

Předmluva	i
Kapitola 0. Úvod	1
0.1. Co je teoretická informatika	1
0.2. Pojem algoritmu	1
0.3. Správnost algoritmu	2
0.4. Složitost algoritmu	2
0.5. Základní datové struktury	5
0.6. Příklad	6
0.7. Literatura	11
0.8. Cvičení	12
Kapitola 1. Vyhledávání v textu	13
1.1. Základní pojmy z teorie jazyků	13
1.2. Naivní algoritmus	14
1.3. Metoda Aho-Corasickové	15
1.3.1. Vyhledávací automat	16
1.3.2. Vlastnosti vyhledávacího automatu	17
1.3.3. Interpret vyhledávacího automatu	17
1.3.4. Konstrukce vyhledávacího automatu (překladač)	20
1.4. Literatura	23
1.5. Cvičení	23
Kapitola 2. Verifikace algoritmů	25
2.1. Vývojové diagramy a Floydova metoda	25
2.1.1. Výpočet podle vývojového diagramu	25
2.1.2. Parciální a totální správnost algoritmu	27
2.1.3. Důkaz parciální správnosti	28
2.1.4. Důkaz konečnosti výpočtu	29
2.2. Strukturované algoritmy a Hoareova logika	30
2.3. Literatura	32
2.4. Cvičení	33
Kapitola 3. Dosažitelnost v grafech a paralelní algoritmy	35
3.1. Základní pojmy z teorie grafů	35
3.2. Datové struktury pro reprezentaci grafů	35
3.3. Výpočet dosažitelných vrcholů	36
3.4. Systematické prohledávání grafů	38
3.5. Výpočetní model RAM	38
3.5.1. Operační paměť a instrukce	39
3.5.2. Jednotková a logaritmická cena instrukce	43
3.6. Rekurzivní řešení dosažitelnosti	48
3.7. Převod rekurze na iteraci	49
3.8. Umocňování boolských matic	51
3.9. Paralelní výpočty	52

3.9.1. Paralelní RAM	53
3.9.2. Paralelní umocňování boolských matic	53
3.9.3. Složitost paralelních výpočtů	54
3.10. Literatura	55
3.11. Cvičení	55
Kapitola 4. Divide et impera	57
4.1. Obecné řešení rekurentních vztahů	57
4.2. Hledání v setříděném poli	60
4.3. Násobení binárních čísel	60
4.4. Násobení matic	61
4.5. Jiný typ rekurentních vztahů	63
4.6. Důkaz správnosti rekurzivních výpočtů	64
4.7. Literatura	64
4.8. Cvičení	64
Kapitola 5. Třídění a kombinační obvody	67
5.1. Třídění slučováním (Mergesort)	67
5.2. Kombinační obvody	69
5.3. Třídící sítě	73
5.3.1. Konstrukce třídící sítě	74
5.3.2. Složitost třídění	77
5.4. Literatura	80
5.5. Cvičení	81
Kapitola 6. Převoditelnost problémů	84
6.1. Třídy složitosti problémů	84
6.2. NP-úplné problémy	85
6.2.1. Problém SAT	85
6.2.2. Problém kliky	87
6.3. Relativní složitost a převoditelnost problémů	87
6.4. Další NP-úplné problémy	89
6.5. Řešení NP-úplných úloh	90
6.6. Literatura	90
6.7. Cvičení	90
Kapitola 7. Aritmetika a kryptografické protokoly	92
7.1. Základní pojmy z teorie čísel	92
7.1.1. Dělitelnost, Euklidův algoritmus	92
7.1.2. Kongruence	94
7.1.3. Čínská věta o zbytcích	95
7.2. Házení mincí po telefonu	97
7.3. Další kryptografické triky	98
7.3.1. Komutující šifry a telefonický poker	98
7.3.2. Diffie-Hellmanovy páry a veřejné kryptografické systémy	99
7.3.3. Šifrování založené na problému batohu	100

7.3.4. Šifra RSA	101
7.4. Bezpečnost šifrování	102
7.5. Literatura	102
7.6. Cvičení	103
Kapitola 8. Distribuované algoritmy a volba koordinátora	104
8.1. Komunikace v kruhové síti	104
8.1.1. Řešení s jednosměrnou komunikací	105
8.1.2. Řešení s obousměrnou komunikací	107
8.2. Literatura	110
8.3. Cvičení	110
Kapitola 9. Pravděpodobnost a algoritmy	112
9.1. Základy teorie pravděpodobnosti	112
9.2. Očekávaná složitost algoritmů	114
9.2.1. Přičítání jedničky k binárnímu číslu	114
9.2.2. Hašování	116
9.2.3. Quicksort	118
9.3. Randomizované algoritmy	120
9.3.1. Randomizovaný Quicksort	120
9.3.2. Testování prvočíselnosti	121
9.3.3. Třídy složitosti randomizovaných algoritmů	122
9.4. Náhodné generátory	122
9.5. Literatura	123
9.6. Cvičení	123