Pseudojuhuslikkus. Generaatorid. Funktsioonid

Sven Laur

19. veebruar - 16.märts

Tänapäeval saab ainult küberneetika koos informatsiooniteooria ülimate võimalustega teha uute statistiliste meetodite abil hetkega sarvekandjateks kõik peokülalised ja snoobid...

Salvador Dalí

1 Sissejuhatus ja motivatisioon

20. sajandil on arenenud kolm juhuslikkuse teooriat: Shannon'i informatsiooni teooria, Kolmogorovi keerukusteooria ja pseudojuhuslikkuse teooria. Esimesed kaks teoooriat vaatavad juhuslikust ontoloogilisest vaatepunktist, mille tulemuseks on, et juhuslikku bitijada ei saa genereerida lühemast bitijadast kui see on. Viimane pseudojuhuslikkus vaatab asjale praktilisest küljest ja postuleerib, et tõenäosusjaotus X on pseudojuhuslik, kui teatud omadustega vaatleja ei suuda eristada jaotust X ühtlasest jaotusest U. Vastavalt praktilistele vajadustele on defineeritud erinevad pseudojuhuslikud generaatorid:

- Arhetüüpne pseudojuhuslik generaator – determineeritud algoritm, mis töötab polünomiaalse ajaga ja suudab petta kõiki polünomiaalses ajas töötavaid algoritme.
- Tugev pseudojuhuslik generaator – determineeritud polünomiaalses ajas töötav algoritm, mis suudab petta kõiki polünomiaalse keerukusega skeeme.
- Ruumilise(ajalise) piiranguga pseudojuhuslik generaator – on polünomiaalne algoritm, mille korral ruumis(ajas) $s(\cdot)$ töötavad eralgajate edu on väiksem kui $\epsilon(\cdot)$.
- Eritüübilised generaatorid
  - Paarikaupa sõltumatud generaatorid – algoritmid, mis genereerivad seemnest 2 $b(k)$ pikkusega juhuslikkus suurust, mis ühtlaselt ja sõltumatult jaotunud.

- Vähese kõrvalekaldega generaatorid – algoritmid, mis petavad ära lineaarse testi st.(XOR-takse mõningaid fikseeritud kohti väljundis)
- Expander Random Walk Generator – algoritmid, mis väljastavad stringide jada, mille elementide kuulumine suurde alamhulka on peaaegu sama tõenäosusega kui juhusliku jaotusega stringidejadal.
- Valijad(samplers) – algoritmid, mis määravad funktsiooni keskvväärtust, valides peaaegu juhuslikult kohad $x_1, x_2, \ldots, x_n$, kus uurida funktsiooni.
- Hajutajad(dispersers) ja sirutajad(extraktors)– algoritmid, mis suudavad petta selleks mõeldud algoritme. Täpsemalt mõõdetakse nende edukust sellega kui palju elemente genereerib algoritm mingi konkreetse arvu seemnete peal(tugevam neist on sirutaja).

Pseudojuhuslikuse kasutamine on motiveeritud:

- Korrektse definitsiooni omamine, mis ei sõltu ründetüüpidest.
- Juhuslikuse vähendamisega algoritmides. Suure venitusfunktsiooniga pseudojuhuslik generaator vähendab tunduvalt algoritmi juhuslikkuskeerukust, ilma algoritmi tulemust "muutmata". Arhetüüpne generaator toimib nii, et erinevus randomiseeritud ja a.g algoritmi vahel pole võimalik polünomiaalse masinaga kindlaks teha, mis ei tähenda et erinevusi pole vaid neid on "raske" leida. Et ka tulemuste erinevus oleks kaduvväike tuuakse mängu tugev generaator. Tulemuseks on see, et vaid lõplikul arvul sisenditel on erinevus.
- Võtme laiendamisega krüptograafias.
- Juhusliku valiku algoritmiseerimisega.

2 Kokkulepped ja definitsioonid

Generaator G saab seemne pikkusega k. Venitusfunktsiooniks $\ell(k)$ nimetatakse generaatori väljundi pikkust. Mõistetavatel põhjustel peab selle pikkus olema suurem kui seemnel. Edaspidi ilmneb, et generaatorit mitukorda rakendades võib genereerida polünomiaalse ajaga suvalise polünomiaalse pikkusega väljundeid. Seega üldsust kitsendamata võib eeldada, et $\ell(k) = k + 1$.

Tähistan U_k oraaklit, mis väljastab ühtlase jaotusega juhuslikke bitijadu pikkusega l. Eraldaja D on algoritm, mis musta kastina saab ette oraakli $\mathcal{O}$. Eraldaja peab otsustama, kas $\mathcal{O} = G(U_k)$ või $\mathcal{O} = U_{l(k)}$.

Definitsioon 1
Tähistan algoritmi A, mis teeb oraakelväljakutseid oraaklile $\mathcal{O}$ sümboliga $A^{\mathcal{O}}$.

Definitsioon 2
Mitedetermineeritud polünomiaalses ajas töötavate algoritmide klassi tähistan $\mathcal{RP}$.

Definitsioon 3
Eraldaja D eduks seemnepikkusega k generaatori G vastu nimetatakse suurust

$$\mathrm{Adv}_D^G(k) = \Pr\big[D^{G(U_k)} = 1\big] - \Pr\big[D^{U_{l(k)}} = 1\big].$$

Arvutuslik eristamatus tuuakse sisse järgmiselt. Vaadeldakse eraldajate klassi $\mathcal{D}$ ja eraldusfunktsioonide klassi $\mathcal{F}$ ja tullakse välja järgmise definitsiooniga, kus keerukust arvutatakse sõltuvalt seemne pikkusest.

Definitsioon 4 (Arhetüüpne pseudojuhuslik generaator)
Determineeritud algoritm nimetatakse pseudojuhuslikuks generaatoriks, kui ta töötab polünomiaalses ajas ning venitusfunktsioon $\ell(k) > k$ ja iga algoritmi korral klassist $\mathcal{D} = \mathcal{RP}$ ja iga f korral klassist $\mathcal{F} = \left\{ \frac{1}{f(x)} \mid f(x) \in \mathbb{R}^+[x] \right\}$ leidub k_0 nii, et $k > k_0$, siis

$$\Big|\mathrm{Adv}_D^G(k)\Big| < f(k)$$

Definitsioon 5 (Tõenäososjaotuste arvutuslik eristamatus)
Olgu $s : \mathbb{N} \to \mathbb{N}$ polünomiaalselt tõkestatud ja olgu meil kaks tõenäosusjaotuste peret $X = \{X_k\}_{k=1}^{\infty}$ ja $Y = \{Y_k\}_{k=1}^{\infty}$. Siis tõenäosusjaotuste pere on arvutuslikult eristamatu $s(\cdot)$ ekseplari valides, kui iga eristaja $D \in \mathcal{RP}$, (mis teeb perele X_k või Y_k $s(k)$ oraakelväljakutset) ning iga $f \in \mathbb{R}^+[k]$ leidub k_0 nii, et $k > k_0$, siis

$$\big|\Pr\big[D^{X_k} = 1\big] - \Pr\big[D^{Y_k} = 1\big]\big| < \frac{1}{f(k)}$$

Definitsioon 6 (Tugev pseudojuhuslik generaator)

Determineeritud algoritm nimetatakse tugevaks pseudojuhuslikuks generaatoriks, kui ta töötab polünomiaalses ajas ning venitusfunktsioon $\ell(k) > k$ ja iga polünomiaalse keerukusega skeemide pere $\{C_k\}_{k=1}^{\infty}$ korral ja iga $f \in \mathbb{R}^+[x]$ leidub k_0 nii, et $k > k_0$, siis

$$\left|\mathrm{Adv}_D^G(k)\right| < \frac{1}{f(k)}$$

3 Põhikonstruktsioonid

Olgu A tõenäosuslik alogoritm, mille juhuslikkuskeerukus on piiratud polünomiaalse funktsiooniga $\rho(n)$. Tähistagu algoritmi A sisendit x ja agoritmi poolt tarvitatud juhuslikku bitijada u. Nüüd $A(u,x)$ olgu A väljund, mis on saadud kasutades sisendiks x ja juhuarvujadaks u. Vaatlen nüüd kahte juhtu. Maailmas 1 olgu $u \leftarrow U_{\rho(k)}$, maailmas 0 valib A esmalt vähima k nii, et $\ell(k) \geq \rho(|x|)$ ja seejärel kasutab juhusliku bitijadana bitijada $u \leftarrow G(U_k)$.

Teoreem 1 (Derandomiseerimise arvutuslik eristamatus)
Olgu A ja G defineeritud nii nagu ülal. Siis iga kahe algoritmi F ja D korral klassist $\mathcal{RP}$ ja iga $f \in \mathbb{R}^+[n]$, leidub n_0 nii, et $n > n_0$, siis

$$\sum_{x\in\{0,1\}^n} \Pr\big[F(n)=x\big]\Delta_{A,D}(x) < \frac{1}{f(n)},$$

kus

$$\Delta_{A,D}(x) = \Pr\big[u \leftarrow U_{\rho(|x|)}, D(x,A(u,x))=1\big] - \Pr\big[u \leftarrow G^{U_k}, D(x,A(u,x))=1\big].$$

Tõestus
Olgu meil kolmik (A,F,D), mis rikub väidet. st leidub positiivne polünoom f ja jada (n_k) nii, et

$$\left|\sum_{x\in\{0,1\}^n} \Pr\big[F(n_k)=x\big]\Delta_{A,D}(x)\right| > \frac{1}{f(n_k)}.$$

Konstrueerime nüüd eristaja D' järgnevalt

$D'(u)$
| $x \leftarrow F(n)$
| return $D(x,A(u,x))$

See eristaja töötab selgelt polünomiaalses ajas ja ta edu on

$$\mathrm{Adv}^G_{D'}(n) = \Pr_1\big[x \leftarrow F(n), D(x,A(u,x))=1\big] - \Pr_0\big[x \leftarrow F(n), D(x,A(u,x))=1\big]$$

Kasutame tõenäosuse omadusi ja saame

$$\begin{aligned}\mathrm{Adv}^G_{D'}(n) = &\sum_{x\in\{0,1\}^n} \Pr_1\big[F(n)=x\big]\Pr_1\big[D(x,A(u,x))=1\big] \\ &- \sum_{x\in\{0,1\}^n} \Pr_0\big[F(n)=x\big]\Pr_0\big[D(x,D(x,A(u,x))=1\big]\end{aligned}$$

Seega

$$\mathrm{Adv}^G_{D'}(n) = \sum_{x\in\{0,1\}^n} \Pr\big[F(n)=x\big]\Delta_{A,D}(x)$$

millest olemegi saanud vastuolu.
□

Venitamise suurendamikseks kasutadakse järgmist konstruktsiooni. Olgu meil pseudojuhuslik generaator G_1 venitusfunktsiooniga $\ell_1(k) = k + 1$ ja $\ell(k) \in \mathbb{R}^+[k]$, siis vaatleme järgmist algoritmi G

$G(s)$
$x_0 = s$
for i=1..$\ell(|x|)$ do
  $\sigma_i x_i = G_1(x_{i-1})$
od;
return $\sigma_1\sigma_2\cdots\sigma_{l(|s|)}$

Teoreem 2 (Venitusfunktsiooni polünomiaalne võimendamine)
Niimoodi defineeritud G on pseudojuhuslik generaator.

Tõestus

Tõestus käib kasutades hübriidkonstruktsiooni. Defineerin järgnevalt hübriidid $H^k_{l(n)}$ (kus $k = 0, 1, \ldots, l(n)$) nii, et $H^k_{l(n)}$ koosneb uv. Need elemendid valitakse järgnevalt $u \leftarrow U_k$ ja v on generaatori G^{U_n} väljundi esimesed $l(n) - k$ bitti. Kuna selline definitsioon ei ole hea formaalseks tõestuseks, siis teen abikonstruktsiooni, defineerides funktsioonid $g^k_n : \{0,1\}^n \to \{0,1\}^k$. Nende definitsioon on induktiivne

$$g^0_n(x) = \lambda(tühisõna)$$
$$g^{k+1}_n(x) = \sigma g^k_n(y), \text{ kus } \sigma y = G_1(x)$$

Lihtne on veenduda, et $g^k_n(s) = \sigma_1\sigma_2\cdots\sigma_k$. Annan nüüd $H^k_{l(n)}$ formaalse definitsiooni

$$H^k_{l(n)} = uv, \text{ kus } u \leftarrow U_k \text{ ja } v = g^k_n(w), \quad w \leftarrow U_n.$$

Oraaklid U_k ja U_n tuleb konstruktsioonis lugeda sõltumatuteks. Nüüd on selge, et ülimad hübriidid $H^k_{l(n)} = G^{U_n}$ ja $H^{l(n)}_{l(n)} = U_{l(n)}$. Edasises on tarvis defineerida abifunktsioonid $f^m : \{0,1\}^{n+1} \to \{0,1\}^m$. Defineerin need induktiivselt

$$f^0(z) = \lambda$$
$$f^{m+1}(z) = \sigma g^m_n(y), \text{ kus } \sigma y = z.$$

Tõestan kaks abitulemust

$$H^k_{l(n)} = u f^{l(n)-k}(v), \quad u \leftarrow U_k \quad v \leftarrow G^{U_n}$$
$$H^{k+1}_{l(n)} = u f^{l(n)-k}(v), \quad u \leftarrow U_k \quad v \leftarrow U_{n+1}$$

Definitsioonist $H^k_{l(n)} = u g^{l(n)-k}(v)$. Et $g^m(x) = \sigma g^{m-1}(y)$, kus $\sigma y = G_1(x)$ ja $f^m(G_1(x)) = \sigma' g^{m-1}(y')$, kus $\sigma' y' = G_1(x)$, siis $g^m(x) = f^m(G_1(x))$ ja seega

on esimene võrdus näidatud. Teise korral $Hl(n)^{k+1} = ug^{l(n)-k-1}(v)$, kuid et definitsiooni kohaselt $f^{m+1}(\sigma y) = \sigma g^m(y)$, siis võin u viimase biti viia selle võrduse abiga f sisse. Tulemuseks on ikkagi ühtlane jaotus.

Oletan, et meil leidub algoritm D, mis murrab G st. leidub lõpmata palju n väärtusi, kus

$$\mathrm{Adv}_D^G(n) = \Pr\left[D^{G(U_n)} = 1\right] - \Pr\left[D^{U_{l(n)}} = 1\right] \geq \frac{1}{q(n)}.$$

Konstrueerin järgmise eraldaja D'

$D'(\alpha)$
$\quad k \leftarrow \{0, 1, 2, \ldots, l(n) - 1\}$
$\quad \beta \leftarrow \{0,1\}^k$
$\quad$ return $D(\beta f^{l(n)-k}(\alpha))$

Arvutan, D' edu

$$\mathrm{Adv}_{D'}^{G_1}(n) = \frac{1}{p(n)} \left(\sum_{k=0}^{p(n)-1} \Pr_1\left[D(\beta f^{p(n)-k}(\alpha)) = 1\right] - \sum_{k=0}^{p(n)-1} \Pr_0\left[D(\beta f^{p(n)-k}(\alpha)) = 1\right] \right).$$

Arvestades abitulemusi $\Pr_1\left[D(\beta f^{p(n)-k}(\alpha)) = 1\right] = \Pr\left[D(H_{l(n)}^k)\right]$ ja $\Pr_0\left[D(\beta f^{p(n)-k}(\alpha)) = 1\right] = \Pr\left[D(H_{l(n)}^{k+1})\right]$. Seega taanduvad summas peaagegu kõik liikmed välja

$$\mathrm{Adv}_{D'}^{G_1}(n) = \frac{1}{p(n)} \left[\Pr\left[D(H_{l(k)}^0) = 1\right] - \Pr\left[D(H_{l(k)}^{l(k)}) = 1\right]\right] = \frac{\mathrm{Adv}_D^G(n)}{p(n)}$$

ja siit on nüüd kege saada, et G_1 pole pseudojuhuslik generaator.
□

4 Ühesuunalised funktsioonid ja predikaat-tuumad

Definitsioon 1

Polünomiaalse ajaga arvutatavat funktsiooni $f : \mathbb{N} \to \mathbb{N}$ *nimetatakse ühesuunaliseks kui iga algoritmi* A' *korral klassist* $\mathcal{RP}$ *ja iga* $p(k) \in \mathbb{R}^+[k]$ *leidub* k_0 *nii, et* $k > k_0$*, siis*

$$\Pr\big[x \leftarrow U_k, A'(f(x)) \in f^{-1}(f(x))\big] < \frac{1}{p(k)}$$

Definitsioon 2 (Predikaat-tuum)

Polünomiaalses ajas arvutatav predikaat $b : \{0,1\}^* \to \{0,1\}$ *on funktsiooni* f *predikaat-tuum kui iga algoritmi* A' *korral klassist* $\mathcal{RP}$ *ja iga* $p(k) \in \mathbb{R}^+[k]$ *leidub* k_0 *nii, et* $k > k_0$

$$\Pr\big[x \leftarrow U_k, A'(f(x)) = b(x)\big] < \frac{1}{2} + \frac{1}{p(k)}$$

Teoreem 1 (Loomulik predikaat-tuum)

Olgu f *suvaline ühesuunaline funktsioon ja* $g(x,r) = f(x)r$*, kus* $|x| = |r|$*. Defineerin predikaadi* $b(x,r) = \sum_i x_i r_i \mod 2$*. Siis* $b(x,r)$ *on funktsiooni* g *predikaat-tuum.*

Teoreem 2 (Lihtsaim pseodojuhuslik generaator)

Olgu b *üksühese polünomiaalses ajas arvutatava funktsiooni* f *predikaat-tuum. Siis algoritm* $G(s) = f(s)b(s)$ *on pseudojuhuslik generaator.*

Tõestus

Oletame vastuväitliselt, et leidun agoritm D, mis lõpmatu arvu n korral

$$\left|\mathrm{Adv}_D^G(n)\right| \geq \frac{1}{q(n)},$$

siis Konstrueerin algoritmi A, mis arvutab f predikaat-tuuma järgnevalt

$A(y)$
$\sigma \leftarrow \{0,1\}$
$d \leftarrow D(y\sigma)$
if $d = 1$ return σ else $\overline{\sigma}$

Arvutan nüüd õige vastuse saamise tõenäosuse. Esmalt saan kaks abitulemust

$$\Pr\big[x \leftarrow U_n, A(f(x)) = b(x) \mid \sigma = b(x)\big] = \Pr\big[x \leftarrow U_n, D(f(x)\sigma) = 1\big]$$

$$\Pr\big[x \leftarrow U_n, A(f(x)) = b(x) \mid \sigma \neq b(x))\big] = \Pr\big[x \leftarrow U_n, D(f(x), \overline{b(x)}) = 0\big] = 1 - \Pr\big[x \leftarrow U_n, D(f(x)\overline{b(x)}) = 1\big].$$

Nendest tulemustest saan

$$\Pr\big[x \leftarrow U_n, A(f(x)), D(f(x)b(x)) = 1\big] = \Pr\big[x \leftarrow U_n, D(G(x)) = 1\big]$$
$$\Pr\big[x \leftarrow U_n, A(f(x)), D(f(x)\overline{b(x)}) = 1\big] =$$
$$2\Pr\big[u \leftarrow U_{n+1}, D(u) = 1\big] - \Pr\big[x \leftarrow U_n, A(f(x)), D(f(x)b(x)) = 1\big]$$

Viimane väide tuleb U_{n+1} jagamisest viimasebit järgi ja sellest f on bijektsioon. Nüüd äraarvamise edukus on

$$\Pr\big[x \leftarrow U_n, A(f(x)) = b(x)\big] = \Pr\big[\sigma = \underline{(}x)\big]\Pr\big[A(f(x)) = b(x) \mid \sigma = b(x)\big] +$$
$$\Pr\big[\sigma \neq b(x)\big]\Pr\big[A(f(x)) = b(x) \mid \sigma \neq b(x)\big] =$$
$$\frac{1}{2}\Big(\Pr\big[D(f(x)b(x)) = 1\big] + 1 - \Pr\big[D(f(x)\overline{b(x)}) = 1\big]\Big) =$$
$$\frac{1}{2}\big(\Pr\big[D(G(x)) = 1\big] + 1 - 2\Pr\big[u \leftarrow U_{n+1}, D(u) = 1\big] + \Pr\big[D(G(x)) = 1\big]\big)$$
$$\frac{1}{2} + \mathrm{Adv}_D^G(k).$$

Siit on lihtne saada vastuolu.
□

Järeldus 2.1
Olgu f ühesuunaline üksühene funktsioon, siis järgnev algoritm G on pseudojuhuslik generaator

$G(s)$
$x_0 = s$
for i=*1..*$\ell(|x|)$ *do*
  $x_i = f(x_{i-1})$
  $\sigma_i = b(x_{i-1})$
od;
return $\sigma_1\sigma_2\cdots\sigma_{l(|s|)}$

Tõestus
Et $G_1(x) = f(x)b(x)$ on pseudojuhusli generaator, siis on seda konstruktsiooni 3.2 tõttu ka algotitm G.
□

Teoreem 3 (Pseudojuhuslike generaatorite eksisteerimine)
Pseudujuhuslik generaator olemasolu ja ühesuunaline funktsiooni leidumine on samaväärsed.

Tõestus

Olgu meil pseudojuhuslik generaator G venitusfunktsiooniga $\ell(k) = 2k$. Nüüd defineerin iga $x, y \in \{0,1\}^k$ korral $f(x,y) = G(x)$, seega f on polünomiaalselt arvutatav. Oletades, nüüd et f pole ühesuunaline st. leidub algoritm A', mis pöörab f lõpmatus arvus punktides suurema eduga kui $\frac{1}{p(k)}$. Saan konstrueerida eraldaja D

$D(z)$
$(x,y) \leftarrow A'(z)$
if $f(x,y) = z$ return 1 else return $d \leftarrow \{0,1\}$

On selge, et kuna A' ja f töötavad polünomiaalses ajas, siis töötab seda ka D. Arvutan nüüd D edu, kus alaindeksiga 1 ja 0 tähistan tõenäosusi vastavalt oraakliga $G(U_k)$ ja U_{2k}

$$\mathrm{Adv}_D^G(k) = \Pr\left[D^{G(U_k)} = 1\right] - \Pr\left[D^{U_{2k}} = 1\right] =$$
$$\Pr_1\left[f(x,y) = z\right] + \frac{1}{2}\Pr_1\left[f(x,y) \neq z\right] - \Pr_0\left[f(x,y) = z\right] - \frac{1}{2}\Pr_0\left[f(x,y) \neq z\right]$$

Et maailmas 0 on tõenäosus sattuda pööratavale elemendile kaduvväike $\Pr\left[z \in f(XY)\right] \leq 2^{-k}$, siis kolmandat liiget on viidav kujule $2^{-k}\Pr\left[A'(z) \in f^{-1}(z)\right]$ ja seega

$$\mathrm{Adv}_D^G(k) \geq \Pr_1\left[f(x,y) = z\right] - 2^{-k}\Pr\left[A'(z) \in f^{-1}(z)\right] - \frac{1}{2}\left(1 - \Pr_1\left[f(x,y) = z\right] - 1\right)$$
$$\frac{1}{2}\Pr_1\left[f(x,y) = z\right] - 2^{-k}\Pr\left[A'(z) \in f^{-1}(z)\right] \geq (2^{-1} - 2^{-k})\Pr\left[A'(z) \in f^{-1}(z)\right]$$

Eelduse järgi on viimane tõenäosus jadal (k_l) suurem $\frac{1}{p(k_l)}$ ja seega saame vastuolu

$$\mathrm{Adv}_D^G(k_l) \geq \frac{1}{4}\frac{1}{p(k_l)}$$

Olgu meil nüüd ühesuunaline funktsioon f, kui f on üksühene, siis saab kasutada f predikaat-tuumaga konstruktsiooni. Vastasel juhul räsitakse $f(U_k)$, niisuguste räsifunktsioonidega milles on kindlad teise originaalileidmise suhtes. Tulemuseks on lühem string. Seda kompemseeritakse räsides algsest seemnest vajaliku arvu bitte juurde.
□

5 Pseudojuhuslikud funktsioonid

Definitsioon 1

Pseudojuhuslike funktsioonide pereks parameetritega $\ell_D, \ell_R : \mathbb{N} \to \mathbb{N}$ *nimetame funktsioonide peret* $\left\{f_s : \{0,1\}^{\ell_D(|s|)} \to \{0,1\}^{\ell_R|s|}\right\}_{s\in\{0,1\}^*}$, *mis rahuldab*

1. *Efektiivsus – leidub determineeritud polünomiaalne algoritm, mis antud seemne* s *ja* $\ell_D(|s|)$ *pikkuse argumendi* x *korral arvutab väärtuse* $f_s(x)$.

2. *Pseudojuhuslikus. Iga algoritmi* M *korral klassist* $\mathcal{RP}$ *ning iga* $p(k) \in \mathbb{R}^+[k]$ *korral leidub* k_0 *nii, et* $k > k_0$

$$\left|\Pr\left[M^{f(U_k)}(k) = 1\right] - \Pr\left[M^{F_k}(k)\right]\right| < \frac{1}{p(k)},$$

kus F_k *on võrdse tõenäosusega valitud kõikide funktsioonide hulgast* $Func_{\ell_D(|s|),\ell_R(|s|)}$.

Märkus: *Preudojuhuslikud funktsioonid on võimsamad. Näiteks* $\ell_D(k) = k$ *ja* $\ell_R(k) = 1$. *Siis pseudojuhuslik funktsioone on* 2^k *samas kui võrreldavas peres on* 2^{2^k} *elementi. Samas pseudojuhuslik generaator genereerib* 2^k *bitijada mis on eristamatud* $2^{p(k)}$ *bitijadast. Muidugi võib funktsiooni vaadelda ka kui bitijada, siis on näha kontrast* 2^{2^k} *versus* $2^{p(k)}$.

Kuid ometigi võib generaatoriga G, mille venitusfunktsioon $\ell(k) = 2k$ genereerida pseudojuhuslike funktsioonidepere. Olgu $G_0(s)$ esimesed $|s|$ bitti $G(s)$ väjundis ja $G_1(s)$ vastavalt viimased. Siis pseudojuhuslikku funktsiooni arvutav algoritm GF näeb välja

$GF(x, k)$
| t=k
| for $i = 1, 2, \ldots, |x|$ do
| $t = G_{x[i]}(t)$
| od;
| return t

kus $\ell_D(k) = \ell_R(k) = k$.

Teoreem 1 (Pseudojuhusliku funktsiooni konstruktsioon)

Ülaltoodud algoritm GF *annab psudojuhuslikku fubktsioonide pere* $f_s : \{0,1\}^{|s|} \to \{0,1\}^{|s|}$.

Teoreem tõestatakse kasutades hübriid tehnikat. Hübriid H_k^i on $2^{2^i k}$ elemendiline funktsioonide pere $\{0,1\}^k \to 0,1^k$. Defineeritakse 2^i juhuslikku k-bitist bitijada mis indekseeritakse $(s_\alpha)_{\alpha\in\{0,1\}^i}$. See sama bitijada jääbki võtmeks. Funktsiooni väärtus kohal $x = \beta\alpha$ võtmega $(s)_{\alpha\in\{0,1\}^i}$ on $GF(\beta, s_\alpha)$. Siis $H_k^0 =$

$GF(x,s)$ ja $H_k^k = Func_{2^k,2^k}$. Nüüd kogu tõestus on ehitatud suuruste H_k^i ja H_k^{i+1} eristamatusele, mis põhineb on $G_j(s)$ ja s' eristamatusel.