

Ülesanded

Ül.1. Näita, et $n! \neq O(2^{18n})$ ja $n! = O(2^{n^2})$.

Ül.2. Olgu $f_n: \{0, 1\}^n \rightarrow \{0, 1\}^n$ mingi $2^{\sqrt{2n}}$ -ühesuunaline funktsioon ja olgu

$$g_n(x) = \begin{cases} x & \text{kui } n < 8, \\ f_8(x_{\{1..8\}}) \| x_{\{9..n\}} & \text{kui } n \geq 8. \end{cases}$$

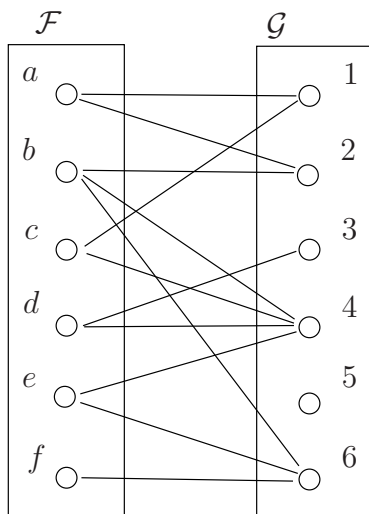
Kas $g_n: \{0, 1\}^n \rightarrow \{0, 1\}^n$ on n^2 -ühesuunaline?

Ül.3. Olgu $f_n: \{0, 1\}^n \rightarrow \{0, 1\}^n$ mingi $2^{\sqrt{2n}}$ -ühesuunaline funktsioon ja olgu

$$h_n(x) = f_{\frac{n}{2}}(x_{\{1..\frac{n}{2}\}}) \| x_{\{\frac{n}{2}+1..n\}},$$

kus n on paarisarv. Kas $h_n: \{0, 1\}^n \rightarrow \{0, 1\}^n$ on $2^{\sqrt{n}}$ -ühesuunaline?

Ül.4. Kas järgneval kahealuselisel graafil alustega \mathcal{F} ja \mathcal{G} on $(\frac{1}{3}, \frac{1}{2})$ -laiendus?



Lahendused

Ül.1. Seose $n! = O(2^{n^2})$ näitamiseks kasutame seost $n \leq 2^{n-1}$, mis kehtib iga $n > 0$ korral. Sellest seosest tulenevalt

$$n! \leq 2^0 \cdot 2^1 \cdot \dots \cdot 2^{n-1} = 2^{1+2+3+\dots+(n-1)} = 2^{\frac{n(n-1)}{2}} \leq 2^{n^2} .$$

$n! \neq O(2^{18n})$ järeldeb piirväärtusest $\lim_{n \rightarrow \infty} \frac{2^{18n}}{n!} = 0$, sest kui $n > 2^{19}$, siis

$$\frac{2^{18(n+1)}}{(n+1)!} = \frac{2^{18}}{n+1} \cdot \frac{2^{18n}}{n!} < \frac{1}{2} \cdot \frac{2^{18n}}{n!} .$$

Seega leidub n nii et $\frac{2^{18n}}{n!} < \frac{1}{c}$, millest tuleneb võrratus $n! > c \cdot 2^{18n}$.

Ül.2. Olgu A vastane, mis sisendi $y \in \{0, 1\}^n$ korral väljastab y , kui $n < 8$ ja kui $n \geq 8$, siis tegutseb järgmiselt:

- Leiab $x_{\{1..8\}}$, nii et $y_{\{1..8\}} = f_8(x_{\{1..8\}})$, milleks kulub $O(1)$ sammu.
- Kopeerib bitid $x_{\{9..n\}} := y_{\{9..n\}}$, milleks kulub $O(n)$ sammu.
- Väljastab x .

Vastase A tööaeg on seega $O(n)$ ja ta pöörab funktsiooni g_n edukusega 1. Seega on tema aeg-edukus suhe samuti $O(n)$, mis piisavalt suurte n väärtuste korral on selgelt väiksem kui n^2 . Seega ei saa g olla n^2 -turvaline.

Ül.3. Olgu A vastane tööajaga $t(m)$, mis pöörab funktsiooni h_m edukusega

$$\delta(m) = \Pr[x \leftarrow \{0, 1\}^m, x' \leftarrow A(h_m(x)): h_m(x') = h_m(x)] .$$

Defineerime vastase A' , mis sisendi $y \in \{0, 1\}^n$ korral teeb järgmist:

- Genereerib juhuslikult $x' \leftarrow \{0, 1\}^n$.
- Leiab $x \leftarrow A(y \| x')$ (kus $y \| x' \in \{0, 1\}^{2n}$ ja seega $m = 2n$).
- Väljastab $x_{\{1..n\}}$.

Vastase A' tööaeg on $t(2n)$ ja edukus $\delta(2n)$. Seega, eeldades et f_n on $2^{\sqrt{2n}}$ -ühesuunaline, saame $\frac{t(2n)}{\delta(2n)} \geq 2^{\sqrt{2n}}$ (iga n korral!), millest tuleneb $\frac{t(m)}{\delta(m)} \geq 2^{\sqrt{m}}$ iga paarisarvu m korral. Oleme näidanud, et iga h_m -i pöörava vastase A aeg-edukus suhe on vähemalt $2^{\sqrt{m}}$, millest järeldebki, et h_n on $2^{\sqrt{n}}$ -turvaline.

Ül.4. $(\frac{1}{3}, \frac{1}{2})$ -laiendus puudub, sest $\frac{|\{e, f\}|}{|\mathcal{F}|} = \frac{1}{3}$, kuid $\frac{|E(\{e, f\})|}{|\mathcal{G}|} = \frac{1}{3} < 1 - \frac{1}{2}$.