

# Obsah prvního svazku

## 1 Úvod

- 1.1 Přehled pojmů a struktur
  - 1.1.1 Množiny, čísla a relace
  - 1.1.2 Funkce
  - 1.1.3 Pravděpodobnost
  - 1.1.4 Grafy
- 1.2 Algebra
  - 1.2.1 Dělitelnost, prvočíselnost a základní kombinatorické vztahy
  - 1.2.2 Grupy
  - 1.2.3 Okruhy a tělesa; polynomy
  - 1.2.4 Lineární algebra
- 1.3 Boolovské funkce
  - 1.3.1 Syntax a sémantika výrokového počtu

## 2 Churchova teze

- 2.1 Turingovy stroje
  - 2.1.1 Definice Turingova stroje a intuitivní pojetí jeho výpočtu
  - 2.1.2 Konfigurace a formální definice výpočtu
  - 2.1.3 Univerzální Turingův stroj
  - 2.1.4 Přirozená čísla, grafy, formule a další konečné objekty
  - 2.1.5 Modifikace Turingových strojů, vícepáskové Turingovy stroje
  - 2.1.6 Časová a prostorová složitost výpočtu
  - 2.1.7 Dodatek — Alan M. Turing: *O vyčíslitelných číslech*
- 2.2 Částečně rekursivní funkce
  - 2.2.1 Primitivně rekursivní funkce, částečně rekursivní funkce, obecně rekursivní funkce
  - 2.2.2 Rekursivní funkce, jež není primitivně rekursivní
  - 2.2.3 Tempo růstu primitivně rekursivních funkcí
- 2.3 Věty o simulacích
  - 2.3.1 Věta o normální formě pro částečně rekursivní funkce; standardní enumerace částečně rekursivních funkcí

## 3 Algoritmická neřešitelnost a nerozhodnutelnost

- 3.1 Rekursivita, rekursivní spočetnost a Postova věta
  - 3.1.1 Částečně rekursivní funkce a rekursivně spočetné množiny; rekursivní funkce a rekursivní množiny
  - 3.1.2 Enumerovatelnost
- 3.2 Problém zastavení
- 3.3 Věta o rekursi
  - 3.3.1 Riceova věta

- 3.4 Převoditelnost, úplnost a stupně
  - 3.4.1  $m$ -převoditelnost
  - 3.4.2 1-převoditelnost
  - 3.4.3 Myhillova věta
  - 3.4.4 Cylindrifikace
  - 3.4.5  $m$ -stupně a 1-stupně
- 3.5 Programy a aritmetika
  - 3.5.1 Robinsonova aritmetika, Peanova aritmetika a fragmenty aritmetiky
  - 3.5.2 Reprezentovatelnost rekursivních množin a funkcí v aritmetice
  - 3.5.3 První Gödelova věta
  - 3.5.4 Slabá reprezentovatelnost
  - 3.5.5 Druhá Gödelova věta
  - 3.5.6 Neoddělitelnost množin
  - 3.5.7 Každé dva páry efektivně neoddělitelných rekursivně spočetných množin jsou rekursivně isomorfní
  - 3.5.8 Berryho paradox
  - 3.5.9 Interpretovatelnost
- 3.6 Turingovská převoditelnost
- 3.7 Aritmetická hierarchie
  - 3.7.1 Aritmetická klasifikace konkrétních množin
- 3.8 Postův problém
  - 3.8.1 Slabý Postův problém
  - 3.8.2 Konstrukce prosté množiny pomocí kolmogorovské složitosti
  - 3.8.3 Produktivita a kreativita: definice
  - 3.8.4 Efektivně prosté množiny
  - 3.8.5 Silný Postův problém
- 3.9 Kreativita
- 3.10 Dodatek — Alan M. Turing: *O vyčíslitelných číslech* (podruhé)



# Obsah druhého svazku

Předmluva k druhému svazku	13
<b>4 Výpočty s omezenými zdroji</b>	<b>15</b>
4.1 Algebraické algoritmy	29
4.1.1 Výpočetní čas aritmetických operací	30
4.1.2 Eukleidův algoritmus	32
4.1.3 RSA	38
4.2 Algoritmy počítající s racionálními čísly	43
4.2.1 Velikost zápisu racionálních čísel, vektorů a matic	44
4.2.2 Gaussova eliminace	46
4.3 Prvočíselnost	51
4.3.1 Krok [3]: nalezení vhodného $r$	53
4.3.2 Krok [7]: test $(x+a)^n \not\equiv_{(Z_n[x])_{x^{r-1}}} x^n + a$	55
4.3.3 Snadná implikace věty o korektnosti AKS algoritmu	56
4.3.4 Obtížná implikace věty o korektnosti AKS algoritmu	58
4.3.5 Dodatek: důkaz existence polynomu $h(x)$	65
4.4 Omezená paměť	68
4.5 Diagonalizace, konstruovatelnost funkcí a věty o hierarchii	72
4.6 Převoditelnost, $PSPACE$ -úplnost a $P$ -úplnost	78
4.6.1 $P$ -úplnost	82
4.6.2 Paralelizovatelnost	90
4.6.3 Výpočty Turingových strojů jako formule	97
4.6.4 $PSPACE$ -úplnost	98
4.6.5 Skladník	104
4.6.6 $PSPACE$ a důkazy	115
<b>5 Nedeterminismus</b>	<b>127</b>
5.1 $NP$	130
5.1.1 Prattova věta	133
5.1.2 Ještě několik příkladů množin v $NP$	137
5.2 Nedeterministický Turingův stroj	140
5.2.1 Definice a vlastnosti	141
5.2.2 Programování nedeterministických Turingových strojů	142
5.2.3 Normalizace nedeterministických Turingových strojů	143
5.2.4 Nedeterministické stroje s oraculem	146
5.3 $NP$ -úplnost	151
5.4 $co-NP$ a důkazové systémy	179
5.4.1 Důkazy a $NP$	184
5.5 Polynomiální hierarchie	185
5.5.1 Třídy $\delta_k^P, S_k^P, \Delta_k^P$	199
5.6 Postův problém v $NP$	201
5.6.1 Polynomiální turingovská redukce	202
5.6.2 Vztahy mezi redukcemi, stupně	204



5.6.3	Rekursivní indexace složitostních tříd . . . . .	208
5.6.4	Uniformní diagonalizace . . . . .	212
5.6.5	Konstrukce rekursivních indexací a aplikace uniformní diagonalizace . . . . .	217
5.6.6	Nesrovnatelné stupně; věty o hustotě . . . . .	223
5.7	Isomorfismus $NP$ -úplných množin: Bermanova-Hartmanisova hypotéza . . . . .	229
5.7.1	Polynomiální isomorfismus . . . . .	230
5.7.2	Mahaneyova věta . . . . .	238
5.8	Obvody . . . . .	246
5.9	Počty nedeterministických výpočtů . . . . .	251
5.9.1	Hlasování . . . . .	251
5.9.2	Sémantické třídy . . . . .	258
5.9.3	Pravděpodobnostní algoritmy . . . . .	261
5.9.4	Relativizace a definice přes svědky . . . . .	268
5.9.5	$BPP$ je „nízko“ v aritmetické hierarchii . . . . .	270
5.9.6	Pravděpodobnostní redukce . . . . .	275
5.9.7	Obecné pojetí počtu nedeterministických výpočtů . . . . .	285
5.9.8	Věty o kolapsu . . . . .	293
5.10	Permanent . . . . .	297
5.10.1	<b>PERMANENT</b> a $\#P$ : Valiantova věta . . . . .	298
5.10.2	<b>PERMANENT</b> a polynomiální hierarchie: Todova věta . . . . .	308
5.11	Zoo složitostních tříd . . . . .	317
5.12	Pravděpodobnostní svědci příslušnosti do množin v $NP$ . . . . .	319
5.12.1	Velké Fourierovy koeficienty . . . . .	324
5.12.2	Konstrukce $PCP$ -důkazu . . . . .	329
5.12.3	Krok 1: test na linearitu . . . . .	330
5.12.4	Čtení hodnot lineárních funkcí . . . . .	330
5.12.5	Krok 2: test na tenzorový součin . . . . .	331
5.12.6	Krok 3: splňuje $u$ systém kvadratických rovnic? . . . . .	333
5.12.7	Jak přesvědčit oponenta, že věta platí, a přitom mu neukázat důkaz . . . . .	336
5.13	$P$ versus $NP$ . . . . .	338
5.13.1	Nerelativizovatelnost důkazu $P \neq NP$ . . . . .	339
5.13.2	Nezávislost $P \neq NP$ na $PA$ . . . . .	347
5.13.3	Prostorová analogie otázky $P \stackrel{?}{=} NP$ . . . . .	356
5.13.4	Prostorová analogie otázky $NP \stackrel{?}{=} co-NP$ . . . . .	359
5.13.5	Na závěr . . . . .	363
	<b>Bibliografická poznámka</b> . . . . .	<b>373</b>
	<b>Přehled symboliky</b> . . . . .	<b>375</b>
	<b>Literatura</b> . . . . .	<b>385</b>
	<b>Rejstřík</b> . . . . .	<b>393</b>

## Obsah třetího svazku

### 6 Matijasevičova věta

- 6.1 Pelliána
- 6.2 Funkce  $\mathcal{A}(z; n)$  a  $\mathcal{B}(z; n)$
- 6.3 Diofantická reprezentace  $\mathcal{B}(z; n)$ , exponenciály a omezené obecné kvantifikace
- 6.4 Třída diofantických funkcí je uzavřená na primitivní rekursi a minimalizaci
- 6.5 Barzdiňovo lemma
- 6.6 Několik nerozhodnutelných problémů
  - 6.6.1 Goniometrické rovnice
  - 6.6.2 Diferenciální rovnice

### 7 Řešitelnost rovnic a nerovnic

- 7.1 Tarského-Mučnikův algoritmus
- 7.2 Racionální řešení
- 7.3 Lineární diofantické rovnice
- 7.4 Rovnice  $ax^2 + by = c$  a Mandersova-Adlemanova věta
- 7.5 Lineární programování
  - 7.5.1 Elipsoidy a  $E$ -norma
  - 7.5.2 Elipsoidové řezy
  - 7.5.3 Geometrie polyedrů
  - 7.5.4 Velikost zápisu řešení soustav lineárních rovnic
  - 7.5.5 Nafukovací lemma
  - 7.5.6 Elipsoidový algoritmus
  - 7.5.7 Zaokrouhlování
  - 7.5.8 Čačijanův algoritmus
  - 7.5.9 Komentář k lineárnímu programování
  - 7.5.10 Lineární programování je  $P$ -úplné
- 7.6 Celočíselné programování
  - 7.6.1 Celočíselné programování je  $NP$ -úplné
  - 7.6.2 Další výsledky o řešitelnosti rovnic; problém batohu
  - 7.6.3 Celočíselné programování v pevné dimenzi
  - 7.6.4 Komentář k celočíselnému programování

### 8 Epilog