Hovoríme, že problém je *rozhodnuteľný*, ak existuje algoritmus, ktorý pre daný „vhodný" kód ľubovoľného prípadu problému dá odpoveď pre tento prípad. Ak takýto algoritmus neexistuje, problém je *nerozhodnuteľný*.

Ak hovoríme o tom, čo to je „vhodné" kódovanie, musíme byť opatrní. Predpokladajme, že chceme „riešiť" problém zastavenia pre Turingove stroje[1]. Budeme kódovať Turingove stroje a vstupné slová ako dvojkové čísla, jedno číslo pre každú dvojicu Turingov stroj a slovo. Potiaľto je všetko v poriadku. Predpokladajme však, že si vyhradíme, že ak Turingov stroj T sa pre vstup w zastaví, potom (T, w) bude párne číslo; v opačnom prípade bude (T, w) nepárne číslo. Potom vieme „rozhodnúť" problém zastavenia tak, že sa pozrieme na posledný bit kódu prípadu.

Niečo tu nebude v poriadku. Podstata ťažkostí je jasne v hypotetickom kódovaní. Taký pojem, ako je Turingov stroj, má svoju „štandardnú" definíciu. V kap. 6 sme ho definovali ako „šesticu" $(K, \Sigma, \Gamma, \delta, q_0, F)$, kde K je množina stavov atď. Neprekvapuje nás, že dostávame čudné výsledky, ak pripustíme kódovania Turingových strojov, ktoré nemajú vzťah k „štandardnej" definícii. Definujeme preto kódovanie ako *vhodné*, ak existujú algoritmy pre preklad z kódovania do „štandardnej" definície a naspäť. Toto očividne nie je prípad kódovania Turingových strojov, o ktorom sme sa už zmienili v tomto článku.

Pochopiteľne, každý má možnosť robiť „neštandardné" definície modelov. Potom ale každá veta, ktorú dostane, bude platiť pre tieto modely, a nie pre tie, ktoré sa dajú nájsť v tejto knihe.

14.2. POSTOV KOREŠPONDENČNÝ PROBLÉM

Vieme už o jednom nerozhodnuteľnom probléme — probléme zastavenia pre Turingove stroje. Na dôkaz toho, že iné problémy sú nerozhodnuteľné, stačí ukázať, že ak by boli rozhodnuteľné, tak by tiež bol rozhodnuteľný problém zastavenia pre Turingove stroje.

[1] Tento problém je samozrejme nerozhodnuteľný

Toto sa dá urobiť priamo, je však ľahšie najprv ukázať nerozhodnuteľnosť *Postovho korešpondenčného problému*.

Postov korešpondenčný problém znie nasledujúco:

Nech Σ je konečná abeceda, nech A a B sú dva zoznamy slov zo Σ^+, pričom tieto zoznamy obsahujú rovnaký počet slov. Povedzme nech

$$A = w_1, w_2, \ldots, w_k \quad \text{a} \quad B = x_1, x_2, \ldots, x_k$$

Budeme hovoriť, že tento prípad Postovho korešpondenčného problému *má riešenie*[1], ak existuje postupnosť prirodzených čísel $i_1, i_2, \ldots, i_m$, kde $m \geqq 1$, taká, že

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

Hovoríme, že $i_1, i_2, \ldots, i_m$ je *riešením* tohto prípadu Postovho korešpondenčného problému.

Príklad 14.1. Nech $\Sigma = \{0, 1\}$. Nech A a B sú zoznamy, ktoré obsahujú po tri slová, definované takto:

i	Zoznam A w_i	Zoznam B x_i
		111
2	10111	10
3	10	0

Postov korešpondenčný problém má v tomto prípade riešenie. Nech $m = 4$, $i_1 = 2$, $i_2 = 1$, $i_3 = 1$ a $i_4 = 3$. Potom $w_2 w_1 w_1 w_3 = x_2 x_1 x_1 x_3 = 101111110$.

Príklad 14.2. Nech $\Sigma = \{0, 1\}$. Nech A a B sú zoznamy troch slov

	Zoznam A w_i	Zoznam B x_i
	10	101
2	011	
3	101	011

[1] Nezamieňajte nerozhodnuteľnosť Postovho korešpondenčného problému so skutočnosťou, že daný prípad môže „mať riešenie".

Predpokladajme, že tento prípad Postovho korešpondenčného problému má riešenie $i_1, i_2, \ldots, i_m$. Je zrejmé, že $i_1 = 1$, pretože žiadne slovo začínajúce sa s $w_2 = 011$ sa nemôže rovnať slovu, ktoré sa začína s $x_2 = 11$, a žiadne slovo začínajúce sa s $w_3 = 101$ sa nemôže rovnať slovu, ktoré sa začína s $x_3 = 011$.

Slovo zo zoznamu A napíšeme nad zodpovedajúce slovo z B. Máme teda

10
101

Ďalší výber z A sa musí začínať symbolom 1. Teda $i_2 = 1$ alebo $i_2 = 3$. Ale $i_2 = 1$ to byť nemôže, lebo žiadne slovo začínajúce sa s $w_1w_1 = 1010$ sa nemôže rovnať slovu, ktoré sa začína s $x_1x_1 = 101101$. Pre $i_2 = 3$ máme

10101
101011

Rovnakou úvahou dostávame, že i_3 3, čiže

10101101
101011011

Je zrejmé, že v tejto úvahe môžeme pokračovať donekonečna. To znamená, že neexistuje výber indexov, ktorý by umožnil, aby dĺžka slova z A „dohonila" slovo z B, čím by sa obidve slová stali totožnými.

Dokážeme nerozhodnuteľnosť Postovho korešpondenčného problému tým, že ukážeme, že ak by bol rozhodnuteľný, dokázali by sme rozhodnúť problém zastavenia pre Turingove stroje. Ukážeme najprv, že ak by bol Postov korešpondenčný problém rozhodnuteľný, bola by tiež rozhodnuteľná modifikovaná verzia Postovho korešpondenčného problému.

Modifikovaný Postov korešpondenčný problém je definovaný takto:

Nech sú dané zoznamy A a B, ktoré obsahujú k slov zo Σ^+, povedzme

$$A = w_1, w_2, \quad , w_k \quad \text{a} \quad B = x_1, x_2, \quad x_k$$

Existuje postupnosť prirodzených čísel $i_1, i_2, \quad , i_r$ taká, že

$$w_1w_{i_1}w_{i_2}\ldots w_{i_r} = x_1x_{i_1}x_{i_2}\ldots x_{i_r}$$

Rozdiel medzi modifikovaným Postovým korešpondenčným problémom a Postovým korešpondenčným problémom je ten, že v modifikovanom Postovom korešpondenčnom probléme sa hľadá riešenie, ktoré sa začína prvým slovom z každého zoznamu.

Lema 14.1. Ak by bol Postov korešpondenčný problém rozhodnuteľný, potom by bol rozhodnuteľný aj modifikovaný Postov korešpondenčný problém.

Dôkaz. Nech $A = w_1, w_2, \ldots, w_k$ a $B = x_1, x_2, \ldots, x_k$ je prípad modifikovaného Postovho korešpondenčného problému. Prevedieme tento prípad modifikovaného Postovho korešpondenčného problému na prípad Postovho korešpondenčného problému, ktorý má riešenie práve vtedy, ak má riešenie náš prípad modifikovaného Postovho korešpondenčného problému. Ak by bol Postov korešpondenčný problém rozhodnuteľný, vedeli by sme potom rozhodnúť aj modifikovaný Postov korešpondenčný problém, čím by bola lema dokázaná.

Nech Σ je najmenšia abeceda, ktorá obsahuje všetky symboly zo zoznamov A a B. Nech ¢ a \$ nepatria do Σ. Definujme dva homomorfizmy h_L a h_R na Σ^* tak, že $h_L(a) = ¢a$ a $h_R(a) = a¢$ pre všetky $a \in \Sigma$. To znamená, že h_L vkladá ¢ naľavo od každého symbolu a h_R vkladá ¢ vpravo. Definujme

$$y_1 \quad ¢h_R(w_1) \quad \text{a} \quad y_{i+} \quad h_R(w_i)$$

pre $1 \leqq i \leqq k$. Nech

$$z_1 \quad h_L(x_1) \quad \text{a} \quad z_{i+1} = h_L(x_i)$$

pre $\quad \leqq i \leqq k$. Nech

$$y_{k+2} = \$ \quad \text{a} \quad z_{k+2} = ¢\$$$

Definujme

$$C = y_1, y_2, \ldots, y_{k+2} \quad \text{a} \quad D = z_1, z_2, \ldots, z_{k+2}$$

Zoznamy C a D, zostrojené zo zoznamov A a B z príkladu 14 , sú:

Zoznam A	Zoznam B
w_i	x_i
1	111
10111	10
10	0

i	Zoznam y_i	Zoznam D z_i
	¢1¢	¢1¢1¢1
2	1¢	¢1¢1¢1
3	1¢0¢1¢1¢1¢	¢1¢0
4	1¢0¢	¢0
5	$	¢$

Zoznamy C a D predstavujú prípad Postovho korešpondenčného problému. Tvrdíme, že v tomto prípade Postov korešpondenčný problém má riešenie práve vtedy, ak prípad modifikovaného Postovho korešpondenčného problému, ktorý predstavujú zoznamy A a B, má riešenie. Na dôkaz toho pripomíname, že ak 1, i_1, i_2, ..., i_r je riešením modifikovaného Postovho korešpondenčného problému pre zoznamy A a B, potom

$$1, i_1 + 1, i_2 + 1, \ldots, i_r + 1, k + 2$$

je riešením Postovho korešpondenčného problému pre zoznamy C a D. Rovnako, ak $i_1, i_2, \ldots, i_r$ je riešením Postovho korešpondenčného problému pre zoznamy C a D, potom $i_1 = 1$ a $i_r = k + 2$, lebo y_1 a z_1 sú jediné slová s rovnakým indexom, ktoré sa začínajú rovnakým symbolom, a y_{k+2} a z_{k+2} sú jediné slová s rovnakým indexom, ktoré sa končia rovnakým symbolom. Nech j je najmenšie prirodzené číslo také, že $i_j = k + 2$. Potom $i_1, i_2, \ldots, i_j$ je tiež riešením (pretože symbol \$ sa vyskytuje iba ako posledný symbol y_{k+2} a z_{k+2}) a pre žiadne l neplatí $i_l = k + 2$, kde $1 \leqq l < j$. Je zrejmé, že $1, i_2 - 1, i_3 - 1, \ldots, i_{j-1} - 1$ je riešením modifikovaného Postovho korešpondenčného problému, a to pre zoznamy A a B.

Ak existuje algoritmus, ktorý rieši Postov korešpondenčný problém, vieme zostrojiť algoritmus, ktorý rieši modifikovaný Postov korešpondenčný problém prevedením ľubovoľnej reprezentácie modifikovaného Postovho korešpondenčného problému na prípad Postovho korešpondenčného problému, ako sme už uviedli predtým.

Veta 14.1. Postov korešpondenčný problém je nerozhodnuteľný

Dôkaz. Na základe lemy 14.1 stačí ukázať, že ak by bol modifikovaný Postov korešpondenčný problém rozhodnuteľný, potom by bol rozhodnuteľný problém zastavenia pre Turingove stroje. Pre daný Turingov stroj M a vstupné slovo w zostrojíme prípad modifikovaného Postovho korešpondenčného problému, ktorý má riešenie vtedy a len vtedy, ak sa stroj M zastaví a akceptuje vstupné slovo w.

Nech $M = (K, \Gamma, \Sigma, \delta, q_0, F)$ a nech B je prázdny symbol. Bez ujmy na všeobecnosti môžeme predpokladať, že pre každé $q \in F$ a $a \in \Sigma$ je $\delta(q, a)$ nedefinované. Konfiguráciu (q, α, i) stroja M môžeme reprezentovať reťazcom $\alpha_1 q \alpha_2$, kde $\alpha_1\alpha_2 = \alpha$ a $|\alpha_1| = i - 1$. To znamená, že q sa nachádza bezprostredne vľavo od symbolu, ktorý číta čítacia hlava stroja M. Ak q_0w, $\alpha_1q_1\beta_1$, $\alpha_2q_2\beta_2$, ..., $\alpha_kq_k\beta_k$ sú reprezentácie možnej postupnosti konfigurácií stroja M a q_k patrí do F, potom bude existovať riešenie modifikovaného Postovho korešpondenčného problému, ktorého každé slovo sa bude začínať $\#q_0w\#\alpha_1q_1\beta_1\# \ldots \#\alpha_kq_k\beta_k\#$. Pritom $\#$ je nový symbol, ktorý nepatrí ani do K ani do Γ.

Dvojice slov, ktoré vytvárajú zoznamy A a B prípadu modifikovaného Postovho korešpondenčného problému, sú formálne uvedené nižšie. Vzhľadom na to, že s výnimkou prvej dvojice, ktorá musí byť použitá prvá, počty dvojíc nie sú pre existenciu riešenia podstatné, uvádzame dvojice bez indexov.

Prvá dvojica je:

Zoznam A	Zoznam B
$\#$	$\#q_0w\#$

Zostávajúce dvojice sú zoskupené nasledujúcim spôsobom

Skupina I:

Zoznam A	Zoznam B		
X	X	pre každé $X \in I$	$\{B\}$
$\#$	$\#$		

Skupina II: Pre každé $q \in K - F$, $p \in K$ a $X, Y, Z \in$ $\{B\}$

Zoznam A	Zoznam B	
qX	Yp	ak $\delta(q, X) = (p, Y, R)$

ZqX	pZY	ak $\delta(q, X)$	(p, Y, L)
$q\#$	$Yp\#$	ak $\delta(q, B)$	(p, Y, R)
$Zq\#$	$pZY\#$	ak $\delta(q, B)$	(p, Y, L)

Skupina III: Pre každé $q \in F$ a $X, Y \in \Gamma \quad \{B\}$.

Zoznam A	Zoznam B
XqY	q
$Xq\#$	$q\#$
$\#qY$	$\#q$

Skupina IV

Zoznam A	Zoznam B	
$q\#\#$	$\#$	pre každé $q \in F$

Hovoríme, že (x, y) je *čiastočné riešenie* modifikovaného Postovho korešpondenčného problému pre zoznamy A a B, ak x je začiatočným podslovom slova y a x, y sú zreťazením zodpovedajúcich si slov zoznamov A, resp. B. Ak $xz = y$, potom z nazývame *zvyškom* čiastočného riešenia (x, y).

Predpokladajme, že z konfigurácie q_0w existuje platná postupnosť konfigurácií $\alpha_1q_1\beta_1$, $\alpha_2q_2\beta_2$, ..., $\alpha_kq_k\beta_k$, kde žiadne z q_1, q_2, ..., q_{k-1} nepatrí do F. Tvrdíme, že existuje čiastočné riešenie

$$(x, y) = (\#q_0w\#\alpha_1q_1\beta_1\#\ldots\#\alpha_{k-1}q_{k-1}\beta_{k-1}\#,\ \#q_0w\#\alpha_1q_1\beta_1\#\ldots\#\alpha_kq_k\beta_k\#)$$

Okrem toho, toto je jediné čiastočné riešenie, ktorého dlhšie slovo má rovnakú dĺžku, ako je $|y|$.

Uvedené tvrdenie sa ľahko dokáže indukciou vzhľadom na k. Pre $k = 0$ je to triviálne, pretože dvojica $(\#, \#q_0w\#)$ sa musí vybrať prvá.

Predpokladajme, že tvrdenie je splnené pre nejaké k a že q_k nepatrí do F. Ľahko sa dá ukázať, že to platí aj pre $k + 1$. Zvyšok dvojice (x, y) je $z = \alpha_kq_k\beta_k\#$. Nasledujúce dvojice treba vybrať tak, že ich slová zo zoznamu A vytvárajú z. Bez ohľadu na to, ktoré symboly sa vyskytujú napravo a naľavo od q_k, v skupine II existuje najviac jedna dvojica, ktorá umožňuje, aby čiastočné riešenie pokračovalo za q_k. Táto dvojica prirodzeným spôsobom reprezentuje

krok stroja M v konfigurácii $\alpha_kq_k\beta_k$. Ostatné symboly zo z si vynucujú výber zo skupiny I. Žiadny iný výber dvojíc neumožňuje, aby bolo slovo z zložené z prvkov zoznamu A.

Dostávame takto nové čiastočné riešenie $(y, y\alpha_{k+1}q_{k+1}\beta_{k+1}\#)$. Bezprostredne sa dá vidieť, že $\alpha_{k+1}q_{k+1}\beta_{k+1}$ je tá konfigurácia, ktorú môže stroj M dosiahnuť jediným krokom z $\alpha_kq_k\beta_k$. Neexistuje taktiež žiadne iné čiastočné riešenie, ktorého druhé slovo má dĺžku $|y\alpha_{k+1}q_{k+1}\beta_{k+1}|$.

Okrem toho, ak q_k patrí do F, ľahko sa dajú nájsť dvojice zo skupín I a III, ktoré, keď ich predchádza čiastočné riešenie (x, y) a nasleduje dvojica zo skupiny IV, dávajú riešenie modifikovaného Postovho korešpondenčného problému pre zoznamy A a B.

Ak teda stroj M, ktorý začne pracovať v konfigurácii q_0w, dosiahne koncový stav, náš prípad modifikovaného Postovho korešpondenčného problému pre zoznamy A a B má riešenie. Ak M nedosiahne koncový stav, môžu existovať čiastočné riešenia, ale slovo z B musí presiahnuť dĺžku slova z A, a teda žiadne riešenie nie je možné.

Usudzujeme teda, že prípad modifikovaného Postovho korešpondenčného problému má riešenie vtedy a len vtedy, ak sa stroj M so vstupným slovom w zastaví v koncovom stave. Keďže uvedená konštrukcia sa dá vykonať pre ľubovoľné M a w, vyplýva z toho, že ak by existoval algoritmus pre riešenie modifikovaného Postovho korešpondenčného problému, existoval by aj algoritmus pre riešenie problému zastavenia pre Turingove stroje. Problém zastavenia pre Turingove stroje je však nerozhodnuteľný. Preto modifikovaný Postov korešpondenčný problém je nerozhodnuteľný a na základe lemy 14.1 je Postov korešpondenčný problém nerozhodnuteľný.

PRÍKLAD 14.3. Nech $M = (\{q_1, q_2, q_3 \quad \{0, \quad B\}, \{0, \quad \}, \delta, q_1, \{q_3\})$. Nech δ je definovaná takto:

q_i	$\delta(q_i, 0)$	$\delta(q_i, 1)$	$\delta(q_i, B)$
q_1	$(q_2, 1, R)$	$(q_2, 0, L)$	$(q_2, 1, L)$
q_2	$(q_3, 0, L)$	$(q_1, 0, R)$	$(q_2, 0, R)$
q_3			