

Pseudojuhuarvud

Ahto Buldas

Pseudojuhuslikud jadad: intuitiivne definitsioon

Millal on jada

0 1 1 0 0 1 1 1 0 0 1 0 0 1 ...

(pseudo) juhuslik?

Intuitsioon 1: Jada on pseudojuhuslik, kui tema järgmise biti ennustamise tõenäosus ei erine kuigi palju $\frac{1}{2}$ -st.

Intuitsioon 2: Jada on pseudojuhuslik, kui ta on eristamatu päris-juhuslikust jadast.

Tõenäosusjaotused ja operatsioonid nendega

Tõenäosusjaotuseks \mathcal{D} lõplikul hulgal \mathcal{X} nimetatakse funktsiooni $\mathcal{X} \rightarrow [0, 1]$, mis igale elemendile $x \in \mathcal{X}$ seab vastavusse tema tõenäosuse $\mathcal{D}(x)$. On eeldatud, et $\sum_{x \in \mathcal{X}} \mathcal{D}(x) = 1$. Kui $\mathcal{D}(x) = \frac{1}{|\mathcal{X}|}$ iga $x \in \mathcal{X}$ korral, siis jaotust \mathcal{D} nimetatakse *ühtlaseks* hulgal \mathcal{X} ja tähistatakse $\mathcal{U}_{\mathcal{X}}$.

Olgu $\mathcal{X}_1, \dots, \mathcal{X}_m$ mingid hulgad ja $\mathcal{D}_1, \dots, \mathcal{D}_m$ tõenäosusjaotused nendel hulkadel. Olgu $\mathcal{X}_1 \times \dots \times \mathcal{X}_m \xrightarrow{f} \mathcal{Y}$ mingi funktsioon. Jaotused $\mathcal{X}_1, \dots, \mathcal{X}_m$ genereerivad loomulikult viisil ka jaotuse $\mathcal{D} = f(\mathcal{D}_1, \dots, \mathcal{D}_m)$ hulgal \mathcal{Y} , mis on iga $y \in \mathcal{Y}$ korral defineeritud kui

$$\mathcal{D}(y) = \sum_{(x_1, \dots, x_m) \in f^{-1}(y)} \mathcal{D}_1(x_1) \cdot \dots \cdot \mathcal{D}_m(x_m).$$

Eeldame, et kui $f^{-1}(y) = \emptyset$, siis $\mathcal{D}(y) = 0$. Jaotuse $\mathcal{D} = f(\mathcal{D}_1, \dots, \mathcal{D}_m)$ olemust on lihtne mõista, kui esitada see juhusliku katse abil järgmiselt:

$$\mathcal{D}(y) = \Pr[X_1 \stackrel{\mathcal{D}_1}{\leftarrow} \mathcal{X}_1, \dots, X_m \stackrel{\mathcal{D}_m}{\leftarrow} \mathcal{X}_m : f(X_1, \dots, X_m) = y].$$

Kui $\mathcal{X} \times \mathcal{X} \xrightarrow{\oplus} \mathcal{X}$ on rühma tehe hulgal \mathcal{X} , siis mis tahes jaotuse \mathcal{D} korral hulgal \mathcal{X} kehtib

$$\mathcal{U} \oplus \mathcal{D} = \mathcal{U},$$

kus $\mathcal{U} = \mathcal{U}_{\mathcal{X}}$. Kui $\mathcal{X} \xrightarrow{f} \mathcal{Y}$ on injektsioon, siis $f(\mathcal{U}_{\mathcal{X}}) = \mathcal{U}_{f(\mathcal{X})}$. Erijuhul kui f on bijektsioon saame $f(\mathcal{U}_{\mathcal{X}}) = \mathcal{U}_{\mathcal{Y}}$. Jaotusi \mathcal{D}_1 ja \mathcal{D}_2 hulkadel \mathcal{X}_1 ja \mathcal{X}_2 nimetatakse *ekvivalentseteks* ja kirjutatakse $\mathcal{D}_1 \cong \mathcal{D}_2$, kui leidub bijektsioon $\mathcal{X}_1 \xrightarrow{f} \mathcal{X}_2$, nii et $\mathcal{D}_1(x) = \mathcal{D}_2(f(x))$ iga $x \in \mathcal{X}_1$ korral.

Näide: Kui $\mathcal{X} = \{0, 1\}^n$ ja \oplus tähistab liitmist bitikaupa (mod 2), siis \oplus on rühmaoperatsioon ja järelikult $\mathcal{U} \oplus \mathcal{D} = \mathcal{U}$ iga jaotuse \mathcal{D} korral hulgal \mathcal{X} .

Pseudojuhuarvude definitsioon

Definitsioon: Olgu $g: \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}$ mingi \mathbf{P} -pere, kus $\ell(n) > n$. Peret g nimetatakse **$\mathbf{S}(n)$ -eristamatuks** juhuarvude generaatoriks, kui iga vastase A korral tööajaga $T(n)$ ja edukusega

$$\delta(n) = \left| \Pr_{X \leftarrow \{0,1\}^n} [A(g(X)) = 1] - \Pr_{Z \leftarrow \{0,1\}^{\ell(n)}} [A(Z) = 1] \right|$$

kehtib võrratus $T(n)/\delta(n) \geq \mathbf{S}(n)$.

Definitsioon: \mathbf{P} -peret $g: \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}$ nimetatakse **$\mathbf{S}(n)$ -prognoosimatuks** kui iga vastase A korral tööajaga $T(n)$ ja edukusega

$$\delta(n) = \Pr_{\mathcal{I}, X} [A(\mathcal{I}, g(X)_{\{1, \dots, \mathcal{I}-1\}}) = g(X)_{\mathcal{I}}] - \frac{1}{2},$$

kehtib võrratus $T(n)/\delta(n) \geq \mathbf{S}(n)$. Siin $\mathcal{I} \leftarrow \{1, \dots, \ell(n)\}$ ja $X \leftarrow \{0, 1\}^n$. Tähistuse $g(X)_{\{1, \dots, \mathcal{I}-1\}}$ all mõeldakse väljundi $g(X)$ esimest $\mathcal{I} - 1$ bitti.

Eristatamatus \Rightarrow Prognoosimatus

Teoreem: Iga eristamatu generaator on prognoosimatu. Reduktsioon on lineaarne.

Tõestus: Olgu A vastane tööajaga $T(n)$ ja edukusega

$$\delta(n) = \Pr_{\mathcal{I}, X} [A(\mathcal{I}, g(X)_{\{1, \dots, \mathcal{I}-1\}}) = g(X)_{\mathcal{I}}] - \frac{1}{2}.$$

Defineerime oraakliga vastase S^A , mis sisendi $Y \in \{0, 1\}^{\ell(n)}$ korral teeb järgmist:

- Genereerib juhuslikult $\mathcal{I} \leftarrow \{1, \dots, \ell(n)\}$.
- Kontrollib, kas $A(\mathcal{I}, Y_{1, \dots, \mathcal{I}-1}) = Y_{\mathcal{I}}$.
- Kui jah, siis tagastab 1, muidu 0.

Kui S^A , sisendis on $Y = g(X)$ juhuslikult valitud $X \leftarrow \{0, 1\}^n$ korral, siis tõenäosus, et $S^A(Y) = 1$ on

$$\Pr_{\mathcal{I}, X} [A(\mathcal{I}, g(X)_{\{1, \dots, \mathcal{I}-1\}}) = g(X)_{\mathcal{I}}] = \delta(n) + \frac{1}{2}.$$

Kui aga sisendis on $Z \leftarrow \{0, 1\}^{\ell(n)}$, siis tõenäosus, et $S^A(Z) = 1$ on fikseeritud \mathcal{I} väärtuse korral

$$\begin{aligned} \Pr_Z [A(\mathcal{I}, Z) = 1 \mid \mathcal{I}] &= \Pr_{Z \leftarrow \{0, 1\}^{\ell(n)}} [A(\mathcal{I}, Y_{1, \dots, \mathcal{I}-1}) = Y_{\mathcal{I}}] \\ &= \Pr_{Y \leftarrow \{0, 1\}^{\mathcal{I}-1}, B \leftarrow \{0, 1\}} [A(\mathcal{I}, Y) \oplus B = 0] \\ &= \Pr_{B \leftarrow \{0, 1\}} [B = 0] = \frac{1}{2}. \end{aligned}$$

Eelviimane võrdusmärk tuleneb asjaolust, et \oplus on rühmatehe ja kui \mathcal{D} on suuruse $A(Y)$ jaotus ja \mathcal{U} suuruse $B = Y_{\mathcal{I}}$ jaotus, siis $\mathcal{D} \oplus \mathcal{U} = \mathcal{U}$. Seega

ka

$$\Pr_{Z \leftarrow \{0,1\}^{\ell(n)}} [S^A(Z) = 1] = \frac{1}{2}.$$

Seega tõenäosuste vahe

$$\begin{aligned} \delta'(n) &= \left| \Pr_{X \leftarrow \{0,1\}^n} [S^A(g(X))] - \Pr_{Z \leftarrow \{0,1\}^{\ell(n)}} [S^A(Z)] \right| \\ &= \delta(n) + \frac{1}{2} - \frac{1}{2} = \delta(n). \end{aligned}$$

Et ka S^A tööaeg on $T'(n)$ enam-vähem sama, mis $T(n)$, siis on ka S^A aeg-edukus suhe sama, mis vastasel A . Reduktsioon on seega lineaarne.

Prognoosimatus \Rightarrow eristmatus

Teoreem: Iga prognoosimatu generaator on eristamatu. Reduktsioon on lineaarne.

Tõestus: Olgu A vastane tööajaga $T(n)$, mis eristab jaotust $g(X)$ edukusega $\delta(n)$. Tähistagu \mathcal{U}_n ühtlast jaotust hulgal $\{0, 1\}^n$ ja \mathcal{U}_ℓ ühtlast jaotust hulgal $\{0, 1\}^\ell$, kus lühiduse mõttes tähistame $\ell = \ell(n)$. Vaatleme järgmist jaotuste jada:

$$\begin{aligned}
 \mathcal{D}_0 &= \mathcal{U}_\ell \\
 \mathcal{D}_1 &= g(\mathcal{U}_n)_1 \parallel (\mathcal{U}_\ell)_{\{2, \dots, \ell\}} \\
 &\dots \\
 \mathcal{D}_i &= g(\mathcal{U}_n)_{\{1, \dots, i\}} \parallel (\mathcal{U}_\ell)_{\{i+1, \dots, \ell\}} \\
 &\dots \\
 \mathcal{D}_{\ell(n)} &= g(\mathcal{U}_n).
 \end{aligned}$$

Olgu $\delta_i = \Pr_{Y \leftarrow \{0,1\}^\ell} [A(Y) = 1]$. Üldisust kitsendamata võib eeldada,

et $\delta_0 > \delta_\ell$. Sisuliselt see tähendab, et A väljastab eelistatult 1, kui ta “arvab”, et sisendiks on juhuslikult ühtlaselt genereeritud jada. Seega, definitsioonidest tulenevalt

$$\delta_0 - \delta_\ell = \delta(n).$$

Et $(\delta_0 - \delta_1) + (\delta_1 - \delta_2) + \dots + (\delta_{\ell-1} - \delta_\ell) = \delta(n)$, siis järelikult

$$\mathbf{E}_{\mathcal{I} \leftarrow \{1, \dots, \ell\}} [\delta_{\mathcal{I}-1} - \delta_{\mathcal{I}}] = \frac{\delta(n)}{\ell}.$$

Defineerime S^A , mis sisendite $\mathcal{I} \in \{1, \dots, \ell\}$ ja $Y = g(X)_{\{1, \dots, i-1\}} \in \{0, 1\}^{i-1}$ (kus $\mathcal{I} \leftarrow \{1, \dots, \ell\}$ ja $X \leftarrow \{0, 1\}^n$) korral käitub järgmiselt:

- Genereerib juhuslikult $Z \leftarrow \{0, 1\}^\ell$.
- Arvutab $z = A(Y_{\{1, \dots, \mathcal{I}-1\}} \| Z_{\{\mathcal{I}, \dots, \ell\}})$.
- Väljastab $z \oplus Z_{\mathcal{I}}$.

Seega, kui A väljastab 0, st “arvab”, et jada on (osaliselt) genereeritud juhuarvude generaatori g poolt, siis väljastab S^A biti $0 \oplus Z_{\mathcal{I}} = Z_{\mathcal{I}}$. Vastasel juhul väljastab S^A vastupidise biti, st $1 \oplus Z_{\mathcal{I}}$.

Edaspidises arutelus kasutame z osade sõltumatust rõhutavat tähistust: $z' = z_{1\dots\mathcal{I}}$ ja $z'' = z_{\mathcal{I}+1\dots\ell}$ ning $z = z' \| z'' = z'_1 \dots z'_{\mathcal{I}} z''_{\mathcal{I}+1} \dots z''_{\ell}$.

Olgu $\Omega \leftarrow \{0, 1\}^{T(n)}$ vastase $A = A_{\Omega}$ juhuslike mündivisete string. Olgu A_{ω} deterministlik vastane, mis on saadud vastasest A_{Ω} juhuarvude stringi Ω fikseerimisel väärtuseks ω . Siis tõenäosus $\delta'_{\mathcal{I}}$, et S^A prognoosib järgmise biti õigesti (fikseeritud \mathcal{I} korral) on võrdne:

$$\begin{aligned}
\delta'_I &= \Pr_{X,Z,\Omega} \left[\begin{array}{l} (A_\Omega(g(X)_{\{1\dots I-1\}} \| Z_{\{I\dots\ell\}}) = 0 \text{ ja } g(X)_I = Z_I) \text{ või} \\ (A_\Omega(g(X)_{\{1\dots I-1\}} \| Z_{\{I\dots\ell\}}) = 1 \text{ ja } g(X)_I \neq Z_I) \end{array} \right] \\
&= \sum_{x,z,\omega} \Pr[x, z, \omega] \left[\begin{array}{l} (1 - [A_\omega(g(x)_{\{1\dots I-1\}} \| z_{\{I\dots\ell\}}) = 1]) \cdot [g(x)_I = z_I] + \\ + ([A_\omega(g(x)_{\{1\dots I-1\}} \| z_{\{I\dots\ell\}}) = 1] \cdot (1 - [g(x)_I = z_I])) \end{array} \right] \\
&= \sum_{x,z,\omega} \Pr[x, z, \omega] \cdot [g(x)_I = z_I] + \sum_{x,z,\omega} \Pr[x, z, \omega] \cdot [A_\omega(g(x)_{\{1\dots I-1\}} \| z_{\{I\dots\ell\}}) = 1] \\
&\quad - 2 \cdot \sum_{x,z,\omega} \Pr[x, z, \omega] \cdot [A_\omega(g(x)_{\{1\dots I-1\}} \| z_{\{I\dots\ell\}}) = 1] \cdot [g(x)_I = z_I] \\
&= \frac{1}{2} + \delta_{I-1} - 2 \sum_{x,\omega} \Pr[x, \omega] \sum_{z',z''} \Pr[z'] \cdot \Pr[z''] [A_\omega(g(x)_{\{1\dots I\}} \| z''_{\{I+1\dots\ell\}}) = 1] \cdot [g(x)_I = z'_I] \\
&= \frac{1}{2} + \delta_{I-1} - 2 \sum_{x,\omega} \Pr[x, \omega] \underbrace{\sum_{z'} \Pr[z'] [g(x)_I = z'_I]}_{\frac{1}{2}} \cdot \sum_{z''} \Pr[z''] [A_\omega(g(x)_{\{1\dots I\}} \| z''_{\{I+1\dots\ell\}}) = 1] \\
&= \frac{1}{2} + \delta_{I-1} - \sum_{x,\omega} \Pr[x, \omega] \cdot \sum_{z''} \Pr[z''] [A_\omega(g(x)_{\{1\dots I\}} \| z''_{\{I+1\dots\ell\}}) = 1] \\
&= \frac{1}{2} + \delta_{I-1} - \delta_I,
\end{aligned}$$

kus $[A_\omega(y) = b]$ tähendab nn. Iversoni sümbolit, st $[A_\omega(y) = b] = 1$ kui $A_\omega(y) = b$ ja $[A_\omega(y) = b] = 0$ kui $A_\omega(y) \neq b$.

Et \mathcal{I} valiti juhuslikult ja ühtlaselt hulgast $\{1, \dots, \ell\}$, siis on S^A õnnestumise tõenäosus

$$\mathbf{E}_{\mathcal{I} \leftarrow \{1, \dots, \ell\}} \left[\frac{1}{2} + \delta_{\mathcal{I}-1} - \delta_{\mathcal{I}} \right] = \frac{1}{2} + \frac{\delta(n)}{\ell}.$$

Et A ja S^A tööajad on umbes samad ja $\ell(n) = n^{\mathcal{O}(1)}$, siis reduktsioon on tõepoolest lineaarne.

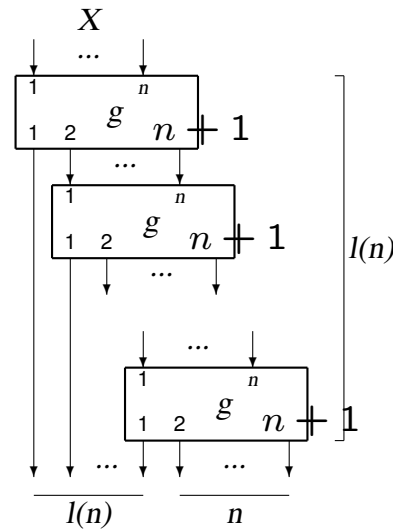
Väljundi venitamine

Juhuarvude generaatori sisendi pikkuse n ja väljundi pikkuse $\ell(n)$ kohta eeldatakse ainult seda, et $\ell(n) > n$. Seega võib juhtuda, et generaatori väljund on vaid ühe biti võrra pikem sisendist, st pikkusega $n+1$. Praktikas on aga enamasti vaja generaatoreid, mis “venitavad” rohkem. Järgnevalt näitame, kuidas generaatorist veniturparameetriga 1 konstrueerida generaator venitusparameetriga $\ell(n)$, kus $\ell(n)$ on suvaline polünomiaalne parameeter.

Olgu $g: \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$ mingi eristamatu juhuarvude generaator. Defineerime induktiivselt funktsioonid $g^0, \dots, g^{\ell(n)}$, kus $\{0, 1\}^n \xrightarrow{g^i} \{0, 1\}^{n+i}$

ja iga $X \in \{0, 1\}^n$ korral:

$$\begin{aligned}
 g^0(X) &= X \\
 g^1(X) &= g(X) \\
 g^{i+1}(X) &= g(X)_1 \| g^i(g(X)_{\{2, \dots, n+1\}})
 \end{aligned}$$



Teoreem: Kui g on eristamatu, siis ka $g^{\ell(n)}$ on eristamatu. Reduktsioon on lineaarne.

Tõestus: Olgu $X \leftarrow \{0, 1\}^n$ ja $Z \leftarrow \{0, 1\}^{n+\ell(n)}$. Olgu A vastane tööajaga $T(n)$, mis eristab generaatorit $g^{\ell(n)}$ edukusega

$$\delta(n) = \Pr_X[A(g^{\ell(n)}(X)) = 1] - \Pr_Z[A(Z) = 1]$$

Näitame, et leidub oraakliga vastane S^A tööajaga $T'(n) \approx T(n)$, mis eristab generaatorit g edukusega $\delta'(n) = \delta(n)/\ell(n)$.

Enne kui asume vastase S^A kirjeldamisele, defineerime tõenäosusjaotuste

jada $\mathcal{D}_0, \dots, \mathcal{D}_{\ell(n)}$, nii et

$$\mathcal{D}_0 = \mathcal{U}_{\ell(n)} \| \mathcal{U}_n$$

$$\mathcal{D}_1 = \mathcal{U}_{\ell(n)-1} \| g^1(\mathcal{U}_n)$$

...

$$\mathcal{D}_i = \mathcal{U}_{\ell(n)-i} \| g^i(\mathcal{U}_n)$$

...

$$\mathcal{D}_{\ell(n)} = g^{\ell(n)}(\mathcal{U}_n) .$$

Olgu $\delta_i = \Pr_{Y \leftarrow \{0,1\}^{n+\ell(n)}} [A(Y) = 1]$. Siis

$$\delta(n) = \delta_{\ell} - \delta_0 = (\delta_{\ell} - \delta_{\ell-1}) + (\delta_{\ell-1} - \delta_{\ell-2}) + \dots + (\delta_2 - \delta_1) + (\delta_1 - \delta_0) ,$$

kus $\ell = \ell(n)$, mistõttu

$$\mathbf{E}_{\mathcal{I} \leftarrow \{1, \dots, \ell(n)\}} [\delta_{\mathcal{I}} - \delta_{\mathcal{I}-1}] = \frac{\delta(n)}{\ell(n)} .$$

Vastane S^A sisendi $Y \in \{0, 1\}^{n+1}$ korral käitub järgmiselt:

- $\mathcal{I} \leftarrow \{1, \dots, \ell(n)\}$;
- $Z \leftarrow \{0, 1\}^{\ell(n) - \mathcal{I}}$;
- Väljasta $A(Z \| Y_1 \| g^{\mathcal{I}-1}(Y_{\{2, \dots, n+1\}}))$.

Olgu \mathcal{I} fikseeritud. Kui $Y \leftarrow \{0, 1\}^{n+1}$, siis S^A väljastab 1 tõenäosusega $\delta_{\mathcal{I}-1}$, sest oraakli A sisendi jaotus on $\mathcal{U}_{\ell(n) - (\mathcal{I}-1)} \| g^{\mathcal{I}-1}(\mathcal{U}_n) = \mathcal{D}_{\mathcal{I}-1}$. Kui aga $Y = g(X)$, kus $X \leftarrow \{0, 1\}^n$, siis tõenäosus, et S^A väljastab 1, on $\delta_{\mathcal{I}}$, sest siis oraakli A sisend on

$$\begin{aligned} Z \| Y_1 \| g^{\mathcal{I}-1}(Y_{\{2, \dots, n+1\}}) &= Z \| g(X)_1 \| g^{\mathcal{I}-1}(g(X)_{\{2, \dots, n+1\}}) \\ &= Z \| g^{\mathcal{I}}(X) \ , \end{aligned}$$

mistõttu A sisendi jaotus on $\mathcal{U}_{\ell(n) - \mathcal{I}} \| g^{\mathcal{I}}(\mathcal{U}_n) = \mathcal{D}_{\mathcal{I}}$. Seega, vastase S^A

edukus on

$$\begin{aligned}\delta'(n) &= \Pr_X[S^A(g(X)) = 1] - \Pr_Z[S^A(Z) = 1] \\ &= \mathbf{E}_{\mathcal{I}}[\delta_{\mathcal{I}}] - \mathbf{E}_{\mathcal{I}}[\delta_{\mathcal{I}-1}] = \mathbf{E}_{\mathcal{I}}[\delta_{\mathcal{I}} - \delta_{\mathcal{I}-1}] \\ &= \frac{\delta(n)}{\ell(n)} .\end{aligned}$$

Derandomiseerimine

Turvaliste juhuarvude generaatorite olemasolu lubab tööestada huvitavaid tulemusi tööenäosuslike ja deterministlike keerukusklasside omavahelistest seostest. Näitena toome ära ühe lihtsaima tulemuse, mis põhineb eelkirjeldatud venituskonstruktsioonil.

Definitsioon: Juhuarvude generaator $g: \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}$ on **turvaline mitteühtlases polünomiaalses mudelis**, kui iga polünomiaalse masina A ja polünomiaalse pikkusega nõuannete jada $a = (a_n)_{n \in \mathbb{N}}$ korral:

$$| \Pr[A(g(X), a_n) = 1] - \Pr[A(Z, a_n) = 1] | = n^{-\omega(1)},$$

kus $X \leftarrow \{0, 1\}^n$ ja $Z \leftarrow \{0, 1\}^{\ell(n)}$ on ühtlase jaotusega sõltumatud juhuslikud suurused.

Teoreem: Kui leiduvad mitteühtlases polünomiaalses mudelis turvalised juhuarvude generaatorid, siis

$$\mathbf{BPP} \subseteq \bigcap_{\gamma > 0} \mathbf{DTIME}(2^{n^\gamma}) ,$$

kus $\mathbf{DTIME}(f(n))$ tähendab kõigi $O(f(n))$ -ajas (deterministliku Turingi masinaga) tuvastatavate keelte klassi.

Tõestus: Olgu $L \in \mathbf{BPP}$. Vastavalt definitsioonile leidub Turingi masin M tööajaga $t(n) = n^{O(1)}$ nii et iga n ja $x \in \{0, 1\}^n$ korral:

$$\begin{aligned} x \in L &\Rightarrow \Pr[M(x, Z) = 1] > \frac{3}{4} \\ x \notin L &\Rightarrow \Pr[M(x, Z) = 1] < \frac{1}{4} , \end{aligned}$$

kus $Z \leftarrow \{0, 1\}^{t(n)}$.

Olgu $\gamma > 0$ mingi konstant, $\epsilon = 0.9\gamma$ ja $g_m: \{0, 1\}^m \rightarrow \{0, 1\}^{t(m^{\frac{1}{\epsilon}})}$ mingi mitteühtlases polünoomiaalses mudelis turvaline juhuarvude generaator.

Asendame ehtsa juhuarvu Z generaatori g sobiva pikkusega väljundiga. Võtame $m = n^\epsilon$ ja $K \leftarrow \{0, 1\}^{n^\epsilon}$. Ütleme, et $x \in \{0, 1\}^n$ on *halb*, kui:

- $x \in L$ ja $\Pr[M(x, g_m(K)) = 1] \leq \frac{1}{2}$, või
- $x \notin L$ ja $\Pr[M(x, g_m(K)) = 1] > \frac{1}{2}$,

st x on halb kui tõenäosus $p(x) = \Pr[M(x, g_m(K)) = 1]$ ei peegelda õigesti tõeväärtust $[x \in L]$.

Kui oleks olemas lõpmata palju halbu sisendeid x , siis leiduks ka lõpmatult paljude n -de korral sisend x_n nii et:

$$\left| \Pr_Z[M(x_n, Z) = 1] - \Pr_K[M(x_n, g(K)) = 1] \right| \geq \frac{1}{4},$$

mis oleks vastuolus generaatori g turvalisusega. Järelikult eksisteerib vaid lõplik hulk $\mathcal{L} = \{x_1, \dots, x_\ell\}$ halbu sisendeid.

Seega saab defineerida järgmise deterministliku masina P , mis sisendi $x \in \{0, 1\}^n$ korral toimib järgmiselt:

- Kui $x \in \mathcal{L}$, siis P väljastab $[x \in L]$ (vastus sisaldub P programmis).
- Võtab $m = \lceil n^\epsilon \rceil$.
- Arvutab tõenäosuse $p(x) = \Pr[M(x, g_m(K)) = 1]$ kasutades valemit:

$$p(x) = \frac{1}{m} \sum_{k \in \{0,1\}^m} M(x, g(k)) .$$

- Kui $p(x) > \frac{1}{2}$, siis P väljastab 1, kui $p(x) \leq \frac{1}{2}$, siis P väljastab 0.

On selge, et $P(x) = [x \in L]$ kõikide sisendite x korral ja P töötab ajas $O(t(n) \cdot 2^{n^\epsilon}) = O(2^{n^\epsilon + \log_2 t(n)}) = O(2^{n^\gamma})$.

Kokkuvõte

Õppisime ehitama pseudojuhuarvude generaatoreid

$$g: \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}$$

suvalise polünoomi $\ell(n)$ korral ... eeldusel, et on olemas turvaline pseudojuhuarvude generaator

$$g: \{0, 1\}^n \rightarrow \{0, 1\}^{n+1} .$$

Vastuse küsimusele, kuidas konstrueerida $g: \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$ ühesuunalistest funktsioonidest, annab järgmine loeng.