

Üldjuht "klassikalise" definitsiooni korral

Näitame, et ühesuunalise funktsiooni *klassikalise* definitsioonist lähtuvalt leiduvad ühesuunalised funktsioonid $f: \{0, 1\}^n \rightarrow \{0, 1\}^n$ ja $g: \{0, 1\}^n \rightarrow \{0, 1\}^n$, nii et nende kompositsioon $f \circ g$ ei ole ühesuunaline. Selleks tuleb aga eeldada, et leidub vähemalt üks ühesuunaline funktsioon $\phi: \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$. Võtame $g = f$ ja defineerime f nii et iga $X_1, X_2 \in \{0, 1\}^{n/2}$ korral:

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

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 $Y = \pi(X)$ korral arvutab $X'_1 X'_2 \leftarrow A(0^{n/2}, Y)$, pöörab funktsiooni π edukusega δ . Seega, kui ϕ on ühesuunaline, siis ka f on ühesuunaline. Teiselt poolt, $f \circ f$ on konstantne funktsioon ja ei ole seega mingil juhul ühesuunaline.

Mõned erijuhud

Selgub, et kui üks funktsioonidest f ja g on bijektiivne, siis kompositsioon on ühesuunaline (isegi siis kui nimetatud bijektsioon ise ei ole ühesuunaline).

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 δ , 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 δ . 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 δ 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 .

Ühesuunalisus väljundi suhtes

Kui ühesuunalisus oleks defineeritud aga nii, et juhusliku sisendi asemel valitakse juhuslik väljund (nn. *ühesuunalisus väljundi suhtes*), siis selgub et ühesuunaliste (väljundi suhtes) funktsioonide kompositsioon on ise samuti ühesuunaline väljundi suhtes.

Def. (Ühesuunalisus väljundi suhtes): Funktsiooni $f: \{0, 1\}^n \rightarrow \{0, 1\}^n$ nimetatakse $S(n)$ -*ühesuunaliseks väljundi suhtes*, kui iga vastase A korral tööajaga t ja edukusega

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

kehtib võrratus $\frac{t}{\delta} \geq S(n)$.

Kui f ja g on ühesuunalised väljundi suhtes ja A on vastane tööajaga t ja edukusega

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

siis vastane A' , kes sisendi Y korral väljastab $g(A(Y))$ pöörab funktsiooni f edukusega δ . Seega ka kompositsioon $f \circ g$ on ühesuunaline väljundi suhtes.