

## Ülesanded

**Ü1.1.** Näita, et kui kompositsioonis  $f \circ g$  (kus  $f, g: \{0, 1\}^n \rightarrow \{0, 1\}^n$ ) on üks funktsioonidest ühesuunaline ja teine bijektiivne, siis  $f \circ g$  on ka ühesuunaline, kusjuures reduktsioon on lineaarne.

**Ü1.2.** Olgu  $f_n: \{0, 1\}^n \rightarrow \{0, 1\}^n$  mingi  $2^{\sqrt{2n}}$ -ühesuunaline funktsioon ja olgu

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

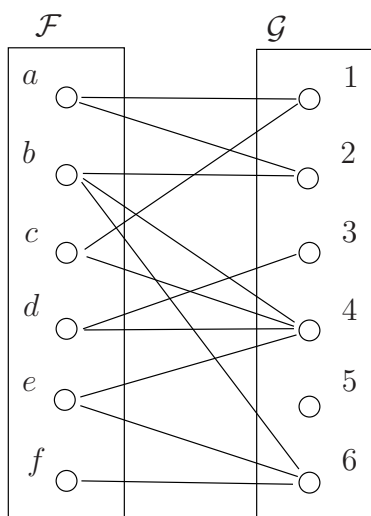
Kas  $g_n: \{0, 1\}^n \rightarrow \{0, 1\}^n$  on  $n^2$ -ühesuunaline?

**Ü1.3.** 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?

**Ü1.4.** Kas järgneval kahealuselisel graafil alustega  $\mathcal{F}$  ja  $\mathcal{G}$  on  $(\frac{1}{3}, \frac{1}{2})$ -laiendus?



**Ü1.5.** Näita, et kui leiduvad  $(S(n)-)$  ühesuunalised funktsioonid tüüpi  $\{0, 1\}^n \rightarrow \{0, 1\}^n$ , siis leidub ka ühesuunaline funktsioon  $f: \{0, 1\}^n \rightarrow \{0, 1\}^n$ , nii et  $f \circ f$  ei ole ühesuunaline (st on kergesti pööratav).

## Lahendused

**Ül.1.** Kui  $f$  on bijektiivne ja  $A$  on vastane edukusega

$$\delta = \Pr[X \leftarrow \{0, 1\}^n, X' \leftarrow A(f(g(x))): f(g(X')) = f(g(X))] ,$$

siis vastane  $A'$ , mis sisendi  $Y = g(X)$  korral väljastab  $X' = A(f(Y))$  pöörab funktsiooni  $g$  edukusega  $\delta$ , sest kui  $f(g(X')) = f(g(X))$ , siis ( $f$  bijektiivsuse tõttu)  $g(X') = g(X)$  ja seega  $A'$  pöörab edukalt funktsiooni  $g$ .

Kui  $g$  on bijektiivne ja  $A$  on vastane edukusega

$$\delta = \Pr[X \leftarrow \{0, 1\}^n, X' \leftarrow A(f(g(x))): f(g(X')) = f(g(X))] ,$$

siis vastane  $A'$ , mis sisendi  $Z = f(Y)$  korral väljastab  $A'(Z) = g(A(Z))$ , pöörab funktsiooni  $f$  edukusega  $\delta$ . Tõepoolest, kui  $X$  on ühtlase jaotusega, siis ka  $Y = g(X)$  on ühtlase jaotusega (sest  $g$  on bijektiivne). Seega kui  $Y$  on ühtlaselt ja juhuslikult valitud, siis tõenäosusega vähemalt  $\delta$  väljastab  $A(Z)$  argumendi  $X'$ , mille korral kehtib  $f(g(X')) = f(g(X))$ . Siit aga järeldub, et vastane  $A'$  väljastab  $Y' = g(X')$ , mille korral  $f(Y') = f(g(X')) = f(g(X)) = f(Y)$  ja seega pöörab  $A'$  edukalt funktsiooni  $f$ .

**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  $x_{\{1\dots n\}}$ .

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 järeldubki, 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  $\frac{|E(\{e, f\})|}{|\mathcal{G}|} = \frac{1}{3} < 1 - \frac{1}{2}$ .

**Ül.5.** Eeldada, et leidub ühesuunaline funktsioon  $\phi: \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$ , defineerime  $f$  nii et iga  $X_1, X_2 \in \{0, 1\}^{n/2}$  korral:

$$f(X_1 X_2) := (0^{n/2}, \phi(X_1)) . \quad (1)$$

On selge, et funktsioon  $f$  on ühesuunaline, sest kui  $A$  oleks vastane edukusega:

$$\delta = \Pr[X_1, X_2 \leftarrow \{0, 1\}^{n/2}, (X'_1 X'_2) \leftarrow A(f(X_1 X_2)): f(X_1 X_2) = f(X'_1 X'_2)] ,$$

siis vastane  $A'$ , mis sisendi  $Y = \phi(X)$  korral arvutab  $X'_1 X'_2 \leftarrow A(0^{n/2}, Y)$ , pöörab funktsiooni  $\phi$  edukusega  $\delta$ . Seega, kui  $\phi$  on ühesuunaline, siis ka  $f$  on ühesuunaline. Teiselt poolt,  $f \circ f$  on konstantne funktsioon ja seega lihtsasti pööratav.