

Obsah druhého svazku

Předmluva k druhému svazku	13
4 Výpočty s omezenými zdroji	15
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 $(x+a)^n \neq (z_n[x])_{x^{r-1}} x^n + a$	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
5 Nedeterminismus	127
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 δ_k^P , S_k^P , Δ_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	PERMANENT a $\#P$: Valiantova věta	298
5.10.2	PERMANENT a polynomiální hierarchie: Todaova 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
	Bibliografická poznámka	373
	Přehled symboliky	375
	Literatura	385
	Rejstřík	393