Das Postsche Korrespondenzproblem (PKP)

Gegeben: k Paare von Wörtern $(a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k)$

$a_i, b_i \in \Sigma^*$

Frage: Gibt es eine Folge $i_1, i_2, \ldots, i_m$ von $m \geq 1$ Indizes $i_j \in \{1, 2, \ldots, k\}$ mit

$$a_{i_1} a_{i_2} a_{i_3} \ldots a_{i_m} = b_{i_1} b_{i_2} b_{i_3} \ldots b_{i_m}$$

Beispiel $(a_1, b_1) = (1, 111)$, $(a_2, b_2) = (10111, 10)$, $(a_3, b_3) = (10, 0)$

$a_2 a_1 a_1 a_3 = 10111.110$
$b_2 b_1 b_1 b_3 = 10111.1110$
} eine Lösung

Beispiel $(a_1, b_1) = (10, 101)$, $(a_2, b_2) = (011, 11)$, $(a_3, b_3) = (101, 011)$

$a_1 a_3 a_3 \ldots = 10101.101 \ldots$
$b_1 b_3 b_3 \ldots = 10101 1.011 \ldots$
keine Lösung

Beispiel $(a_1, b_1) = (0, 1)$, $(a_2, b_2) = (0, 011)$, $(a_3, b_3) = (011, 0)$

Die kürzeste Lösung hat Länge $m = 75$.

SATZ: Das PKP ist unentscheidbar.

Beweisidee: Simulation einer Turingmaschine

δ	1	B
q_0	$(q_1, 1, R)$	(q_1, B, R)
q_1	(q_0, B, L)	$(q_2, 1, R)$
q_2	(q_1, B, R)	$(q_3, 1, L)$
q_3	$(q_3, 1, N)$	(q_3, B, N)

a_i: $1q_1$, 1, $\#$, B, $q_0 1\mathrm{B}$, $1q_2$, $q_0\mathrm{BB}$,

b_i: $q_0 1$, 1, $\#$, B, $1q_1 1$, $q_1\mathrm{B}$, $\mathrm{B}q_1 1$,

a_i: $\#q_0\mathrm{B}1$, $1q_2\#$, $\#$, $\#$, $\#$ ← Abschluss

b_i: $\#q_1 1$, $q_1\#$, $\#\mathrm{B}$, $\mathrm{B}\#$, $q_F\#\#$

Bewegung über den Rand

↑ B am Rand löschen

Lösung: Folge von Konfigurationen, getrennt durch #.
Das obere Wort $(a_{i_1} a_{i_2} \dots)$ ist immer 1 Schritt voraus.

$\#q_0 1111\#\ 1q_1 111\#\ q_0 1\mathrm{B}11\#\ 1q_1\mathrm{B}11\#\ 11q_2 11\#\ \dots\ \#q_F\#\#$

$\#q_0 1111\#\ 1q_1 111\#\ q_0 1\mathrm{B}11\#\ 1q_1\mathrm{B}11\#\ \dots\ \#q_F\#\#$

Annahme: Bevor die Turingmaschine akzeptiert, löscht sie das ganze Band.

MODIFIZIERTES PKP (MPKP):

wie PKP, aber der Anfang muss a_1 / b_1 sein.
Das Paar (a_1, b_1) darf sonst nicht verwendet werden.

$a_1 = \#q_0 1111\#$ (1111: Eingabewort w)

$b_1 = \#$

$H \leq \mathrm{MPKP}$

M hält mit w ⇔ MPKP hat eine Lösung.

Schritt 2: $\mathrm{MPKP} \leq \mathrm{PKP}$

Bsp: Eingabe für MPKP: $(a_1, b_1) = (10111, 10)$, $(a_2, b_2) = (1, 111)$, $(a_3, b_3) = (10, 0)$

für PKP (zusätzlicher *)

$(a_1, b_1) = (*1*0*1*1*1*, *1*0)$, $(a_2, b_2) = (1*, *1*1*1)$, $(a_3, b_3) = (1*0*, *0)$

$a_1 a_2 a_2 a_3 = *1*0*1*1*1*1*1*1*0*\$$

$b_1 b_2 b_2 b_3 = *1*0*1*1*1*1*1*1*0*\$$

$(a_4, b_4) = (\$, *\$)$ ← zusätzliche Regel

Füge ein Symbol * vor jedem Symbol in b_i und nach jedem Symbol in a_i ein.

Nicht berechenbare Funktionen f

Beispiel $(a_1, b_1) = (0,1)$, $(a_2, b_2) = (0,011)$, $(a_3, b_3) = (011,0)$

Die kürzeste Lösung für dieses PKP hat Länge $m = 75$.

$s(k,\ell)$:= die kleinste Schranke s, sodass jedes PKP mit k Wortpaaren (a_i, b_i) über dem Alphabet $\{0,1\}$ mit Längen $|a_i|, |b_i| \leq \ell$, das lösbar ist, eine Lösung mit Länge $m \leq s$ hat.

$s(3,3) = 75$

$s(n,n)$ wächst schneller als jede berechenbare Funktion $f(n)$.

Genauer: Es gibt keine berechenbare Funktion f, sodass $f(n) \geq s(n,n)$ für alle n gilt.

(Insbesondere ist $s(n,n)$ nicht berechenbar.)

Beweis: Wenn es eine solche Funktion gäbe, dann könnte man das PKP lösen.

Eingabe: $(a_1, b_1) \ldots (a_k, b_k)$ für das PKP über $\{0,1\}$

- Bestimme $\ell := \max\{|a_i|, |b_i|\}$
- $n := \max\{k, \ell\}$
- Berechne $s := f(n)$
- Durchsuche alle potentiellen Lösungen $i_1, i_2, \ldots, i_m$ mit $m \leq s$
- Wenn keine Lösung gefunden: PKP unlösbar

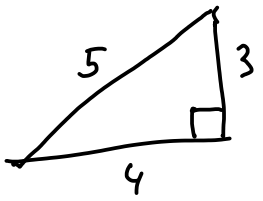
*Ähnliche Funktionen: Fleißige Biber, ...

Diophantische Gleichungen

Hat eine Polynomgleichung $f(x,y,\dots)=0$ eine Lösung in positiven ganzen Zahlen $x, y, \dots$?

Bsp. $x^2+y^2=z^2$ $\quad x^2+y^2-z^2=f(x,y,z)=0$

JA: $x=3$, $y=4$, $z=5$



Bsp. $x+y=4$
$x-y=1$ $\quad \dots f(x,y)=(x+y-4)^2+(x-y-1)^2=0$

$x=5/2$ $y=3/2$ NEIN

Bsp. $x^{100}+y^{100}=z^{100}$ NEIN (Satz von Fermat)

Lösbarkeit diophantischer Gleichungen ist unentscheidbar. (Matijasewitsch 1970)
(10. Hilbertsches Problem 1900)

- Lösbarkeit von Polynomgleichungen über den <u>reellen</u> Zahlen ist entscheidbar!
- über den rationalen Zahlen ist es noch offen.

<u>Erkennen von Schadsoftware</u>

- Wird ein Programm gewisse (verbotene) Aktionen ausführen?

UNENTSCHEIDBAR