

Ülesanded

Ü1.1. Millised järgnevatest väidetest on tõesed? Põhjenda!

- (a) $2^{n+\log n} = O(2^n)$;
- (b) $2^{n+\log n} = O(2^{1.01n})$;
- (c) $2^{n+\sin n} = O(2^n)$.

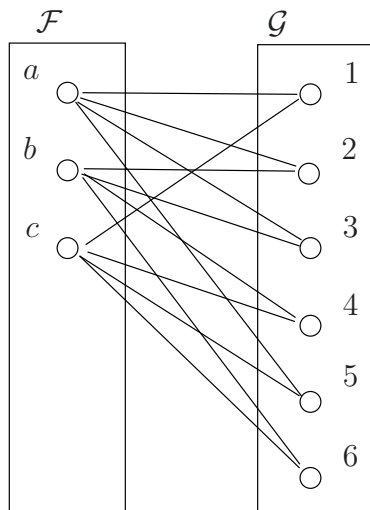
Ü1.2. Kas $\mathbf{ZPP} \subseteq \mathbf{BPP}$? Põhjenda!

Ü1.3. Olgu $f: \{0, 1\}^n \rightarrow \{0, 1\}^n$ mingi $S(n)$ -ühesuunaline funktsioon. Näita, et siis leiduvad $S(n)$ -ühesuunalised funktsioonid g_1 ja g_2 tüübiga $\{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$, nii et funktsioon

$$(g_1 \times g_2)(x) = g_1(x) \mid g_2(x)$$

ei ole ühesuunaline, st leidub vastane tööajaga $O(n)$ ja edukusega 1.

Ü1.4. Kas järgneval kahealuselisel graafil alustega \mathcal{F} ja \mathcal{G} on $(0, 0, \frac{1}{2})$ -pöördlaiendus? Nagu jooniselt näha, on selles graafis $N = 2$.



Lahendused

Ül.1. a) $2^{n+\log n} \neq O(2^n)$, sest $2^{n+\log n} = n \cdot 2^n$ ja n kasvab kiiremini mis tahes konstandist.

b) $2^{n+\log n} = O(2^{1.01n})$, sest $2^{1.01n} = 2^{0.01n} \cdot 2^n$ ja $2^{0.01n}$ kasvab kiiremini kui n . Saab näidata, et kui $n \geq 1000$, siis $2^{0.01n} \geq n$.

c) $2^{n+\sin n} = O(2^n)$, sest $2^{n+\sin n} \leq 2^{n+1} \leq 2 \cdot 2^n$.

Ül.2. Et $\mathbf{ZPP} \subseteq \mathbf{RP}$, siis leidub stohhastiline Turingi masin N , nii et iga sisendi $x \in \{0, 1\}^*$ korral:

1) Kui $x \in L$, siis $\Pr[N(x) = 1] > \frac{1}{2}$;

2) Kui $x \notin L$, siis $\Pr[N(x) = 1] = 0$.

Moodustades uue stohhastilise algoritmi N' järgmiselt: $N'(x)$ kutsub kaks korda välja $N(x)$ ja väljastab 1 parajasti siis kui vähemalt ühel katsel saadi $N(x) = 1$. Vastasel korral $N'(x) = 0$. On lihtne näha, et N' on \mathbf{BPP} algoritm vea tõenäosusega $\frac{1}{4}$.

Ül.3. Defineerime g_1 ja g_2 järgmiselt:

$$\begin{aligned}g_1(x) &= f(x_{\{1\dots n\}}) | x_{\{n+1\dots 2n\}} \\g_2(x) &= x_{\{1\dots n\}} | f(x_{\{n+1\dots 2n\}})\end{aligned}$$

On selge, et g_1 ja g_2 on $S(n)$ -ühesuunalised, kuid funktsiooni $g_1 \times g_2$ saab pöörata lineaarses ajas.

Ül.4. Joonisel kujutatud graafil on tõepoolest $(0, 0, \frac{1}{2})$ -pöördlaiendus, sest iga alamhulk $G \subseteq \mathcal{G}$ tõenäosusmõõduga $\Pr[Y \in G] \geq 0 + \frac{1}{2}$ on vähemalt kolmeelemendiline. Et igal tipul $x \in \mathcal{F}$ on täpselt 4 naabrit, siis vähemalt üks naaber peab olema hulgas G (sest hulgas \mathcal{G} on 6 elementi). Seega, tõenäosusega vähemalt $\frac{1}{4} = \frac{2}{N}$ satub juhuslikult valitud naaber hulka G . Seetõttu võib alati võtta $F = \mathcal{F}$.