

$L = L_1 \cap L_2 = \{a^{2n}b^{4n}a^{8n} \mid n \geq 0\}$

(d) [**2 Punkte**] Kann $L = L_1 \cap L_2$ von einem linear beschränkten Automaten akzeptiert werden? Begründen Sie Ihre Antwort.

Lösung

Ja. L_1 wie auch L_2 sind kontextfrei, wie oben bewiesen. Kontextfreie Sprachen sind zwar nicht unter Durchschnitt abgeschlossen, und in der Tat ist $L = L_1 \cap L_2$ nicht kontextfrei. Kontextfreie Sprachen sind aber eine echte Teilmenge der kontextsensitiven, welche sehr wohl unter Durchschnitt abgeschlossen sind. L ist also jedenfalls kontextsensitiv, und kann somit auch von einem linear beschränkten Automaten akzeptiert werden.

Aufgabe 3

Betrachten Sie folgendes RM-Programm P zur Berechnung von f vom Typ $\mathbb{N}^2 \to \mathbb{N}$:

$$P = (0,\ \{(0, A_1, 1),\ (1, t_2, 5, 2),\ (2, S_2, 3),\ (3, A_1, 4),\ (4, A_1, 0)\})$$

(a) [**3 Punkte**] Führen Sie eine Beispielrechnung mit den Registerinhalten $R(1) = 3$, $R(2) = 1$ durch.

Falls P für diese Eingabe hält, geben Sie alle Schritte an bis $f(3,1)$ feststeht. Falls P in eine Endlosschleife gerät, so deuten Sie das mit „…“ an.

Lösung

0:$(3,1) \Rightarrow$ 1:$(4,1) \Rightarrow$ 2:$(4,1) \Rightarrow$ 3:$(4,0) \Rightarrow$ 4:$(5,0) \Rightarrow$ 0:$(6,0) \Rightarrow$ 1:$(7,0) \Rightarrow$ 5:$(7,0)$.
5 ist eine Endmarke. Das Programm terminiert also und es gilt $f(3,1) = 7$.

(b) [**3 Punkte**] Welche Funktion f wird durch P berechnet?

Lösung

$f(m,n) = m + 3n + 1$

(c) [**2 Punkte**] Welche Funktion wird durch μf dargestellt?

Lösung

$\mu f(n) = \min_{y\geq 0}[f(y,n) = 0] = \min_{y\geq 0}[y + 3n + 1 = 0]$.
μf definiert die 1-stellige Funktion, deren Ergebnis für jeden Eingabewert undefiniert ist.

(d) [**2 Punkte**] Welche Funktion wird durch $\overline{\mu} f$ dargestellt?

Lösung

$\overline{\mu} f(m,n) = \min_{y\geq 0}[f(y,n) = m] = \min_{y\geq 0}[y + 3n + 1 = m] = \min_{y\geq 0}[y = m - 3n - 1]$
Es gilt daher

$$\overline{\mu} f(m,n) = \begin{cases} m - 3n - 1 & \text{falls } m \geq 3n + 1 \\ \text{undefiniert} & \text{sonst} \end{cases}$$

(e) [**2 Punkte**] Kann man ein Programm schreiben, das für jede vorgelegte Turingmaschine entscheidet, ob sie die selbe Funktion berechnet wie das RM-Programm P? Begründen Sie Ihre Antwort kurz.
Anmerkung: Punkte gibt es nur für eine hinreichend begründete Antwort.

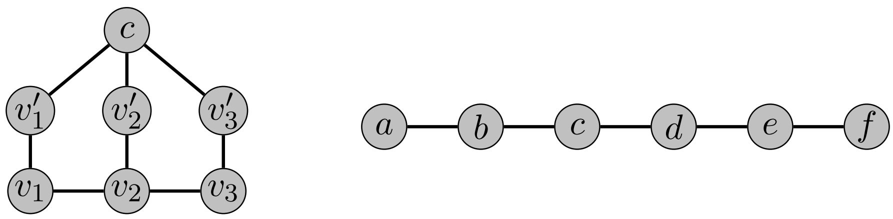
Lösung

Die Menge $\{f\}$ ist eine (extensionale) nicht-triviale Funktions-Eigenschaft. Daher ist der Satz von Rice für Funktionen anwendbar. Das Problem ist folglich unentscheidbar.

Aufgabe 4 [12 Punkte]

Ein ungerichteter Graph $G = (V, E)$ heisst *Quasistern* wenn es zumindest einen "Zentral-Knoten" $c \in V$ gibt sodass alle anderen Knoten $v \in V$ maximal Distanz 2 von c haben, also entweder direkt mittels Kante mit c verbunden sind, oder über einen Pfad der Länge 2 ($[v, v'], [v', c] \in E$).

Beispiele: G_1 ist ein Quasistern mit Zentral-Knoten c. G_2 hingegen ist kein Quasistern, da es keinen Knoten gibt der alle anderen mit einem Pfad mit maximaler Länge 2 verbindet.



G_1 G_2

Wir betrachten das klassische Dreifärbbarkeitsproblem (3-COL) und die auf Quasisterne eingeschränkte Variante davon (3-COL-Q).

3-COL Instanz: Ein ungerichteter Graph $G = (V, E)$. Frage: Gibt es eine Funktion $f\colon V \to \{0, 1, 2\}$, so dass für alle Kanten $[v_i, v_j] \in E$ gilt: $f(v_i) \neq f(v_j)$.

3-COL-Q Instanz: Ein Quasistern $G = (V, E)$. Frage: Gibt es eine Funktion $f\colon V \to \{0, 1, 2\}$, so dass für alle Kanten $[v_i, v_j] \in E$ gilt: $f(v_i) \neq f(v_j)$.

Betrachten Sie die folgende Reduktion R von 3-COL nach 3-COL-Q die jedem Graph $G = (V, E)$ einen Quasistern $R(G) = (V^*, E^*)$ mit

$$\begin{aligned} V^* &= V \cup \{v' \mid v \in V\} \cup \{c\};\ \text{und} \\ E^* &= E \cup \{(v, v'), (v', c) \mid v \in V\}, \end{aligned}$$

zuweist.
Zeigen Sie die Korrektheit der Reduktion, also:
G ist eine positive Instanz von 3-COL $\iff$ $R(G)$ ist eine positive Instanz von 3-COL-Q.

Lösung

$\Longrightarrow$: Sei G eine positive Instanz von 3-COL. Dann gibt es eine Funktion $f\colon V \to \{0, 1, 2\}$, so dass für alle Kanten $[v_i, v_j] \in E$ gilt: $f(v_i) \neq f(v_j)$. Wir definieren $f^* : V^* \to \{0, 1, 2\}$ mit (1) $f^*(v) = f(v)$ für alle $v \in V$, (2) $f^*(v) = 0$ für alle $v \in V$ mit $f(v) \in \{1, 2\}$, (3) $f^*(v) = 1$ für alle $v \in V$ mit $f(v) = 0$, (4) $f^*(c) = 2$.
Wir zeigen dass f^* eine gültige Färbung für $R(G)$ ist. Sei also $[u, w]$ eine Kante aus E^*. Gemäß der Definition von E^* unterscheiden wir folgende Fälle: (1) $u, w \in V$; (2) $u = v$ und $w = v'$ für $v \in V$; (3) $u = v'$, $w = c$ für $v \in V$.
Für den Fall (1) gilt laut Definition von f^* und aufgrund der Annahme dass f eine gültige Färbung für G ist: $f^*(u) = f(u) \neq f(w) = f^*(w)$. Für den Fall (2) gilt laut Definition von f^* (Bedingungen (2) und (3)) $f^*(u) \neq f^*(w)$; Für den Fall (3) wissen wir dass $f^*(w) = 2 \neq f^*(u) \in \{0, 1\}$ (Bedingungen (2)–(3)).
Wir haben somit gezeigt dass für alle Kanten $[u, w] \in E^*$, $f^*(u) \neq f^*(w)$ gilt. f^* ist daher eine gültige Färbung für $R(G)$; und $R(G)$ daher eine positive Instanz von 3-COL-Q.
$\Longleftarrow$: Sei $R(G)$ eine positive Instanz von 3-COL-Q. Da G ein Subgraph von $R(G)$, ist klarerweise G auch eine positive Instanz von 3-COL.

Aufgabe 5

(a) [6 Punkte] Zeigen Sie mit Hilfe der Annotierungsregeln, dass die folgende Korrektheitsaussage wahr hinsichtlich *partieller* Korrektheit ist.
Einige nützliche Annotierungsregel:
$\{F\} v := e \quad \mapsto \quad \{F\} v := e \{\exists v' (F\left[\begin{smallmatrix} v' \\ v \end{smallmatrix}\right] \land v = e\left[\begin{smallmatrix} v' \\ v \end{smallmatrix}\right])\}$

`if` e `then` $\{F\} \cdots$ `else` $\{G\} \quad \mapsto \quad \{(e \supset F) \wedge (\neg e \supset G)\}$`if` e `then` $\{F\} \cdots$ `else` $\{G\}$
$\{F\}$`if` e `then` $\cdots$ `else` $\quad \mapsto \quad \{F\}$`if` e `then` $\{F \wedge e\} \cdots$ `else` $\{F \wedge \neg e\}$
`abort` $\quad \mapsto \quad \{1\}$`abort`$\{0\}$

$\boldsymbol{\{\, y > 1 \,\}}$
{`if` $x > 0$ `then`
    `if` $x > y$ `then`
        $z \coloneqq x$
    `else`
        `abort`
    // end if
`else`
    $z \coloneqq y * y$;
// end if
$z \coloneqq z - y$ }
$\boldsymbol{\{\, z > 0 \,\}}$

Lösung

$\{\, y > 1 \,\}$
{`if` $x > 0$ `then`
    $\{\, y > 1 \wedge x > 0 \,\}$
    `if` $x > y$ `then`
        $\{\, y > 1 \wedge x > 0 \wedge x > y \,\}$
        $\{\, x - y > 0 \,\}$
        $z \coloneqq x$
        $\{\, z - y > 0 \,\}$
    `else`
        $\{\, y > 1 \wedge x > 0 \wedge x \not> y \,\}$
        $\{\, 1 \,\}$
        `abort`
        $\{\, 0 \,\}$
        $\{\, z - y > 0 \,\}$
    // end if
    $\{\, z - y > 0 \,\}$
`else`
    $\{\, y > 1 \wedge x \not> 0 \,\}$
    $\{\, y * y - y > 0 \,\}$
    $z \coloneqq y * y$;
    $\{\, z - y > 0 \,\}$
// end if
$\{\, z - y > 0 \,\}$
$z \coloneqq z - y$ }
$\{\, z > 0 \,\}$

$(y > 1 \wedge x > 0 \wedge x > y) \supset x - y > 0$
gültig, da $x - y > 0$ der Prämisse $x > y$ entspricht.

$(y > 1 \wedge x \wedge 0 \wedge x \leq y) \supset 1$
gültig, da $F \supset 1$ für beliebiges F gültig ist.

$0 \supset z - y > 0$
gültig, da $0 \supset F$ für beliebiges F gültig ist.

$(y > 1 \wedge x \leq 0) \supset y^2 > y$
$y^2 > y$ gilt für alle Werte von y ausgenommen $y \in \{0, 1\}$. Diese Werte werden aber von der Prämisse $y > 1$ ausgeschlossen, daher ist diese Formel gültig.

Die vier Implikationen, die durch die Annotierungsregeln entstehen, sind alle gültig, daher ist die Aussage wahr hinsichtlich partieller Korrektheit.

(b) [6 Punkte] Zeigen Sie, dass die Korrektheitsaussage in der vorigen Teilaufgabe falsch hinsichtlich totaler Korrektheit ist.

Vorgangsweise: Geben Sie ein Gegenbeispiel an und argumentieren Sie, dass es tatsächlich ein solches ist. Genauer: Wählen Sie eine passende Eingabe und zeigen Sie, dass diese zulässig, das Ergebnis des Programms für diese Eingabe aber nicht definiert ist. Verwenden Sie dafür die strukturelle operationale Semantik oder die natürliche Semantik. Folgende Gleichungen können dabei helfen.

$$[\{\Pi\,;\Omega\}]\,\sigma = [\Omega]\,[\Pi]\,\sigma \qquad\qquad [\texttt{if } e \texttt{ then } \Pi \texttt{ else } \Omega]\,\sigma = \begin{cases} [\Pi]\,\sigma & \text{wenn } [e]\,\sigma \neq 0 \\ [\Omega]\,\sigma & \text{wenn } [e]\,\sigma = 0 \end{cases}$$

Lösung

Das Ergebnis des Programms ist undefiniert, falls die `abort`-Anweisung ausgeführt wird. Diese wird erreicht, wenn die Vorbedingung und die erste If-Bedingung wahr sowie die zweite If-Bedingung falsch ist. Wir benötigen daher eine Eingabe σ, die die Bedingungen $y > 1$, $x > 0$ und $x \leq y$ erfüllt. Wir wählen $\sigma(x) = 1$, $\sigma(y) = 2$ und $\sigma(v) = 0$ für $v \notin \{x, y\}$.

σ ist eine zulässig Eingabe (σ erfüllt die Vorbedingung):

$$[y > 1]\,\sigma = (\sigma(y) > 1) = (2 > 1) = 1 \text{ (wahr)}$$

Das Ergebnis ist undefiniert:

$$\begin{aligned} &[\{\texttt{if } x > 0 \ \ldots\texttt{;} z \coloneqq z - y\}]\,\sigma \\ &= [z \coloneqq z - y]\,[\texttt{if } x > 0 \ \ldots]\,\sigma && [x > 0]\,\sigma = (1 > 0) = 1 \text{ (wahr)} \\ &= [z \coloneqq z - y]\,[\texttt{if } x > y \ \ldots]\,\sigma && [x > y]\,\sigma = (1 > 2) = 0 \text{ (falsch)} \\ &= [z \coloneqq z - y]\,[\texttt{abort}]\,\sigma \\ &= \text{undefiniert} \end{aligned}$$