Tartalomjegyzék

Előszó **1**

1. Számítási modellek **5**
1.1. Véges automata 6
1.2. A Turing-gép 9
1.3. A RAM-gép 18
1.4. Boole-függvények és logikai hálózatok 23

2. Algoritmikus eldönthetőség **31**
2.1. Eldönthető és felsorolható nyelvek 32
2.2. Egyéb algoritmikusan eldönthetetlen problémák 36
2.3. Kiszámíthatóság a logikában 43
2.3.1. Gödel nemteljességi tétele 43
2.3.2. Elsőrendű logika 45

3. Tár és idő **51**
3.1. Polinomiális idő 52
3.2. Egyéb bonyolultsági osztályok 58
3.3. Általános tételek a tár- és időbonyolultságról 62

4. Nemdeterminisztikus algoritmusok **71**
4.1. Nemdeterminisztikus Turing-gépek 71
4.2. Nemdeterminisztikus algoritmusok bonyolultsága 73
4.3. Példák NP-beli nyelvekre 78
4.4. NP-teljesség 84
4.5. További NP-teljes problémák 89

5. Randomizált algoritmusok **99**
5.1. Polinomazonosság ellenőrzése 99
5.2. Prímtesztelés 102
5.3. Randomizált bonyolultsági osztályok 106

6. Információs bonyolultság **111**
6.1. Információs bonyolultság 111
6.2. Önkorlátozó információs bonyolultság 116
6.3. A véletlen sorozat fogalma 119
6.4. Kolmogorov-bonyolultság, entrópia és kódolás 121

7. Pszeudovéletlen számok **127**
7.1. Klasszikus módszerek 128
7.2. A pszeudovéletlenszám-generátor fogalma 130
7.3. Egyirányú függvények 134
7.4. Egyirányú függvény jelöltek 138
7.4.1. Diszkrét négyzetgyökök 139

8. Döntési fák **143**
8.1. Döntési fákat használó algoritmusok 143
8.2. Nemdeterminisztikus döntési fák 148
8.3. Alsó korlátok döntési fák mélységére 151

9. Algebrai számítások **159**
9.1. Algebrai számítási modellek 159
9.2. Szorzás 161
9.2.1. Nagy számokon végzett aritmetikai műveletek 161
9.2.2. Mátrixok szorzása 163
9.2.3. Mátrixok invertálása 165
9.2.4. Polinomok szorzása 166
9.2.5. A diszkrét Fourier-transzformált 168
9.3. Algebrai bonyolultságelmélet 170
9.3.1. Négyzetösszegek kiszámításának bonyolultsága 170
9.3.2. Polinomok kiértékelése 171
9.3.3. Képletbonyolultság és hálózati bonyolultság 174

10. Párhuzamos algoritmusok **177**
10.1. Párhuzamos RAM-gép 177
10.2. Az NC osztály 182

11. A kommunikáció bonyolultsága **187**
11.1. A kommunikációs mátrix és a protokoll-fa 188
11.2. Néhány protokoll 193
11.3. Nemdeterminisztikus kommunikációs bonyolultság 194
11.4. Randomizált protokollok 198

12. A bonyolultság alkalmazása: kriptográfia **201**
12.1. A klasszikus probléma 201

12.2. Egy egyszerű bonyolultságelméleti modell 202
12.3. Nyilvános kulcsú kriptográfia 203
12.4. A Rivest-Shamir-Adleman kód (RSA kód) 204

13. Hálózatok bonyolultsága **209**
13.1. Alsó korlát a TÖBBSÉG-re 210
13.2. Monoton hálózatok 213

14. Interaktív bizonyítások **215**
14.1. Hogyan tároljuk az utolsó lépést sakkban? 215
14.2. Hogyan ellenőrizzük a jelszót – anélkül, hogy tudnánk? . . 217
14.3. Hogy használjuk a jelszavunkat – anélkül, hogy elmondanánk? 217
14.4. Hogyan bizonyítsunk nemlétezést? 219
14.5. Hogyan győződjünk meg egy bizonyítás helyességéről – annak ismerete nélkül? 221
14.6. Hogyan bíráljunk exponenciálisan hosszú cikkeket? 222
14.7. Közelíthetőség 224

Irodalom **227**