

Ü1.1: Tõesta, et $n \cdot \log_2 n = O(n^2)$, $n! = 1 \cdot 2 \cdot \dots \cdot n \neq O(2^n)$ ja $n! = O(2^{n^2})$.

Ü1.2: Olgu meil keel L , mis koosneb bitijadadest $b_1 b_2 \dots b_m$ (kus m võib olla erinev iga sõna korral), nii et leiduvad $x_1, \dots, x_m \in \{0, 1\}$, nii et

$$\begin{aligned} b_1 x_1 &\oplus b_2 x_2 \oplus \dots \oplus b_m x_m = 1 \\ b_{m+1} x_1 &\oplus b_{m+2} x_2 \oplus \dots \oplus b_{2m} x_m = 1 \\ &\dots \\ b_{m(m-1)+1} x_1 &\oplus b_{m(m-1)+2} x_2 \oplus \dots \oplus b_{m^2} x_m = 1 . \end{aligned}$$

Kas $L \in \mathbf{NP}$? Kas $L \in \mathbf{P}$? Põhjenda vastuseid!

Ü1.3: Mängus visatakse 120 täringut. Kui tulemuseks on vähemalt 40 kuute, siis on mängija võitnud ja saab auhinnaks 1000 EEK. Kui piisaval arvul kuutesid ei tule, siis mängija kaotab 1001 EEK. Kas mäng on kasulik? Põhjenda!

Ü1.4: Leida funktsioon $f: \mathbb{N} \rightarrow \mathbb{N}$ (kus $\mathbb{N} = \{0, 1, 2, \dots\}$), mis on polünoomiaalse kasvukiirusega (st. $f(n) = n^{O(1)}$), kuid mis ei ole polünoomiaalne parameeter.

Ü1.5: Tõesta, et leidub ajas $O(n)$ arvutatav funktsioon $f: \{0, 1\}^n \rightarrow \{0, 1\}^n$, nii et iga vastase A korral:

$$\Pr[x \leftarrow \mathcal{U}\{0, 1\}^n, x' \leftarrow A(f_n(x)): x' = x] \leq 2^{-n} .$$

Ü1.6: On vaja koostada 2^{80} -turvaline e-valimissüsteem, kasutades ehituskivina ühesuunalisi funktsioone $f: \{0, 1\}^n \rightarrow \{0, 1\}^n$, kus $n \leq 160$ (oletame, et suurema n korral praktilisi funktsioone ei teata!). Teadlased on välja pakkunud kavandatavale e-valimissüsteemile järgmise tulemusega turvatõestuse:

- Kui A on vastane tööajaga t , mis edukusega δ murrab kavandatava valimissüsteemi, siis leidub vastane A' , mis töötab ajaga $t' = 4t$ ja murrab vastava ühesuunalise funktsiooni tõenäosusega $\delta' = \frac{t}{\delta^2}$.

Kas sellest turvatõestusest on ülesande eelduste kohaselt abi kavandatava e-valimissüsteemi turvalisuse põhjendamisel? Miks?