

Obsah prvního svazku

Předmluva k prvnímu svazku	13
1 Úvod	15
1.1 Přehled pojmů a struktur	27
1.1.1 Množiny, čísla a relace	27
1.1.2 Funkce	34
1.1.3 Pravděpodobnost	40
1.1.4 Grafy	41
1.2 Algebra	45
1.2.1 Dělitelnost, prvočíselnost a základní kombinatorické vztahy	45
1.2.2 Grupy	51
1.2.3 Ohruhy a tělesa; polynomy	56
1.2.4 Lineární algebra	61
1.3 Boolovské funkce	68
1.3.1 Syntax a sémantika výrokového počtu	75
1.4 Predikátový počet	77
1.4.1 Teorie množin	83
2 Churchova teze	87
2.1 Turingovy stroje	89
2.1.1 Definice Turingova stroje a intuitivní pojetí jeho výpočtu	92
2.1.2 Konfigurace a formální definice výpočtu	98
2.1.3 Univerzální Turingův stroj	101
2.1.4 Přirozená čísla, grafy, formule a další konečné objekty	104
2.1.5 Modifikace Turingových strojů, vícepáskové Turingovy stroje	106
2.1.6 Časová a prostorová složitost výpočtu	112
2.1.7 Dodatek — Alan M. Turing: <i>O vyčíslitelných číslech</i>	114
2.2 Částečně rekursivní funkce	130
2.2.1 Primitivně rekursivní funkce, částečně rekursivní funkce, obecně rekursivní funkce	131
2.2.2 Rekursivní funkce, jež není primitivně rekursivní	140
2.2.3 Tempo růstu primitivně rekursivních funkcí	141
2.3 Věty o simulacích	146
2.3.1 Věta o normální formě pro částečně rekursivní funkce; standardní enumerace částečně rekursivních funkcí	151
3 Algoritmická neřešitelnost a nerozhodnutelnost	157
3.1 Rekursivita, rekursivní spočetnost a Postova věta	164
3.1.1 Částečně rekursivní funkce a rekursivně spočetné množiny; rekursivní funkce a rekursivní množiny	167
3.1.2 Enumerovatelnost	171
3.2 Problém zastavení	175

3.3	Věta o rekursi	176
3.3.1	Riceova věta	185
3.4	Převoditelnost, úplnost a stupně	187
3.4.1	m -převoditelnost	187
3.4.2	1-převoditelnost	190
3.4.3	Myhillova věta	192
3.4.4	Cylindrifikace	195
3.4.5	m -stupně a 1-stupně	200
3.5	Programy a aritmetika	206
3.5.1	Robinsonova aritmetika, Peanova aritmetika a fragmenty aritmetiky	208
3.5.2	Reprezentovatelnost rekursivních množin a funkcí v aritmetice	222
3.5.3	První Gödelova věta	227
3.5.4	Slabá reprezentovatelnost	236
3.5.5	Druhá Gödelova věta	241
3.5.6	Neoddělitelnost množin	246
3.5.7	Každé dva páry efektivně neoddělitelných rekursivně spočetných množin jsou rekursivně isomorfní	250
3.5.8	Berryho paradox	254
3.5.9	Interpretovatelnost	257
3.6	Turingovská převoditelnost	259
3.7	Aritmetická hierarchie	269
3.7.1	Aritmetická klasifikace konkrétních množin	278
3.8	Postův problém	287
3.8.1	Slabý Postův problém	289
3.8.2	Konstrukce prosté množiny pomocí kolmogorovské složitosti	291
3.8.3	Produktivita a kreativita: definice	293
3.8.4	Efektivně prosté množiny	295
3.8.5	Silný Postův problém	298
3.9	Kreativita	306
3.10	Dodatek — Alan M. Turing: <i>O vyčíslitelných číslech</i> (podruhé)	309

Bibliografická poznámka 317

Přehled symboliky 319

Literatura 323

Rejstřík 329

Obsah druhého svazku

4 Výpočty s omezenými zdroji

- 4.1 Algebraické algoritmy
 - 4.1.1 Výpočetní čas aritmetických operací
 - 4.1.2 Eukleidův algoritmus
 - 4.1.3 RSA
- 4.2 Algoritmy počítající s racionálními čísly
 - 4.2.1 Velikost zápisu racionálních čísel, vektorů a matic
 - 4.2.2 Gaussova eliminace
- 4.3 Prvočíselnost
 - 4.3.1 Krok [3]: nalezení vhodného r
 - 4.3.2 Krok [7]: test $(x+a)^n \not\equiv_{(Z_n[x])_{x^{r-1}}} x^n + a$
 - 4.3.3 Snadná implikace věty o korektnosti AKS algoritmu
 - 4.3.4 Obtížná implikace věty o korektnosti AKS algoritmu
 - 4.3.5 Dodatek: důkaz existence polynomu $h(x)$
- 4.4 Omezená paměť
- 4.5 Diagonalizace, konstruovatelnost funkcí a věty o hierarchii
- 4.6 Převoditelnost, **PSPACE**-úplnost a **P**-úplnost
 - 4.6.1 **P**-úplnost
 - 4.6.2 Paralelizovatelnost
 - 4.6.3 Výpočty Turingových strojů jako formule
 - 4.6.4 **PSPACE**-úplnost
 - 4.6.5 Skladník
 - 4.6.6 **PSPACE** a důkazy

5 Nedeterminismus

- 5.1 **NP**
 - 5.1.1 Prattova věta
 - 5.1.2 Ještě několik příkladů množin v **NP**
- 5.2 Nedeterministický Turingův stroj
 - 5.2.1 Definice a vlastnosti
 - 5.2.2 Programování nedeterministických Turingových strojů
 - 5.2.3 Normalizace nedeterministických Turingových strojů
 - 5.2.4 Nedeterministické stroje s oraculem
- 5.3 **NP**-úplnost
- 5.4 **co-NP** a důkazové systémy
 - 5.4.1 Důkazy a **NP**
- 5.5 Polynomiální hierarchie
 - 5.5.1 Třídy δ_k^P , S_k^P , Δ_k^P
- 5.6 Postův problém v **NP**
 - 5.6.1 Polynomiální turingovská redukce
 - 5.6.2 Vztahy mezi redukcemi, stupně

- 5.6.3 Rekursivní indexace složitostních tříd
- 5.6.4 Uniformní diagonalizace
- 5.6.5 Konstrukce rekursivních indexací a aplikace uniformní diagonalizace
- 5.6.6 Nesrovnatelné stupně; věty o hustotě
- 5.7 Isomorfismus NP -úplných množin: Bermanova-Hartmanisova hypotéza
 - 5.7.1 Polynomiální isomorfismus
 - 5.7.2 Mahaneyova věta
- 5.8 Obvody
- 5.9 Počty nedeterministických výpočtů
 - 5.9.1 Hlasování
 - 5.9.2 Sémantické třídy
 - 5.9.3 Pravděpodobnostní algoritmy
 - 5.9.4 Relativizace a definice přes svědky
 - 5.9.5 BPP je „nízko“ v aritmetické hierarchii
 - 5.9.6 Pravděpodobnostní redukce
 - 5.9.7 Obecné pojetí počtu nedeterministických výpočtů
 - 5.9.8 Věty o kolapsu
- 5.10 Permanent
 - 5.10.1 **PERMANENT** a $\#P$: Valiantova věta
 - 5.10.2 **PERMANENT** a polynomiální hierarchie: Todaova věta
- 5.11 ZOO složitostních tříd
- 5.12 Pravděpodobnostní svědci příslušnosti do množin NP
 - 5.12.1 Velké Fourierovy koeficienty
 - 5.12.2 Konstrukce PCP -důkazu
 - 5.12.3 Krok 1: test na linearitu
 - 5.12.4 Čtení hodnot lineárních funkcí
 - 5.12.5 Krok 2: test na tenzorový součin
 - 5.12.6 Krok 3: splňuje u systém kvadratických rovnic?
 - 5.12.7 Jak přesvědčit oponenta, že věta platí, a přitom mu neukázat důkaz
- 5.13 P versus NP
 - 5.13.1 Nerelativizovatelnost důkazu $P \neq NP$
 - 5.13.2 Nezávislost $P \neq NP$ na PA
 - 5.13.3 Prostorová analogie otázky $P \stackrel{?}{=} NP$
 - 5.13.4 Prostorová analogie otázky $NP \stackrel{?}{=} co-NP$
 - 5.13.5 Na závěr

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