Einführung in die Theoretische Informatik

Martin Avanzini Christian Dalvit Jamie Hochrainer
Georg Moser Johannes Niederhauser Jonas Schöpf

https://tcs-informatik.uibk.ac.at

universität innsbruck

Zusammenfassung

Satz

Sei Σ ein Alphabet und sei $x \in \Sigma^*$. Die folgenden Beschreibungen kontextfreier Sprachen sind äquivalent:

1. $x \in \mathrm{L}(A)$ *nach dem rekursiven Inferenzverfahren*
2. $A \stackrel{*}{\Rightarrow} x$
3. $A \stackrel{*}{\underset{\ell}{\Rightarrow}} x$
4. $A \stackrel{*}{\underset{r}{\Rightarrow}} x$
5. *Es existiert ein Syntaxbaum mit Wurzel A und Ergebnis x*

$$
\begin{tikzcd}
x \in \mathrm{L}(A) \arrow[r, Rightarrow] & \exists\ \text{Syntaxbaum} \arrow[d, Rightarrow] \\
A \stackrel{*}{\Rightarrow} x \arrow[u, Rightarrow] & A \stackrel{*}{\underset{\ell}{\Rightarrow}} x \arrow[l, Rightarrow]
\end{tikzcd}
$$

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Formales Beweisen, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

Algebraische Strukturen, Boolesche Algebra, Universelle Algebra

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Chomsky-Hierarchie, Reguläre Sprachen, Kontextfreie Sprachen, Anwendungen von formalen Sprachen

Einführung in die Berechenbarkeitstheorie und Komplexitätstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen, Komplexitätstheorie

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare universität innsbruck

Berechenbarkeitstheorie

Einführung in die Berechenbarkeitstheorie

Frage

Ist jedes Problem algorithmisch lösbar?

Antwort

Nein

Ein einfaches Programm

```
main()
{
      printf("hello, world");
}
```

Beispiel

betrachte Programm F:

```
main()
{
  int n, summe = 3, x, y, z;
  scanf(``%d'', &n);
  while (1) {
    for (x=1; x <= summe-2; x++)
    for (y=1; y <= summe-x-1; y++) {
      z = summe - x - y;
      if (pow(x,n) + pow(y,n) == pow(z,n))
      printf("hello, world");
    } summe++;
  }
}
```

Das Programm F ist kein „hello, world“-Programm

Beispiel (Fortsetzung)

- Code repräsentiert den großen Fermat; $x^n + y^n = z^n$, für alle n
- widerlegt von Andrew Wiles, 1980er
- In der Simpons Folge “The Wizard of Evergreen Terrace” schreibt Homer die folgende (scheinbare) Lösung an die Tafel:

$$3987^{12} + 4365^{12} = 4472^{12} \ .$$

  Das ist zwar falsch, aber auf einem einfachen Taschenrechner erscheint die Lösung (durch Rundungsfehler) als richtig.

Beispiel

betrachte Programm G

```
main()
{
  int n, x, y, z, test, summe=4;
  while (1) {
    test = 0;
    for (x=2; x <= summe; x++) {
      y = summe - x;
      if (is_prime(x) && is_prime(y)) test = 1;
    }
    if (!test) printf("hello, world");
    summe = summe + 2;
  }
}
```

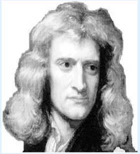
Das Programm G ist wahrscheinlich kein „hello, world“-Programm[1]

[1] G ist kein „hello, world“-Programm für Zahlen $\leqslant 10^{17}$

Großer Fermat (1637)

Die Gleichung $a^n + b^n = c^n$ besitzt für $n > 2$ keine Lösung in $\mathbb{N}$

Vermutung von Goldbach (1742)



Jede gerade Zahl ($\geqslant$ 2) kann als Summe zweier Primzahlen dargestellt werden

Satz

Es kann niemals ein Testprogramm für „hello, world"-Programme geben

Entscheidbarkeit & Unentscheidbarkeit

Definition (informell)

Ein Problem, das algorithmisch nicht lösbar ist, wird unentscheidbar genannt; andernfalls heißt das Problem entscheidbar

Definition

Als Halteproblem bezeichnen wir das Problem, ob ein beliebiges Programm auf seiner Eingabe hält.

Definition

Postsches Korrespondenzproblem: Gegeben zwei gleich lange Listen von (nicht-leeren) Wörtern $w_1, w_2, \dots, w_n$ und $x_1, x_2, \dots, x_n$. Gesucht sind Indizes $i_1, i_2, \dots, i_m$, sodass

$$w_{i_1} w_{i_2} \dots w_{i_m} = x_{i_1} x_{i_2} \dots x_{i_m}$$

Satz

Die folgenden Probleme sind entscheidbar:

- *das Erfüllbarkeitsproblem der Aussagenlogik (SAT)*
- *das Wortproblem der Boolschen Algebra*
- *sei G eine KFG, ist $\mathsf{L}(G) = \varnothing$?*
- *...*

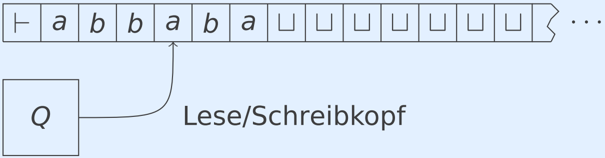
Satz

Die folgenden Probleme sind unentscheidbar:

- *das Halteproblem*
- *das Postsche Korrespondenzproblem*
- *sei G eine KFG über Σ, ist $\mathsf{L}(G) = \Sigma^*$?*
- *...*

Definition (informell)

deterministische, einbändige Turingmaschine (TM):



- Eine TM verwendet ein einseitig unendliches Band als Speicher
- Zu Beginn der Berechnung steht die Eingabe auf dem Band
- Der Speicher wird mit einem Lese/Schreibkopf gelesen oder beschrieben
- Das Verhalten der TM wird durch die endliche Kontrolle Q kontrolliert

Definition (formal)

eine deterministische, einbändige Turingmaschine (TM) M ist ein 9-Tupel

$$M = (Q, \Sigma, \Gamma, \vdash, \sqcup, \delta, s, t, r)$$

sodass

1. Q eine endliche Menge von Zuständen,
2. Σ eine endliche Menge von Eingabesymbolen,
3. Γ eine endliche Menge von Bandsymbolen, mit $\Sigma \subseteq \Gamma$,
4. $\vdash \in \Gamma \setminus \Sigma$, der linke Endmarker,
5. $\sqcup \in \Gamma \setminus \Sigma$, das Blanksymbol,
6. $\delta \colon Q \times \Gamma \to Q \times \Gamma \times \{\mathrm{L}, \mathrm{R}\}$ die Übergangsfunktion,
7. $s \in Q$, der Startzustand,
8. $t \in Q$, der akzeptierende Zustand und
9. $r \in Q$, der verwerfende Zustand mit $t \neq r$.

Definition (Übergangsfunktion)

die Gleichung $\delta(p, a) = (q, b, d)$ bedeutet: Wenn die TM M im Zustand p das Symbol a liest, dann

1. M ersetzt a durch b auf dem Band
2. der Lese/Schreibkopf bewegt sich einen Schritt in die Richtung d
3. M wechselt in den Zustand q

Definition (Zusatzbedingungen)

- Der linke Endmarker darf nicht überschrieben werden

$$\forall\, p \in Q, \exists\, q \in Q \quad \delta(p, \vdash) = (q, \vdash, \mathsf{R})$$

- Wenn die TM akzeptiert/verwirft, bleibt die TM in diesem Zustand

$$\forall\, b \in \Gamma, \exists\, c, c' \in \Gamma \text{ und } d, d' \in \{\mathsf{L}, \mathsf{R}\}\colon \quad \begin{aligned} \delta(t, b) &= (t, c, d) \\ \delta(r, b) &= (r, c', d') \end{aligned}$$

Beispiel

sei $M = (\{s, t, r, q_1, q_2, q_3\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1, \mathrm{X}, \mathrm{Y}\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ wie folgt

$p \in Q$	$a \in \Gamma$	$\delta(p, a)$	$p \in Q$	$a \in \Gamma$	$\delta(p, a)$
s	$\vdash$	$(s, \vdash, \mathrm{R})$	q_2	$\vdash$	$(r, \vdash, \mathrm{R})$
s	$\sqcup$	$(r, \sqcup, \mathrm{R})$	q_2	$\sqcup$	$(r, \sqcup, \mathrm{R})$
s	0	$(q_1, \mathrm{X}, \mathrm{R})$	q_2	0	$(q_2, 0, \mathrm{L})$
s	1	$(r, 1, \mathrm{R})$	q_2	1	$(r, 1, \mathrm{R})$
s	X	$(r, \mathrm{X}, \mathrm{R})$	q_2	X	$(s, \mathrm{X}, \mathrm{R})$
s	Y	$(q_3, \mathrm{Y}, \mathrm{R})$	q_2	Y	$(q_2, \mathrm{Y}, \mathrm{L})$
q_1	$\vdash$	$(r, \vdash, \mathrm{R})$	q_3	$\vdash$	$(r, \vdash, \mathrm{R})$
q_1	$\sqcup$	$(r, \vdash, \mathrm{R})$	q_3	$\sqcup$	$(t, \sqcup, \mathrm{R})$
q_1	0	$(q_1, 0, \mathrm{R})$	q_3	0	$(r, 0, \mathrm{R})$
q_1	1	$(q_2, \mathrm{Y}, \mathrm{L})$	q_3	1	$(r, 1, \mathrm{R})$
q_1	X	$(r, \mathrm{X}, \mathrm{R})$	q_3	X	$(r, \mathrm{X}, \mathrm{R})$
q_1	Y	$(q_1, \mathrm{Y}, \mathrm{R})$	q_3	Y	$(q_3, \mathrm{Y}, \mathrm{R})$
t	$*$	$(t, *, \mathrm{R})$	r	$*$	$(r, *, \mathrm{R})$

Konfiguration einer TM

Definition

eine Konfiguration einer TM M ist ein Tripel (p, x, n), sodass

1. $p \in Q$ Zustand,
2. $x = y\sqcup^\infty$ Bandinhalt $\qquad y \in \Gamma^*$
3. $n \in \mathbb{N}$ Position des Lese/Schreibkopfes

Definition

Startkonfiguration bei Eingabe $x \in \Sigma^*$: $(s, \vdash x\sqcup^\infty, 0)$

Beispiel

Sei 0011 die Eingabe der TM M, dann ist die Startkonfiguration gegeben durch $(s, \vdash 0011\sqcup^\infty, 0)$

Schrittfunktion von TMs

Definition

Relation $\xrightarrow[M]{1}$ ist wie folgt definiert:

$$(p, z, n) \xrightarrow[M]{1} \begin{cases} (q, z', n-1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{L}) \\ (q, z', n+1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{R}) \end{cases}$$

z' ist String, den wir aus z erhalten, wenn z_n durch b ersetzt

Definition

reflexive, transitive Hülle $\xrightarrow[M]{*}$:

1. $\alpha \xrightarrow[M]{0} \alpha$
2. $\alpha \xrightarrow[M]{n+1} \beta$, wenn $\alpha \xrightarrow[M]{n} \gamma \xrightarrow[M]{1} \beta$ für Konfiguration γ
3. $\alpha \xrightarrow[M]{*} \beta$, wenn $\exists\, n \quad \alpha \xrightarrow[M]{n} \beta$

Beispiel (Wiederholung)

sei $M = (\{s, t, r, q_1, q_2, q_3\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1, \mathsf{X}, \mathsf{Y}\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ wie folgt

$p \in Q$	$a \in \Gamma$	$\delta(p, a)$	$p \in Q$	$a \in \Gamma$	$\delta(p, a)$
s	$\vdash$	$(s, \vdash, \mathsf{R})$	q_2	$\vdash$	$(r, \vdash, \mathsf{R})$
s	$\sqcup$	$(r, \sqcup, \mathsf{R})$	q_2	$\sqcup$	$(r, \sqcup, \mathsf{R})$
s	0	$(q_1, \mathsf{X}, \mathsf{R})$	q_2	0	$(q_2, 0, \mathsf{L})$
s	1	$(r, 1, \mathsf{R})$	q_2	1	$(r, 1, \mathsf{R})$
s	X	$(r, \mathsf{X}, \mathsf{R})$	q_2	X	$(s, \mathsf{X}, \mathsf{R})$
s	Y	$(q_3, \mathsf{Y}, \mathsf{R})$	q_2	Y	$(q_2, \mathsf{Y}, \mathsf{L})$
q_1	$\vdash$	$(r, \vdash, \mathsf{R})$	q_3	$\vdash$	$(r, \vdash, \mathsf{R})$
q_1	$\sqcup$	$(r, \vdash, \mathsf{R})$	q_3	$\sqcup$	$(t, \sqcup, \mathsf{R})$
q_1	0	$(q_1, 0, \mathsf{R})$	q_3	0	$(r, 0, \mathsf{R})$
q_1	1	$(q_2, \mathsf{Y}, \mathsf{L})$	q_3	1	$(r, 1, \mathsf{R})$
q_1	X	$(r, \mathsf{X}, \mathsf{R})$	q_3	X	$(r, \mathsf{X}, \mathsf{R})$
q_1	Y	$(q_1, \mathsf{Y}, \mathsf{R})$	q_3	Y	$(q_3, \mathsf{Y}, \mathsf{R})$
t	$*$	$(t, *, \mathsf{R})$	r	$*$	$(r, *, \mathsf{R})$

Beispiel

Wir betrachten die Schrittfunktion für eine akzeptierende Berechnung von M bei Eingabe 0011:

$$
\begin{aligned}
(s, \vdash 0011\sqcup^\infty, 0) &\xrightarrow[M]{1} (s, \vdash 0011\sqcup^\infty, 1) \xrightarrow[M]{1} (q_1, \vdash X011\sqcup^\infty, 2)\\
&\xrightarrow[M]{1} (q_1, \vdash X011\sqcup^\infty, 3) \xrightarrow[M]{1} (q_2, \vdash X0Y1\sqcup^\infty, 2)\\
&\xrightarrow[M]{1} (q_2, \vdash X0Y1\sqcup^\infty, 1) \xrightarrow[M]{1} (s, \vdash X0Y1\sqcup^\infty, 2)\\
&\xrightarrow[M]{1} (q_1, \vdash XXY1\sqcup^\infty, 3) \xrightarrow[M]{1} (q_1, \vdash XXY1\sqcup^\infty, 4)\\
&\xrightarrow[M]{1} (q_2, \vdash XXYY\sqcup^\infty, 3) \xrightarrow[M]{1} (q_2, \vdash XXYY\sqcup^\infty, 2)\\
&\xrightarrow[M]{1} (s, \vdash XXYY\sqcup^\infty, 3) \xrightarrow[M]{1} (q_3, \vdash XXYY\sqcup^\infty, 4)\\
&\xrightarrow[M]{1} (q_3, \vdash XXYY\sqcup^\infty, 5) \xrightarrow[M]{1} (t, \vdash XXYY\sqcup\sqcup^\infty, 6)
\end{aligned}
$$

Definition

eine TM M

- akzeptiert $x \in \Sigma^*$, wenn $\exists\, y, n$:

$$(s, \vdash x \sqcup^\infty, 0) \xrightarrow[M]{*} (t, y, n)$$

- verwirft $x \in \Sigma^*$, wenn $\exists\, y, n$:

$$(s, \vdash x \sqcup^\infty, 0) \xrightarrow[M]{*} (r, y, n)$$

- hält bei Eingabe x, wenn x akzeptiert oder verworfen
- hält nicht bei Eingabe x, wenn x weder akzeptiert, noch verworfen
- ist total, wenn M auf allen Eingaben hält

Definition

die Sprache einer TM M ist wie folgt definiert:

$$\mathrm{L}(M) := \{x \in \Sigma^* \mid M \text{ akzeptiert } x\}$$

Satz

Sei L eine Sprache, die von einer TM akzeptiert wird. Dann ist L rekursiv aufzählbar.

Folgerung

Sei L eine Sprache, die von einer TM akzeptiert wird, dann existiert eine Grammatik G, sodass $L = \mathrm{L}(G)$

Definition (Berechenbarkeit mit einer TM)

- Sei $M = (Q, \{\sqcap, \square\}, \{\vdash, \sqcup, \sqcap, \square\}, \vdash, \sqcup, \delta, s, t, r)$
- Eine partielle Funktion $f \colon \mathbb{N}^k \to \mathbb{N}$ heißt M-berechenbar, wenn:

$$f(n_1, \ldots, n_k) = m \quad \text{gdw.} \quad (s, \vdash \sqcap^{n_1} \square \cdots \square \sqcap^{n_k} \sqcup^{\infty}, 0) \xrightarrow[M]{*} (t, \vdash \sqcap^{m} \sqcup^{\infty}, n)$$

- Eine partielle Funktion $f \colon \mathbb{N}^k \to \mathbb{N}$ heißt berechenbar mit einer TM, wenn eine TM M über dem Alphabet $\{\sqcap, \square\}$ existiert, sodass f M-berechenbar

universität
innsbruck

Demo: Turing Machine Simulator

Frohe Feiertage & Guten Rutsch