

Ülesanded

Ü1.1. Olgu $g_1: \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$ ja $g_2: \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$ pseudojuhuarvude generaatorid, mis on defineeritud valemitega $g_1(X) = X \| z \odot X$ ($z \in \{0, 1\}^n$ mingi avalik konstant) ja $g_2(X) = X \| h(X)$, kus \odot tähistab skalaarkorrutist mooduliga 2 ja $h(X)$ tähistab 1-bitide arvu (n -bitises) argumentis X mooduliga 2. Kas g_1 ja g_2 on head pseudojuhuarvude generaatorid? Leida võimalikult efektiivsed eristavad vastased A_1 ja A_2 .

Ü1.2. Olgu $g_1: \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$ ja $g_2: \{0, 1\}^{n+1} \rightarrow \{0, 1\}^{n+2}$ pseudojuhuarvude generaatorid, kusjuures $g_2(T)$ on (iga $T \in \{0, 1\}^{n+1}$ korral) arvutatav ajaga $t_2(n)$. Näita, et kui g_1 ja g_2 on eristamatud, siis ka nende kompositsioon $g_2 \circ g_1$ on eristamatu. Täpsemini, kui leidub kompositsiooni eristav vastane A tööajaga $t(n)$ ja edukusega

$$\delta(n) = | \Pr_X[A(g_2(g_1(X))) = 1] - \Pr_Z[A(Z) = 1] |, \quad (1)$$

kus $X \in \{0, 1\}^n$ ja $Z \in \{0, 1\}^{n+2}$ on ühtlase jaotusega sõltumatud juhuslikud suurused; siis leidub vähemalt üks järgmistest vastastest:

- (a) generaatorit g_1 eristav vastane tööajaga $t(n) + t_2(n)$ ja edukusega $\frac{\delta(n)}{2}$
- (b) generaatorit g_2 eristav vastane tööajaga $t(n)$ ja edukusega $\frac{\delta(n)}{2}$.

Ü1.3. Olgu $g: \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}$ mingi pseudojuhuarvude generaator. Ütleme, et g on *eristamatu kahe katsega*, kui iga vastase A korral tööajaga $T(n)$ ja edukusega

$$\delta(n) = | \Pr[A(g(X_1), g(X_2)) = 1] - \Pr[A(Z_1, Z_2) = 1] |$$

kehtib $\frac{T(n)}{\delta(n)} \geq S(n)$, kus $X_1, X_2 \leftarrow \{0, 1\}^n$ ja $Z_1, Z_2 \leftarrow \{0, 1\}^{\ell(n)}$ on sõltumatud ühtlase jaotusega juhuslikud suurused. Tõesta, et kui g on eristamatu tavalises mõttes, siis on ta eristamatu ka kahe katsega, kusjuures reduktsioon on seejuures lineaarne.

Lahendused

Ü1.1. Generaatorit g_1 murdev vastane A_1 töötab järgmiselt. Sisendi $Y \in \{0, 1\}^{n+1} = Y' \| b$ korral väljastab 1 kui $z \odot Y' = b$ ja 0 vastupidisel juhul. Kui sisend Y on ühtlaselt valitud juhuslik suurus $Z \leftarrow \{0, 1\}^{n+1}$, siis $\Pr[A_1(Z) =$

$1] = \frac{1}{2}$. Kui aga sisendiks Y on võetud generaatori g_1 väljund $g_1(X)$, siis $\Pr[A_1(g_1(X)) = 1] = 1$. Seega on vastase A_1 edukus

$$|\Pr[A_1(g_1(X)) = 1] - \Pr[A_1(Z) = 1]| = \frac{1}{2},$$

mis on väga suur (kaugel kaduvväiksest suuruselt!). Seetõttu tuleb järeldada, et generaator g_1 on väga nõrk. Analooilise arutelu saab läbi viia ka generaatori g_2 korral.

Ü1.2. Olgu $T \leftarrow \{0, 1\}^{n+1}$ ühtlase jaotusega juhuslik suurus. Liites ja lahutades vastase A edukuse avaldises (1) absoluutväärtuse märgi all tõenäosuse $\Pr_T[A(g_2(T))=1]$, ja defineerides $A_1(y) := A(g_2(y))$ (iga $y \in \{0, 1\}^{n+1}$ korral) saame

$$\begin{aligned} \delta(n) &= |\Pr_X[A(g_2g_1(X))=1] - \Pr_T[A(g_2(T))=1] + \Pr_T[A(g_2(T))=1] - \Pr_Z[A(Z)=1]| \\ &= |\Pr_X[A_1(g_1(X))=1] - \Pr_T[A_1(T)=1] + \Pr_T[A(g_2(T))=1] - \Pr_Z[A(Z)=1]| \\ &\leq \underbrace{|\Pr_X[A_1(g_1(X))=1] - \Pr_T[A_1(T)=1]|}_{\delta_1(n)} + \underbrace{|\Pr_T[A(g_2(T))=1] - \Pr_Z[A(Z)=1]|}_{\delta_2(n)} \\ &= \delta_1(n) + \delta_2(n). \end{aligned}$$

Seega kas $\delta_1(n) \geq \frac{\delta(n)}{2}$, millest järelduks, et vastane $A_1 = A \circ g_2$ tööajaga $t(n) + t_2(n)$ eristab generaatori g_1 väljundit edukusega vähemalt $\frac{\delta(n)}{2}$; või siis $\delta_2(n) \geq \frac{\delta(n)}{2}$, millest järelduks, et vastane A tööajaga $t(n)$ eristab generaatori g_2 väljundit edukusega vähemalt $\frac{\delta(n)}{2}$.

Ü1.3. Defineerime eristava vastase A' järgmiselt. Sisendi $Y \in \{0, 1\}^{\ell(n)}$ korral vastane A' :

1. Genereerib ühtlase jaotusega $Z' \leftarrow \{0, 1\}^{\ell(n)}$ ja $X' \leftarrow \{0, 1\}^n$.
2. Valib juhuslikult ja ühtlaselt $i \leftarrow \{1, 2\}$ ja:
 - (a) Kui $i = 1$, siis tagastab $A(Y, Z')$.
 - (b) Kui $i = 2$, siis tagastab $A(g(X'), Y)$.

Tõenäosus ühtöaselt valitud $X, X_1, X_2 \leftarrow \{0, 1\}^n$ ja $Z, Z_1, Z_2 \leftarrow \{0, 1\}^{\ell}$ korral

$$\Pr_X[A'(g(X_2)) = 1] = \frac{1}{2} \Pr_{Z_2, X_1}[A(g(X_1), Z_2) = 1] + \frac{1}{2} \Pr_{X_1, X_2}[A(g(X_1), g(X_2)) = 1]$$

ja

$$\Pr_Z[A'(Z) = 1] = \frac{1}{2} \Pr_{Z_1, Z_2}[A(Z_1, Z_2) = 1] + \frac{1}{2} \Pr_{Z_2, X_1}[A(g(X_1), Z_2) = 1] .$$

Seega on A' eristab g väljundit edukusega:

$$\begin{aligned} \delta'(n) &= | \Pr_X[A'(g(X_2)) = 1] - \Pr_Z[A'(Z) = 1] | \\ &= \frac{1}{2} | \Pr[A(g(X_1), g(X_2)) = 1] - \Pr[A(Z_1, Z_2) = 1] | \\ &= \frac{\delta(n)}{2} . \end{aligned}$$