Eötvös Loránd Tudományegyetem

Természettudományi kar

Marton Péter

Pszeudovéletlen sorozatok

MSc Szakdolgozat

Témavezető:

Gyarmati Katalin, egyetemi docens

Algebra és Számelmélet Tanszék

Bevezetés

A szakdolgozatban az egyik legelterjedtebb és bizonyítottan biztonságos titkosítási eljárásról, a One Time Padről adok bevezetést, illetve az ehhez szükséges nagy mennyiségű véletlen bit generálásához egy technikát. Ennek továbbfejlesztése és elemzése saját munka, melyben nem bitekkel, hanem tetszőleges m-szimbólumokkal dolgozok. Bevezetést adok a kvadratikus maradékokon alapuló pszeudovéletlen sorozatok generálásába, egy saját bizonyítással. Leírást adok a lineáris komplexitás fogalmáról. A pszeudovéletlen sorozatokat előállító, azok lineáris komplexitását, eloszlási, normalitási, korreláció és kombinált mértékeit kiszámító program saját munka és a szakdolgozat melléklete.

Egyszer használatos kulcs

1917-ben találta fel, majd 1919-ben szabadalmaztatta Gilbert Vernam. A telegráfokon bitenként küldött adatok véletlenszerűen választott bitjeinek megváltoztatásával titkosítható a küldött üzenet. Ha a lehallgató nem ismeri, mely biteket változtatta meg a küldő (tehát nem ismeri a véletlen vagy pszeudovéletlen kulcsot), az üzenet tartalmáról semmivel sem tud több információt szerezni, mint az üzenet hossza. A titkosított üzenet a kulcs ismeretében elolvasható, ha a megváltoztatott biteket visszaváltoztatjuk. Ez az egyetlen (Claude Shannon által) bizonyítottan biztonságos rejtjelzés, úgynevezett „tökéletesen biztonságos titkosítás”. A titkosítás nehézsége, hogy elő kell állítani véletlen biteket, kommunikáció előtt a feleknek rendelkezniük

közös kulccsal, ezeket titokban kell tartani, a felhasznált biteket meg kell semmisíteni, ha az összes rendelkezésre álló bitet elhasználták a felek, a további kommunikációhoz új kulcsot kell generálni és eljuttatni a feleknek. A One Time Pad alkalmas úgynevezett szuper titkosításra, azaz már titkosított üzenetek ismételt titkosítására, nyílt szöveg más titkosításalgoritmussal történő titkosítása előtti titkosítására illetve több különböző kulcs szerinti One Time Pad titkosításra feltéve, hogy minden One Time Pad kulcsa minden mástól független. A One Time Pad titkosítás „nem ronthat" el más titkosításokat, ismételt alkalmazása biztonságosabbá teszi a kommunikációt gyengébb véletlen kulcsok esetén is, de kizárólag csak akkor, ha a kulcsok függetlenek és valóban csak egyszer használták fel. Ehhez célszerű szem előtt tartani, hogy titkosítás/fejtés után a kulcsot azonnal meg kell semmisíteni, hogy ne követhessünk el a két kulcsos láda modellhez hasonló hibákat.

Entrópia: ξ valószínűségi változó $p_1, p_2, \ldots > 0$ valószínűséggel veszi fel különböző lehetséges értékeit. Ekkor ξ entrópiája

$$-\sum p_i \log_2 p_i.$$

Mivel p_i pozitív valószínűségek, $p_i \log_2 p_i$-k nem pozitív számok, ezek összegének ellentettje tehát nemnegatív. Mivel $\sum p_i = 1$, az entrópia legfeljebb 1 lehet. Az entrópia akkor és csak akkor 1, ha a valószínűségi változó a nem nulla valószínűséggel felvett értékeit egyenlet eloszlás szerint veszi fel, 0, ha egy értéket 1 valószínűséggel vesz fel.

Neumann fehérítés

Ez a fejezet Neumann János 1951-es Various techniques used in connection with random digits[17] munkáján alapul.

Tegyük fel, rendelkezésünkre állnak $\xi_1, \xi_2, \ldots$ nem feltétlenül 1 entrópiájú, független, azonos eloszlású valószínűségi változók. Képezzük α_j valószínűségi változók sorozatát a következőképpen:

- $\xi_{2i-1} = 0, \xi_{2i} = 1$ esetén a soron következő $\alpha_j = 0$
- $\xi_{2i-1} = 1, \xi_{2i} = 0$ esetén a soron következő $\alpha_j = 1$

Tehát ha $\xi_{2i-1} = \xi_{2i}$, azokat elvetjük, és a soron következő α_j-t a következő ξ_{2i+1}, ξ_{2i+2} pár szerint választjuk.

Állítás: α_j entrópiája 1

Bizonyítás: Származzon α_j a ξ_{2i-1}, ξ_{2i} valószínűségi változókból. Mivel α_j definiált, $\xi_{2i-1} \neq \xi_{2i}$. Mivel ξ_{2i-1} és ξ_{2i} független és azonos eloszlású

$$\begin{aligned} \mathrm{P}\left(\alpha_j = 0\right) &= \mathrm{P}\left(\xi_{2i-1} = 0, \xi_{2i} = 1\right) = \mathrm{P}\left(\xi_{2i-1} = 0\right) \cdot \mathrm{P}\left(\xi_{2i} = 1\right) = \\ &= \mathrm{P}\left(\xi_{2i-1} = 1\right) \cdot \mathrm{P}\left(\xi_{2i} = 0\right) = \mathrm{P}\left(\xi_{2i-1} = 1, \xi_{2i} = 0\right) = \mathrm{P}\left(\alpha_j = 1\right) \end{aligned}$$

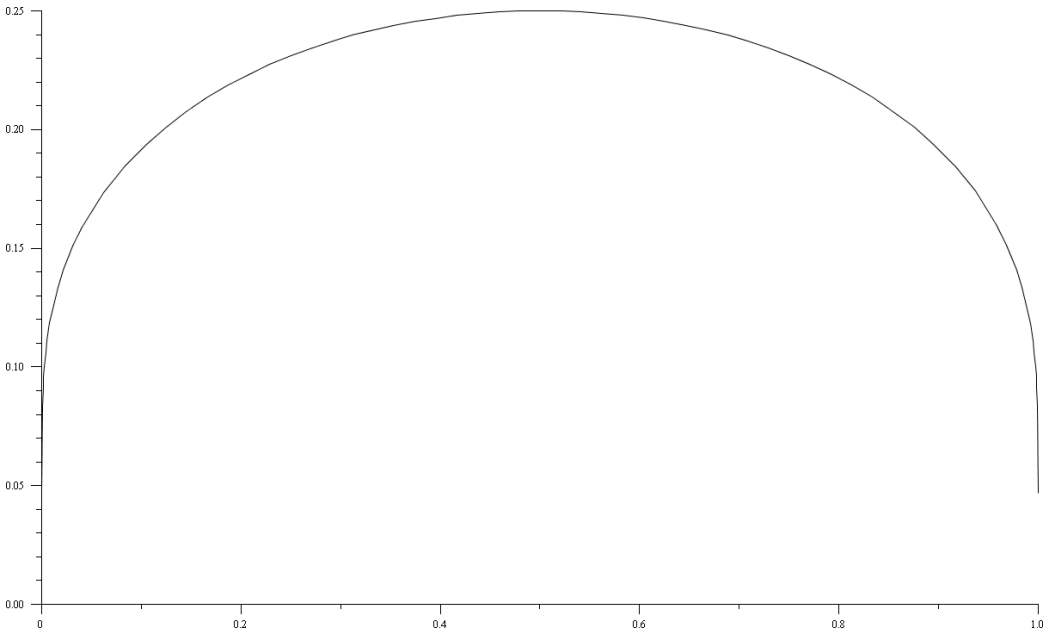
Ez a módszer lehetővé teszi a One Time Pad használatát abban az esetben is, ha nem tudunk egyenletes eloszlással véletlen biteket generálni. Bármilyen nem konstans eloszlás alkalmas, azonban kisebb entrópiájú ξ valószínűségi változókból többre lesz szükség ugyanannyi 1 entrópiájú α előállításához.

Állítás: Ha a $\xi_1, \ldots, \xi_n$ valószínűségi változók entrópiája $0 < x = -p \log_2 p - (1-p) \log_2 (1-p) \leq 1$, akkor a teljes $\xi_1, \ldots, \xi_n$ sorozat entrópiája nx, mely-

ből várható értékben $np(1-p)$ darab 1 entrópiájú α_j valószínűségi változót generálunk.

Bizonyítás: Az 1 entrópiát az imént beláttuk, csak a várható elemszámot kell bizonyítanunk. Mivel elempárokhoz rendelünk α_j elemeket, eleve legfeljebb feleannyi lesz. Ráadásul csak akkor írunk le ténylegesen egy α_j-t, ha ξ_{2i-1}, ξ_{2i} különböző. Mivel $P(\xi_{2i-1} \neq \xi_{2i}) = 2p(1-p)$ és $\frac{n}{2}$ változó-párunk van, várható értékben $np(1-p)$ különböző lesz köztük.

Láthatjuk tehát, hogy a Neumann fehérítés során csökkentjük a sorozat entrópiáját. Ha ξ $50-50\%$-kal vesz fel $0-1$ értékeket, úgy $1/4$-ére csökkentettük az entrópiát, sőt minél inkább eltérnek a ξ változók az egyenletes eloszlástól, annál nagyobb arányban csökken az elkészített sorozat entrópiája (hiszen egyre tipikusabb lesz a két egyforma). Jó hír azonban, hogy ez az arány nem „száll el", például $p = 10^{-6}$ esetén is csak 20-adára csökken az entrópia, így a gyakorlatban szélsőséges esetben is hatékonyan használható. Az entrópia csökkenés arányát (ξ entrópiájának függvényében) az alábbi grafikon szemlélteti.



Tetszőleges m-elemű értékkészletű valószínűségi változók fehérítése

Elempárok helyett elem m-eseket vegyünk. Ha előfordul benne két egyforma értéket felvevő ξ_i, dobjuk el, ha a $\xi_{km+1}, \ldots, \xi_{km+k}$-k csupa különböző értéket vesznek fel, írjunk le $\alpha_j := \xi_{km+1}$-et, tehát (a ξ_i-k által felvett értékeket értékeket $0 \ldots m$ számjegyekkel jelölve):

$$
\left.\begin{array}{c}
01234\ldots m \\
02134\ldots m \\
\vdots \\
0m\ldots 4321
\end{array}\right\} \quad \alpha_j := 0
$$

$$
\left.\begin{array}{c}
12345\ldots m \\
13245\ldots m \\
\vdots \\
1m\ldots 4320
\end{array}\right\} \quad \alpha_j := 1
$$

$$
\vdots
$$

$$
\left.\begin{array}{c}
m01234\ldots \\
\vdots \\
m\ldots 43210
\end{array}\right\} \quad \alpha_j := m
$$

Kérdés most, hogy hogyan változott a sorozat entrópiája (azaz hány α_j-t írtunk le). Akkor írunk le egy α_j-t, ha $\xi_{km+1} \neq \ldots \neq \xi_{km+m}$. Ennek az esélye

$$
m! \prod_{i=1}^{m} p_i,
$$

ahol p_i szokásosan a ξ változók által felvett különböző értékek valószínűségét jelöli. Vegyük észre, hogy egyenletes eloszlás esetén α_j leírásának esélyére

$$
\frac{m!}{m^m}
$$

adódik, ezt összevetve azzal, hogy most változó m-esekkel dolgozunk adódik, hogy az entrópia a fehérítés során legalább

$$\frac{m!}{m^{m+1}}$$

-ed részére csökken. Továbbá ha valamelyik értéket nagyon kis p_i valószínűséggel veszi fel, úgy az entrópia eleve kisebb kell legyen, mint $\frac{m!}{p_i}$. Ennek javítására szolgál az alábbi ötlet: vegyük a t legnagyobb valószínűséggel előforduló értéket, tekintsük a $t!$ lehetséges permutációt lexikografikus sorrendben. Tegyük fel, a soron következő $\xi_{kt+1}, \ldots, \xi_{kt+t}$ m-es szerepel ezen a listán, mégpedig a σ-adik helyen:

$$\begin{aligned}
1 \leq \quad \sigma \quad &\leq \left\lfloor \frac{t!}{m} \right\rfloor \Rightarrow \alpha_j := 0 \\
1 + \left\lfloor \frac{t!}{m} \right\rfloor \leq \quad \sigma \quad &\leq 2 \cdot \left\lfloor \frac{t!}{m} \right\rfloor \Rightarrow \alpha_j := 1 \\
&\vdots \\
1 + i \cdot \left\lfloor \frac{t!}{m} \right\rfloor \leq \quad \sigma \quad &\leq (i+1) \cdot \left\lfloor \frac{t!}{m} \right\rfloor \Rightarrow \alpha_j := i \\
&\vdots \\
1 + (m-1) \cdot \left\lfloor \frac{t!}{m} \right\rfloor \leq \quad \sigma \quad &\leq m \cdot \left\lfloor \frac{t!}{m} \right\rfloor \Rightarrow \alpha_j := m-1
\end{aligned}$$

Egyéb esetekben (tehát $1+m\cdot\left\lfloor \frac{t!}{m} \right\rfloor \leq \sigma \leq t!$, vagy σ nem is szerepel a listán), $\xi_{kt+1}, \ldots, \xi_{kt+t}$-et eldobjuk, és vesszük a következő $\xi_{kt+t+1}, \ldots, \xi_{kt+t+t}$-t.

Mi a várható értékben optimális t?

Egyrészt világos, hogy $t! \geq m$ kell, különben a fenti egyenlőségek nem teljesülhetnének, és nem írhatnánk le egy α_j-t sem. Ez után ha hozzáveszünk

a soron következő p_{k+1} valószínűséggel felvehető értéket, akkor egy felől a permutációk $k+1$ hosszúak lesznek, így az entrópia $\frac{k}{k+1}$-ed részére csökken. Másfelől eddig szerepelt egy p_{k+1}^k szorzó az entrópiában (ugyanis ha a p_{k+1} valószínűségi bejött bármikor a k-asba, rögtön érvénytelen lett, ezután érvényes marad). Szerepel ugyan egy $1 + m \cdot \left\lfloor \frac{t!}{m} \right\rfloor \leq \sigma \leq t!$ eset, de ezt hanyagoljuk el. Így az adódik, hogy a p_{k+1} valószínűségi érték hozzávételével az entrópiaváltozás szorzója:

$$\frac{k}{(k+1)\, p_{k+1}^k}$$

Tehát ha ez > 1, hozzávesszük, ha nem elutasíthatjuk és megállunk, hiszen a még valószínűtlenebb p_{k+l}-ek hozzávétele csak még rosszabb lenne (feltéve az említett elhanyagolást).

Lineáris komplexitás

Ez a fejezet a 2004-es Fundamentals of Cryptography[15] kurzuson alapul.

Definíció: *LFSR (Linear Feedback Shift Register, Lineáris Visszacsatolási Regiszter): $r_{1,0}, \ldots, r_{n,0}$ adott, $r_{1,i} = \sum \alpha_j r_{i-1,j}$ ahol α_j-k szintén adottak, $i > 0$, $r_{k,i} = r_{k-1,i-1}$ ahol $k, i > 0$. Kimenetnek nevezzük az $r_{1,i}$-ket $i > 0$-ra. Úgy érdemes rágondolni, hogy $r_{i,j}$-ben az i egy sorszám, j az idő, $r_{1,0}, \ldots, r_{n,0}$ kezdeti állapot, minden következő időpillanatban az egész „rendszer" jobbra tolódik, ezért a jobb szélső kilökődik, a bal szélső helyére pedig az előző ál-*

lapot egy lineáris kombinációja kerül. Véletlenszám generálásra használjuk, tipikusan $\mathbb{Z}_2$ felett.

Definíció: *LFSR hossza: a fenti definícióban szereplő n.*

Definíció: *Lineáris komplexitás: egy (véges vagy végtelen) számsorozat lineáris komplexitása n, ha az azt előállító legrövidebb LFSR hossza n. Jelölje $LC()$.*

Példa:

1. $x \equiv 0$ számsorozat az üres LFSR-rel generálható, lineáris komplexitása 0

2. $x \equiv 1$számsorozat az $r_{1,0} = 1, \alpha_1 = 1$ egy tagú LFSR-rel generálható, lineáris komplexitása 1

3. $x_1, x_2, \ldots, x_{s-1} = 0, x_s = 1$ (esetleg néhányszor vagy végtelenszer megismételve): $r_{1,0}, \ldots, r_{s-1,0} = 0, \alpha_2, \ldots, \alpha_s = 0, r_{s,0} = 1, \alpha_1 = 1$, lineáris komplexitása s

Rekurzió megoldása: jelölje $f(x)$ az alábbi m-ed fokú polinomot:

$$\sum_{i=0}^{m} \alpha_i x^i$$

Reciprociális megoldás:

$$f^*(x) := x^m f\left(x^{-1}\right) = \sum_{i=0}^{m} \alpha_i x^{m-i}$$

ahol $\alpha_m = 1$.

Állítás: $degf^*(x) \leq degf(x)$, $degf^*(x) = degf(x) \Leftrightarrow \alpha_0 = 1$

Állítás: $h(x) = f(x)\,g(x) \Rightarrow h^*(x) = f^*(x)\,g^*(x)$

Definíció: $\Omega(f) =$ *„az összes* $m = degf$ *hosszú számsorozat mint* $r_{1,0}, \ldots, r_m, 0$ *folytatva* f α_i *együtthatói által diktált szabály szerint" halmaz, nevezzük* f *által generált számsorozatok halmazának.*

Állítás: $\Omega(f)$ m *dimenziós vektortér*

Állítás: *ha egy* S *polinomot generál* f*, akkor létezik egy* P *polinom (*$degP < m$*), hogy* $S = P/f^*$

Állítás: $\Omega(f) = \{S = P/f^* | degP < m\}$

Állítás: *ha* $P \in \Omega(f), S \in \Omega(g)$*, akkor* $P + S \in \Omega(h)$*, ahol* $h = [f, g]$*, azaz a legkisebb közös többszörös.*

Állítás: $f \mid h \Rightarrow \Omega(f) \subseteq \Omega(h)$

Definíció: $f \in \mathbb{Z}_2[x]$ *exponense a legkisebb* $e \geq 1$ *szám, melyre* $f(x) \mid x^e + 1$*. A következő* f*-ek (melyekben exponensről beszélünk) legyenek* $\mathbb{Z}_2[x]$*-beliek.*

Állítás: $\Omega(f)$*-beli számsorozat periódusa osztja* f *exponensét*

Állítás: f *irreducibilis* $\Leftrightarrow$*minden nem-nulla* $\Omega(f)$*-beli számsorozat periódushossza* f *exponense*

Definíció: f *primitív, ha exponense* $2^m - 1$

Állítás: *primitív polinom által generált számsorozat periódusa* $2^m - 1$

Állítás: *egy számsorozat lineáris komplexitása legyen* L

1. *bármely legfeljebb* L *elemű részsorozata lineárisan független*

2. *bármely* L*-nél nagyobb elemszámú részsorozata lineárisan összefüggő*

3. *bármely legalább $2L$ elemű részsorozat egyértelműen meghatározza f-et.*

Berlekamp–Massey-tétel: *Ha egy számsorozat első k elemét generáló polinom nem generálja az első $k+1$ elemből álló sorozatot, akkor*

1. *Az első $k+1$ elem lineáris komplexitása $L_{k+1} = max\{L_k, k+1-L_k\}$ (ahol L_k az első k elem lineáris komplexitása)*

2. $f_{k+1}(x) = x^{L_{k+1}} f_k(x) + x^{L_{k+1}-k+m-L_m} f_m(x)$, *ahol f_j az első j elemet generáló polinom, $m = \max\{i \mid L_i < L_k\}$*

Pszeudovéletlen mértékek

Ez a fejezet Gyarmati Katalin Measures of pseudorandomness[4] cikkén alapul.

Eloszlási mérték

Legyen E_N egy N elemű ± 1 sorozat, és legyen U az a-adik, az $a+b$, az $a+2b$-edik stb. $t+1$ elemű részsorozat-összeg, azaz

$$U\left(E_N, t, a, b\right) = \sum_{j=0}^{t} e_{a+jb}.$$

Maduit és Sárközy vezette be[10] az eloszlási mértéket, mely az összes számtani sorozatot (felvett értékek: 1-től N-ig) vizsgálja: melyiken a legkiegyenlítetlenebb a ± 1-ek száma. A generált sorozat akkor rossz, ha van benne egy hosszú számtani sorozat, amin a ± 1-ek aránya jelentősen eltér az 50%. Nyilván nem vehetjük figyelembe a legkiegyenlítetlenebb arányt, hiszen az egy elemű részsorozatokban ez 0%. Végülis a kiegyenlítetlenség és a hossz szorzata a legkézenfekvőbb és legkönnyebben kiszámítható. Az eloszlás mértéket így az alábbi képlet definiálja:

$$W\left(E_N\right) = \max_{a,b,t} \left|U\left(E_N, t, a, b\right)\right| = \max_{a,b,t} \left|\sum_{j=0}^{t} e_{a+jb}\right|$$

Korrelációs mérték

Legyen V az első M szorzat az összege, melyeket egy D lyukkulcsból kapnánk a következőképpen: adott egy ℓ elemű $D = d_1, \ldots, d_\ell$ számhalmaz, mi pedig egy rácsos papírcsík d_1-edik, d_2-edik, ..., d_ℓ-edik rácsát kilyukasztanánk.

A lyukakban látható elemeket összeszorozzuk: ez tehát -1, ha páratlan sok -1 van a lyukak alatt, $+1$ egyébként. Ezt M-szer végezzük el: először a papírcsík elejét az első elemre tesszük, aztán a másodikra, ..., végül az M-edikre. Akkor tapasztalunk rossz pszeudovéletlen tulajdonságot, ha nem $50-50\%$ körül alakul a $+1$ és -1 szorzatok aránya. Ez alól felmentés, ha M túl kicsi: például ha $M = 1$, akkor $0 - 100\%$ lesz az arány. Végülis az M értéke és az arány szorzata ismét a legkézenfekvőbb és legkönnyebben kiszámítható formula:

$$V\left(E_N, M, D\right) = \sum_{n=1}^{M} \prod_{i=1}^{i=\ell} e_{n+d_i}$$

Vegyük az összes lehetséges ℓ elemű D halmazt (2^ℓ darab) és hozz az összes lehetséges M-et (1 és $N - d_\ell$ közöttiek), és ezek maximumaként definiálta Maduit és Sárközy[10] az ℓ-edrendű korrelációs mértéket:

$$C_l\left(E_n\right) = \max_{M,D} \left|V\left(E_N, M, D\right)\right| = \max_{M,D} \sum_{n=1}^{M} \prod_{i=1}^{i=\ell} e_{n+d_i}$$

Kombinációs mérték

Az ℓ-edrendű korrelációs mértéket (amikor a papírcsík első mezőjét E_N első, második, ...,M-edik bitjére tettük) és az eloszlási mértéket (amikor egy $t+1$ elemű a kezdőértékű b differenciájú számtani sorozattal dolgoztunk) kombinálva jutunk Maduit és Sárközy [10] kombinációs mértékéhez. Így kapjuk a kombunációs mértéket, amikor a papírcsíkot a számtani sorozat elemeinek megfelelő helyekre kell lerakni, aztán ugyanazt csinálni, mint az ℓ-edrendű korrelációs mértéknél: venni a lyukak alatti számok szorzatát (páros/páratlan db -1-es), majd ennek a t darab ± 1-nek az összegét. Az ℓ-edrendű kombináció mérték (Q_ℓ) képlete:

$$Z\left(E_N, a, b, t, D\right) = \sum_{j=0}^{t} \prod_{i=1}^{\ell} e_{a+jb+d_i}$$

$$Q_\ell\left(E_N\right) = \max_{a,b,t,D} \left|Z\left(E_N, a, b, t, D\right)\right| = \max_{a,b,t,D} \left|\sum_{j=0}^{t} \prod_{i=1}^{\ell} e_{a+jb+d_i}\right|$$

Normalitás mérték

Legyen X egy tetszőleges ℓ elemű ± 1 bitsorozat (gonduljunk rá szóként). Ezt a szót fogjuk keresni összefüggő részsorozatként E_N-ben (mint egy könyvben). Adott X szóra E_N könyvre és M limitre T azt mutatja meg, hányszor fordul elő az X szó a könyv elejében (csak az első $M+\ell$ bit számít — tehát ha az $M+1$-edik bit az X szó első bitje, az még beleszámít). Képlettel:

$$T\left(E_N, M, X\right) = \left|n : 0 \leq n \leq M, \left(e_{n+1}, \ldots, e_{n+\ell}\right)\right|.$$

Ennek segítségével definiáljuk a normalitás mértéket, mely T legfurcsább az összes lehetséges 2^ℓ szó és az összes lehetséges $0 \leq M \leq N - \ell$ kezdőszeletre. Jól látható, hogy ℓ értékére nem maximalizálhatunk, továbbá, hogy $T(E_N, M, X)$ várható értéke

$$\frac{M}{2^\ell},$$

tehát az ettől vett nagy eltérés számít majd furcsának; a furcsaság nagysága pedig a különbség (abszolútértékben). Így kapjuk Maduit és Sárközy[10] ℓ-edrendű normalitás mértékét:

$$N_\ell(E_N) = \max_{M,X} \left| T(E_N, M, X) - \frac{M}{2^l} \right|.$$

Különböző pszeudovéletlen mértékek

p	$f(x)$	n	S	W	N_1	N_2	N_3	C_1	C_2	C_3	Q_1	Q_2	Q_3
7	$7x^{10} - 8x^7 + 3x^5 - 14$	3	2	2	0	0	0	2	2	2	2	1	0
11	$7x^{10} - 8x^7 + 3x^5 - 14$	5	0	4	1	2	1	4	4	3	4	3	2
13	$7x^{10} - 8x^7 + 3x^5 - 14$	6	2	5	1	1	0	3	4	3	5	4	3
17	$7x^{10} - 8x^7 + 3x^5 - 14$	8	1	7	1	1	1	3	4	5	7	6	5
19	$7x^{10} - 8x^7 + 3x^5 - 14$	9	1	8	0	2	2	2	7	3	8	7	6
23	$7x^{10} - 8x^7 + 3x^5 - 14$	11	1	10	2	2	2	5	4	7	10	9	8
29	$7x^{10} - 8x^7 + 3x^5 - 14$	14	0	13	2	1	1	5	7	7	13	12	11

Rácsok

Ez a fejezet Gyarmati Katalin On finite pseudorandom binary lattices[18] cikkén alapul.

A sorozatok általánosítása a rács, melyben nem csak egy dimenziósban $(a_1, a_2, a_3, \ldots)$ követik egymást elemek, hanem tetszőleges N dimenzióban (például 2 dimenzióban a koordináta rendszer első síknegyedébe eső rácspontokon értelmezünk elemeket). Ha pszeudovéletlen sorozatok helyett pszeudovéletlen rácsokra van szükségünk, más eljárással kell ellenőriznünk, kielégítően véletlennek tűnik-e a generált rács. Ehhez Hubert, Mauduit, Sárközy defiiálta a bináris rácsokon értelmezett pszeudovéletlen mértékeket[9].

Definíció: *n dimenziós N-rács:*

$$I_N^n = \{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in \{0, 1, \ldots, N\}\}$$

Azaz azokból az n dimenziós vektorokból álló halmaz, melyek kordinátái $0, 1, \ldots, N$. n gyakran fixen 2 vagy 3: ha nyilvánvaló, gyakran elhagyjuk, és csak N-rácsról beszélünk. Ez az $N \times N$-es négyzetrács vagy $N \times N \times N$-es kockarács. A definíció kiterjeszthető téglalaprácsra/téglatestrácsra, ilyenkor egy $M \times N$-es téglalap esetén például (M, N)-rácsként hivatkozunk rá.

Definíció: *n dimenziós bináris N-rács:*

$$\eta\left(x_1, \ldots, x_n\right) : I_N^n \to \{-1, +1\}.$$

Röviden bináris rács, tehát egy rácson értelmezett bináris η függvény.

Definíció: *n dimenziós N-tégla: adott $u \in \{1, \ldots, N\}^n$ vektor többszörösei, amik beleesnek $t \in \{0, \ldots, N\}^n$ vektor által meghatározott (kifeszített origó csúcs tengelypárhuzamos) n dimenziós téglába.*

Definíció (Hubert–Maudit–Sárközy): *η bináris háló k-adrendű pszeudorandom mértéke:*

$$Q_k(\eta) = \max_{B, d_1, \ldots, d_k} \sum_{x \in B} \prod_{i=1}^{k} \eta(x + d_i),$$

ahol $d_1, \ldots, d_k \in \{0, \ldots, N\}^n$ és B olyan N-tégla, hogy

$$B + d_i \in I_N^n \qquad \forall i = 1, \ldots, k.$$

Ez a sorozatokra értelmezett k-adrendű Q_k kombinációs mérték általánosítása.

Hubert, Maudit és Sárközy megmutatta[9],[14], hogy

$$\sqrt{N^n}$$

körüli, egész pontosan minden elég nagy N-re és elég kis $\delta > 0$-ra

$$P\left(Q_k(\eta) > \delta\sqrt{N^n}\right) > 1 - \varepsilon$$

és

$$P\left(Q_k(\eta) > \sqrt{81kN^n \log N^n}\right) < \varepsilon$$

Nagyságrendileg tehát $\sqrt{N^n}$ és $\sqrt{N^n kn \log N}$ közötti.

Egy aszimptotikusan jól korlátozható konstrukció: legyen $\mathbb{F}_{p^n}$-nek (mint véges testnek) kvadratikus karaktere γ, és (mint $\mathbb{F}_p$ feletti n dimenziós vektortérnek) egy bázisa $\underline{v} = v_1, \ldots, v_n$. Ekkor ha η n dimenziós bináris p-rács

$$\eta(\underline{x}) = \gamma(\underline{x} \cdot \underline{v}),$$

ahol p páratlan prím $\underline{x} \in \mathbb{F}_p^n$, $\cdot$ a skalárszorzat, $\gamma(\underline{0})$-t pedig 1-gyel helyettesítsük, akkor

$$Q_k(\eta) < k\sqrt{q}\,(1 + \log p)^n,$$

nagyságrendileg tehát

$$Q_k(\eta) = O\left(\sqrt{N^n} k (\log N)^n\right).$$

Definíció: *Legyen $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_{p^n}$ (p prím). $\mathcal{A}+\mathcal{B}$-t P-tulajdonságnak mondjuk, ha minden $c \in \mathbb{F}_{p^n}$ páros sokféleképpen áll elő*

$$a + b = c \qquad a \in \mathcal{A}, b \in \mathcal{B}$$

alakban (beleértve a 0-féleképpent is).

Definíció: *(k, l, q)-t megengedett hármasnak mondjuk, ha minden olyan $\mathcal{A}, \mathcal{B} \subset$*

$\mathbb{F}_p$ *halmazra amelyre*

$$\begin{aligned} |\mathcal{A}| &= k \leq q \\ |\mathcal{B}| &= l \leq q \end{aligned}$$

tudjuk, hogy $\mathcal{A} + \mathcal{B}$ *P-tulajdonságú.*

Általánosítsuk az előző konstrukciót: $\underline{x} \cdot \underline{v}$-t behelyettesíthetjük egy tetszőleges $f(\underline{x} \cdot \underline{v})$, $0 < \deg f < p$, $f \in \mathbb{F}_q[x]$ polinomba. Ha minden $r < \deg f$-re, a pszeudovéletlen mérték k-jára, a véges test/vektortér q-jára (r, k, q) megengedett hármas, akkor ezzel az általánosított konstrukcióval nyert η rácsok aszimptotikusan jól korlátozható pszeudovéletlen mértékkek rendelkeznek; tudjuk ugyanis, hogy

$$Q_k(\eta) < kl\left(\sqrt{q}\,(1 + \log p)^n + 2\right)$$

azaz

$$Q_k(\eta) = O\left(\sqrt{N^n} kl\,(\log N)^n\right)$$

Ebben az általánosított konstrukcióban feltettük, hogy (r, k, q) megengedett hármas, de eddig nem adtunk receptet megengedett hármasok készítésére, sem egy gyorsan eldönthető kritériumot arra, hogy egy számhármas megengedett hármas-e. Kiderül azonban, hogy megengedett hármast készíteni igen

könnyű; a következő két típus megngedett hármas:

$$(l, 2, q) \qquad \text{ha } l < p, \text{ ahol } q = p^n$$

$$(k, l, q) \qquad \text{ha } 4^{n(k+l)} < p, \text{ ahol } q = p^n.$$

Pszeudovéletlenségi tesztek

Ez a fejezet Noga, Kohayakawa, Mauduit, Moreira, Rödl - Measures of pseudorandomness for finite sequences: Typical Values (2006)[14] munkáján, a NIST (National Institute of Stadards and Technology) általánosan használt pszeudovéletlen sorozat generátor tesztjein alapul. A tesztek hivatalos outputja véletlen vagy nem véletlen, valójában azonban mindig egy P értéket számolnak ki, azaz annak a valószínűségét, hogy ha a sorozat véletlen lenne, mennyi eséllyel mutatná a tesztelt tulajdonságra a rossz pszeudogenerátor jellemzőit. Ha ez 1% alá megy, nem véletlennek, egyébként véletlennek minősíti a sorozatot. Így az elsőfajú hiba (valódi véletlen nem véletlennek minősítése) valószínűsége 1%. Természetesen a véletlenné minősítésre nincs semmilyen felső korlát —sőt az sem egyértelmű, milyen valószínűségi mértéket kéne használunk—, tehát egy (a tesztelt tulajdonság szempontjából) nagyon jó pszeudovéletlen generátort minimális eséllyel buktat le. Sőt készíthetünk kifejezetten a tesztelt tulajdonságra szabott generátort is (mely más szempontok alapján akár bőven megbukhatna), erre 100% is lehet a másodfajú hiba valószínűség, azaz biztosan valódi véletlennek tippelné a teszt. Ebből is látszik, hogy ezek a tesztek semmiféle értelemben bizonyítják a sorozat „véletlenségét” — melyet egyébként nem is definiálunk. Az azonban

igaz, hogy az elsőfajú hibakorlátot növelve a másodfajú hibáknak csak egy valódi részhalmazát tartjuk meg. Általában azonban elfogadjuk véletlennek azokat, melyek ezeken a teszteken átmennek.

Ezek a tesztek nagyon gyakorlatiasak: a pszeudovéletlen generátorok tipikus és kihasználható „hibáira” fejlesztették ki, gyors futási idővel. Vannak tesztek, amik csak paraméterezésükben különböznek, úgy tűnhet, elég az egyiket (erősebbet) lefuttatni: a szerzők azonban ún. kétmintás Kolmogorov–Szmirnov-próbával (t-próba) szűrték ki a túlzottan korreláló teszteket.

Bár a bitek szokásos jelölése 0 és 1, most egyszerűbb képletekhez jutunk, ha ± 1-ekként gondolunk a bitekre. Mint előrevetítettük, nem csak eldönteni szeretnénk, hogy egy sorozat véletlen-e vagy sem, hanem (a P érték segítségével) mérni a véletlenségét.

A rács és a sorozat közti lényegi különbség az egyes elemek egymástól vett távolsága. Ha egy sorozat teszt ezt nem használja ki (tehát nem számít, hanyadik az adott elem, csak az egyes elemek darabszáma) az általánosítás automatikus. A NIST ezt a tesztet Gyakoriság teszt néven vezeti be[14].

Gyakoriság teszt:

Leírás

Adott egy $e_1, e_2, \ldots, e_n$ ± 1 bitsorozat, kérdés, mennyivel tér el a bitek száma. Ha ez az eltérés „túl nagy”, a sorozatot egy rossz minőségű véletlen szám generátor eredményének tekintjük, nem pedig valódi véletlen sorozatnak. Mivel egy valódi véletlen sorozatban a $+1$ és -1 bitek egyenlő gyakorisággal érkeznek a sorozat elemeinek összegének várható értéke 0, szórása $\sqrt{n}$.

Várható érték

$$\mathrm{E}\left(\sum_{i=1}^{n} e_i\right) = 0$$

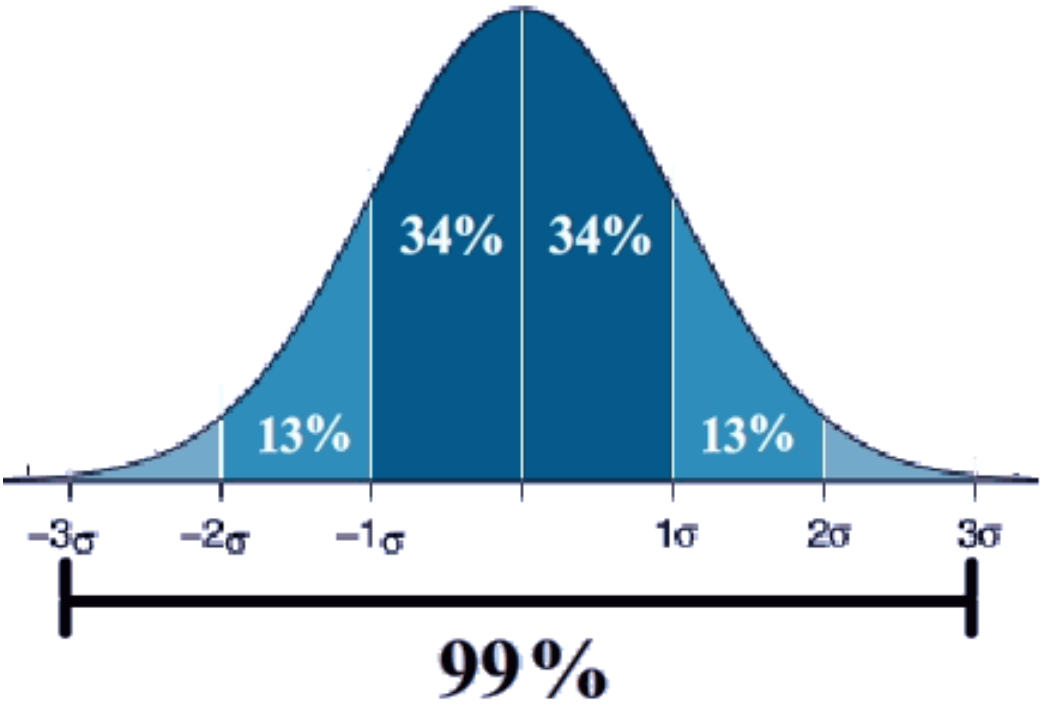
Szórás

$$\mathrm{D}\left(\sum_{i=1}^{n} e_i\right) = \sqrt{n}$$

Hosszabb bitsorozatokban várható értékben nyilván nagyobb számot kapunk, ezért normálni fogunk a bitek összegének szórásával — ezt az értéket fogjuk tesztstatisztikaként használni.

$$\frac{\sum e_i}{\sum e_i^2 - 0^2} = \frac{\sum e_i}{\sqrt{n}}$$

Mint véletlen bolyongást felfogva, a bitek összegének eloszlása a jól ismert haranggörbét adja.



Statisztikában szokásos módon, ha a kapott érték a „háromszoros szóráson” túl helyezkedik el — pontosabban a haranggörbe alatti terület legkülső 1%-ában —, túl valószínűtlennek tartjuk, hogy a sorozat valódi véletlen eloszlásból származzon, és nem tekintjük véletlennek. Tudjuk, hogy valódi véletlen sorozat esetén a sorozat elemeinek összegének várható értéke 0, szórása $\sqrt{n}$, ahol n az elemszám.

A tesztstatisztika a ± 1-ek normálva a szórással, azaz

Tesztstatisztika

$$\frac{E}{D} = \frac{\sum e_i}{\sqrt{n}}$$

P-érték

$$\frac{2}{\sqrt{\pi}} \int\limits_{\frac{\sum e_i}{\sqrt{n}}}^{\infty} e^{-u^2} \mathrm{d}u$$

Ez a P-érték mutatja meg, mennyi annak az esélye, hogy a ± 1-ek összege (abszolút értékben) legalább ilyen magas legyen véletlen inputra.

Példa

Input:

$$1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1$$

Elemek összege:

$$\sum e_i = 2$$

Elemek száma:

$$n = 14$$

Várható érték:

$$0$$

Szórás:

$$\sqrt{14}$$

Tesztstatisztika:

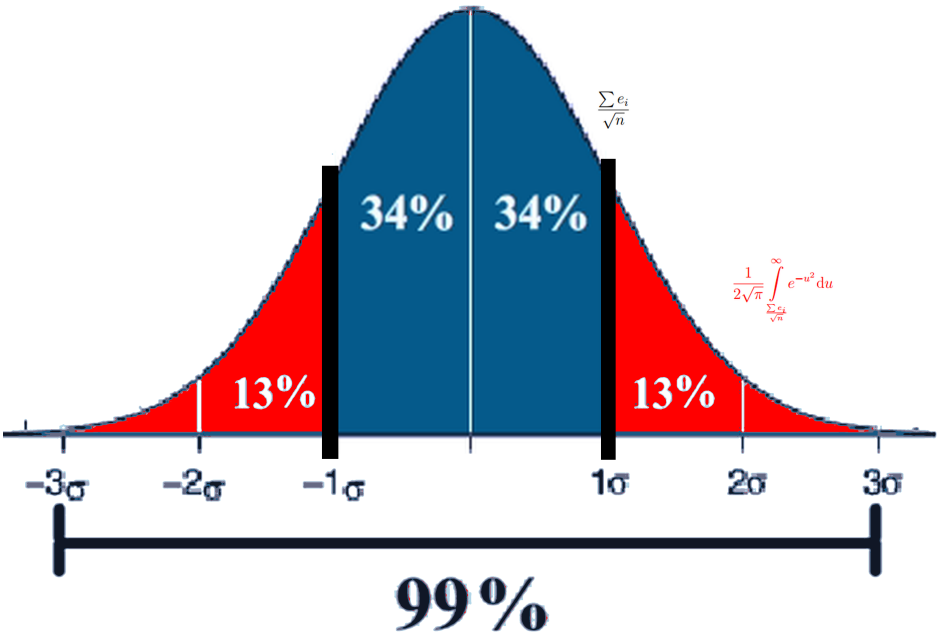
$$\frac{\sum e_i}{\sqrt{n}} = \frac{2}{\sqrt{14}} \approx 0,5345$$

P-érték:

$$\frac{2}{\sqrt{\pi}} \int\limits_{\frac{\sum e_i}{\sqrt{n}}}^{\infty} e^{-u^2} \mathrm{d}u = 0,3985$$

Következtetés:

A P-érték nagyobb 1%-nál, tehát az ennél szélsőségesebb összegű bitsorozatok ennél nagyobb részét (40%-át) adják a haranggörbének, a sorozatot véletlennek tekintjük.



Alkalmazási feltétel

Legalább 100 elemű mintára alkalmazzuk. $n \geq 100$

Gyakoriság teszt rácsokra:

Leírás

Adott egy

$$\begin{array}{ccccc} e_{n,1} & & & & e_{n,n} \\ \vdots & & & \iddots & \\ e_{3,1} & e_{3,2} & e_{3,3} & & \\ e_{2,1} & e_{2,2} & e_{2,3} & & \\ e_{1,1} & e_{1,2} & e_{1,3} & \cdots & e_{1,n} \end{array}$$

rács + és − bitekkel. Vizsgáljuk meg a + és − bitek különbségének és ezen különbség szórásának arányát. Ha ez az érték 3-nál nagyobb,

$$\frac{\sum\limits_{\substack{i=1\ldots n \\ j=1\ldots n}} e_i}{n} > 3,$$

a sorozatot nem tekintjük véletlennek, pontosabban, ha

$$\frac{2}{\sqrt{\pi}} \int\limits_{\frac{\sum e_i}{n}}^{\infty} e^{-u^2} \mathrm{d}u < 1\%.$$

Várható érték

$$\mathrm{E}\left(\sum_{i=1}^{n^2} e_i\right) = 0$$

Szórás

$$\mathrm{D}\left(\sum_{i=1}^{n^2} e_i\right) = n$$

Tesztstatisztika

$$\frac{\sum e_i}{n}$$

P-érték

$$\frac{2}{\sqrt{\pi}} \int\limits_{\frac{\sum e_i}{n}}^{\infty} e^{-u^2} \mathrm{d}u$$

Ez a P-érték mutatja meg, mennyi annak az esélye, hogy a ± 1-ek összege (abszolút értékben) legalább ilyen magas legyen véletlen inputra.

Példa

Input:

$$\begin{array}{ccccc} + & - & - & + & - \\ + & + & + & - & - \\ - & + & + & - & - \\ - & - & + & - & + \\ + & + & - & + & + \end{array}$$

Elemek összege:

$$\sum e_i = 1$$

Elemek száma:

$$n^2 = 25$$

Várható érték:

$$0$$

Szórás:

$$\mathrm{D} = 5$$

Tesztstatisztika:

$$\frac{\sum e_i}{n} = \frac{1}{25} = 0,04$$

P-érték:

$$\frac{2}{\sqrt{\pi}} \int\limits_{0,04}^{\infty} e^{-u^2} \mathrm{d}u = 0,9545$$

Következtetés:

A P-érték nagyobb 1%-nál, tehát a $0,04$-szeres szórásnál nagyobb különbséget adó rácsok az összes lehetséges rácsnak több mint 1%-át (95%-át) adják, ezért ezt a rácsot véletlennek tekintjük.

Alkalmazási feltétel

Legalább 100 elemű mintára alkalmazzuk. $n \geq 10$

Futam

Egy bitsorozatban futamnak nevezzük a legbővebb egymást követő egyforma biteket tartalmazó részsorozatokat, például

$$e_1 = 1, e_2 = 1, e_3 = 0, e_4 = 1, e_5 = 0$$

esetén a 3 futam:

e_1, e_2, e_3 3 hosszú egyes futam,

e_4 1 hosszú nullás futam,

e_5 1 hosszú egyes futam.

1101100010001000011111001010101

A NIST[13] 2 futam tesztje felteszi, hogy a sorozat átment a gyakoriság teszten. Ha bukja a gyakoriság tesztet (az ottani P érték $< 1\%$), a futamhossz teszt P értékét 0-nak definiálja. Ezt a konvenciót ne alkalmazzuk, ha nem eldönteni szeretnénk egy sorozatról, hogy véletlen-e vagy sem, hanem mérni szeretnénk a véletlenségét.

Bár egy véletlen sorozatban várható értékben a ± 1 bitek összege 0, most csak az S összegű sorozatokkal foglalkozunk. Eszerint a futamhosszak számának várható értéke $\frac{2}{n}(S+n)(S-n)+1$. Az egyszerűség kedvéért a futamok száma -1-gyel dolgozunk.

A fenti képen jól látszik, a futamok száma -1, a piros-sárga színátmenetek számával egyezik meg.

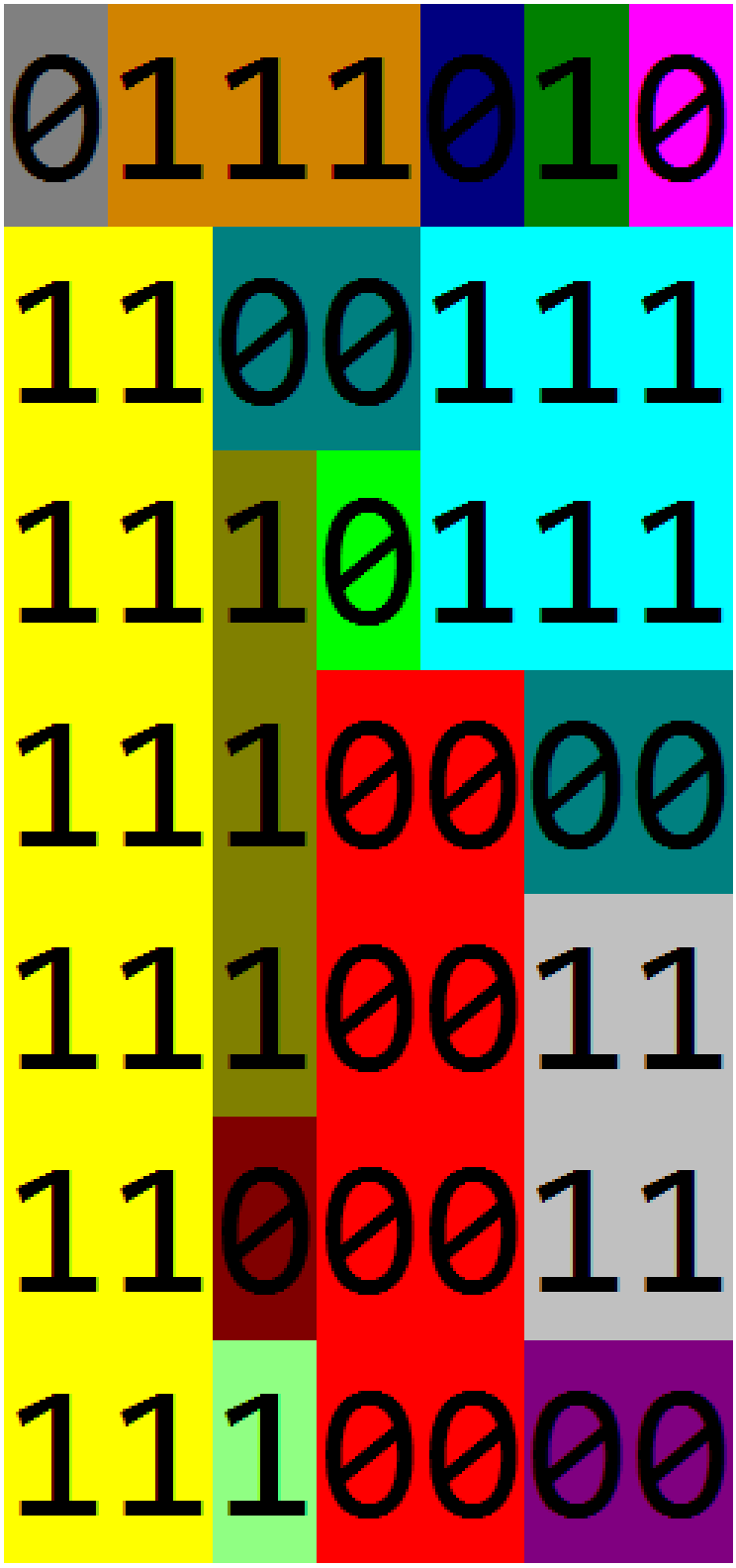
A Futam tesztben szeretnénk meghatározni, az inputban a bitek összegének várható értéke 0-e, azaz a ± 1-ek előfordulási esélye 50-50%-e. Erről önmagában a tapasztalati várható értékből nem következtethetünk: az tipikusan valamennyire el fog térni a 0-től. Ha csak kicsit tér el, az még nyilván belefér a véletlenbe, de ha nagyon, akkor már nem fogjuk véletlennek tekinteni. A „kicsi” viszont nem függhet az általunk elképzelt várható értéktől (mit is neveznénk a 0-hoz képest kicsinek vagy nagynak); a „kicsit” az ugyanilyen hosszú sorozatoknál „szokásoshoz” képest kell érteni, ennek függvényében kell a 0-tól vett eltérést meghatározni. Emlékeztetünk: a várható értéket szeretnénk becsülni (pontosabban azt, hogy 0-e vagy sem). Akár valódi véletlen, akár nem, akár 0 várható értékű akár nem, használhatjuk a szórás becslésére vonatkozó képletet (mely feltételezi, hogy 0 várható értékű inputot kap). Ha a becslésként kapott szórás valószínűtlenül magas, akkor arra következtethetünk, nem egy valódi véletlen sorozatról van szó, ami (nagyon kis eséllyel) mutathat ilyen magas empirikus szórást, hanem az input bitek egy nem 0 várható értékű sorozatokat generáló pszeudovéletlen generátorból származnak. Azonban ahhoz, hogy szórást tudjunk becsülni, több „mérésre”, több várható érték becslésre is szükségünk van, de csak egy input sorozat áll rendelkezé-

sünkre. Ezt úgy érjük el, hogy az inputot blokkokra osztjuk, és mindegyikben összeadjuk a biteket (± 1-eket).

Ha rácsokra szeretnénk általánosítani ezeket a teszteket, szükségünk van rácsokon értelmezett futamokra. Nevezzük futamnak a tovább nem bővíthető egyforma biteket tartalmazó összefüggő téglalapokat, azaz

$$\begin{aligned} &\text{nullás futam:} && \{((i_1, j_1), (i_2, j_2)) \mid (i, j) = 0 \ \forall i_1 \leq i \leq i_2 \forall j_1 \leq j \leq j_2\} \\ &\text{egyes futam:} && \{((i_1, j_1), (i_2, j_2)) \mid (i, j) = 0 \ \forall i_1 \leq i \leq i_2 \forall j_1 \leq j \leq j_2\} \end{aligned}$$

Az alábbi képen látható egy 7×7-es rács a 16 futam egy lehetséges ábrázolásával. Maguk a futamok nem meghatározottak egyértelműen, mégis használhatjuk ezt a definíciót. Vegyük a rács összes lehetséges felosztását futamokra, és vegyük az összes felosztás közül azt, melyben a futamok száma minimális. Ez a szám, a minimumérték, már egyértelműen definiált az adott rácsra.


0111010
1100111
1110111
1110000
1110011
1100011
1110000

Futam teszt:

Leírás

Számoljuk le, hány futam van a sorozatunkban. Vegyük észre ez éppen eggyel kevesebb a különböző egymás utáni bitpárok számánál, azaz azon i indexek számánál, melyre

$$e_i \neq e_{i+1}.$$

Definiáljuk a bitsorozatra $r(i)$ függvényt $i = 1 \ldots n-1$ értelmezési tartományon a következőképp:

$$r(i) = \begin{cases} 0 & \text{,ha } e_i = e_{i+1} \\ 1 & \text{,ha } e_i \neq e_{i+1} \end{cases}$$

Jelölje X a futamok számát, ekkor

$$X = \sum_{i=1}^{n-1} r(i).$$

Jelölje a az egyesek arányát, b a nullákét. Mivel a futam tesztet eleve csak olyan bitsorozatokon értelmezzük, melyek átmennek a gyakoriság teszten, ezért

$$\left| a - \frac{1}{2} \right| \sqrt{n} < 3$$

feltételnek biztosan teljesülnie kell. Hogy kiszámíthassuk a tesztstatisztikát, számítsuk ki X várható értékét és szórását.

Várható érték

$$E = 2nab$$

Szórás

$$D = 2\sqrt{2n}ab$$

Tesztstatisztika

$$\frac{|X - E|}{D} = \frac{|X - 2nab|}{2\sqrt{2n}ab}$$

P-érték

$$\frac{2}{\sqrt{\pi}} \int\limits_{\frac{|X-2nab|}{2\sqrt{2n}ab}}^{\infty} e^{-u^2} \mathrm{d}u$$

Példa

Input: (e_i)

$$1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1$$

Különböző elempárok: (r_i)

$$1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0$$

Különböző elempárok száma (elemek összege r_i-ben):

$$X = \sum r_i = 8$$

Futamok száma:

$$1 + \sum r_i = 7$$

Elemek száma:

$$n = 15$$

1**-esek száma:** (π)

$$\pi = \sum_{i=1}^{n} e_i = 8$$

0**-ások száma:**

$$n - \pi = 7$$

1**-esek aránya:** (a)

$$a = \frac{8}{15} \approx 0,53$$

0**-ások aránya:** (b)

$$b = \frac{7}{15} \approx 0,47$$

Futamok számának várható értéke:

$$\mathrm{E} = 2nab \approx 7,47$$

Szórás:

$$\mathrm{D} = 2\sqrt{2n}ab \approx 2,73$$

Tesztstatisztika:

$$\frac{X - 2nab}{2\sqrt{2n}ab} \approx 0,19$$

P-érték:

$$\frac{2}{\sqrt{\pi}} \int\limits_{0,19}^{\infty} e^{-u^2} \mathrm{d}u = 0,79$$

Következtetés:

A P-érték nagyobb 1%-nál, tehát a $0,2$-szeres szórásnál nagyobb különbséget adó sorozatok az összes lehetséges rácsnak több mint 1%-át (95%-át) adják, ezért ezt a sorozatot véletlennek tekintjük.

$$\frac{8 - 7,47}{2,73} \approx 0,2$$

A kapott tesztstatisztika a szórás 20%-a.

Alkalmazási feltétel

Legalább 100 elemű mintára alkalmazzuk. $n \geq 100$

Alternatív futamteszt:

Ismét használjuk ki, hogy a futamok száma a különböző bitszomszédok számánál eggyel nagyobb, de most induljunk ki abból, hogy a $n-1$ lehetséges „szomszéd bit” várható értékben fele lesz „különböző”. Képletben:

$$\mathrm{P}\left(e_{i+1} \neq e_i\right) = 50\%$$

Emiatt könnyen látszik a különböző bitpárok várható értéke:

$$\frac{n-1}{2}$$

Melyből adódik a futamok számának várható értéke:

$$\frac{n+1}{2}$$

Az $n-1$ szomszéd bit értékével számoljunk 1-ként, ha különböző, 0-ként ha egyező, azaz

$$x_i := \begin{cases} 0 & \text{, ha } e_i = e_{i+1} \\ 1 & \text{, ha } e_i \neq e_{i+1} \end{cases}$$

Most legyen Δ_i 0 várható értékű,

$$\Delta_i := \begin{cases} -0.5 & \text{, ha } e_i = e_{i+1} \\ 0.5 & \text{, ha } e_i \neq e_{i+1} \end{cases}$$

Így az átlagtól vett négyzetes eltérés, maga Δ_i^2.

$$\Delta_i^2 \equiv \frac{1}{4}$$

Mint konstans függvénynek, ennek az átlaga is $\frac{1}{4}$, innen a szórás és szórásnégyzet:

$$\begin{aligned} \mathrm{D}^2\Delta_i^2 &= \frac{1}{4} \\ \mathrm{D}\Delta_i^2 &= \frac{1}{2} \end{aligned}$$

Tekintve, hogy

$$\mathrm{D}^2\left(\xi + c\right) = \mathrm{D}^2\xi$$

illetve

$$\mathrm{D}\left(\xi + c\right) = \mathrm{D}\xi$$

ezzel megkaptuk a különböző bitpárok számának és a futamok számának szórását is, hiszen mindezek egyenlők.

$$\mathrm{D} = \frac{1}{2}$$

Számoljuk le, hány futam van a sorozatunkban és vonjunk le belőle 1-et. Vegyük észre ez éppen 1+#két egymást követő különböző bit -1. Ez várható értékben $\frac{n-1}{2}$, szórása $\frac{1}{2}$. Ebből adódik a P érték

$$\frac{1}{2\sqrt{\pi}} \int_{n+1}^{\infty} e^{-u^2} \mathrm{d}u$$

ahol x a megfigyelt futamok számánál eggyel kevesebb.

Példa

Input: (e_i)

$$1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1$$

Különböző elempárok: (r_i)

$$0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0$$

Különböző elempárok száma (elemek összege r_i-ben):

$$\sum r_i = 6$$

Futamok száma:

$$X = 1 + \sum r_i = 7$$

Elemek száma:

$$n = 13$$

Futamok számának várható értéke:

$$\mathrm{E} = \frac{n+1}{2} = 7$$

Szórás:

$$\mathrm{D} = \frac{1}{2}\sqrt{n} \approx 1,8$$

Tesztstatisztika:

$$\frac{X-E}{D} = \frac{X - 1 - \sum\limits_{i=1}^{n} r_i}{\frac{1}{2}\sqrt{n}} = 0$$

P-érték:

$$\frac{2}{\sqrt{\pi}} \int\limits_0^\infty e^{-u^2} \mathrm{d}u = 1$$

Következtetés:

A kapott érték pontosan a várható érték. Ezt semmilyen elsőfajú hibakorlát mellett sem utasítjuk el, a sorozatot valódi véletlennek tekintjük.

Alkalmazási feltétel

Legalább 100 elemű mintára alkalmazzuk. $n \geq 100$

Futam teszt rácsokra:

Leírás

Adott egy

$$
\begin{array}{ccccc}
e_{n,1} & & & & e_{n,n} \\
\vdots & & & \iddots & \\
e_{3,1} & e_{3,2} & e_{3,3} & & \\
e_{2,1} & e_{2,2} & e_{2,3} & & \\
e_{1,1} & e_{1,2} & e_{1,3} & \cdots & e_{1,n}
\end{array}
$$

rács, és becsüljük meg benne a rácsokra általánosított futamok számát, azaz a csupa egyforma biteket tartalmazó téglalapokat. Másképp megfogalmazva: a kérdés, legalább hány darab csak 0 illetve 1 bitet tartalmazó téglalapra van szükségünk, hogy lefedjük a mátrixot. Formálisan:

$$t_i = \{a, a+1, \ldots, b\} \times \{c, c+1, \ldots, d\}$$

tengelypárhuzamos téglalapok, melyek bal alsó csúcsa $(a, c) \in \{1, \ldots, n\}^2$ jobb felső $(b, d) \in \{1, \ldots, n\}^2$

A fedő téglalapok száma k

$$
\begin{aligned}
t_1 &= \{a_1, a_1+1, \ldots, b_1\} \times \{c_1, c_1+1, \ldots, d_1\} \\
t_2 &= \{a_2, a_2+1, \ldots, b_2\} \times \{c_2, c_2+1, \ldots, d_2\} \\
\\
t_k &= \{a_k, a_k+1, \ldots, b_k\} \times \{c_k, c_k+1, \ldots, d_k\}
\end{aligned}
$$

továbbá ezen téglalapok csupa egyforma bitet tartalmaznak:

$$\forall 1 \leq i \leq k \forall (x,y), (z,w) \in t_i \; e_{x,y} = e_{z,w}$$

A rács minden eleme pontosan egyszeresen fedett, azaz

$$\forall (x,y) \in \{1,\ldots,n\}^2 \; \exists! 1 \leq i \leq k \;\; (x,y) \in t_i$$

A fedés pedig minimális, azaz

$$\nexists t'_1, \ldots, t'_{k'} \; k' < k$$

$$\begin{aligned} t'_1 &= \{a'_1, a'_1+1, \ldots, b'_1\} \times \{c'_1, c'_1+1, \ldots, d'_1\} \\ t'_2 &= \{a'_2, a'_2+1, \ldots, b'_2\} \times \{c'_2, c'_2+1, \ldots, d'_2\} \end{aligned}$$

$$t'_k = \{a'_k, a'_k+1, \ldots, b'_k\} \times \{c'_k, c'_k+1, \ldots, d'_k\}$$

$$\forall 1 \leq i \leq k' \forall (x,y), (z,w) \in t'_i \; e_{x,y} = e_{z,w}$$

$$\forall (x,y) \in \{1,\ldots,n\}^2 \; \exists! 1 \leq i \leq k' \;\; (x,y) \in t'_i$$

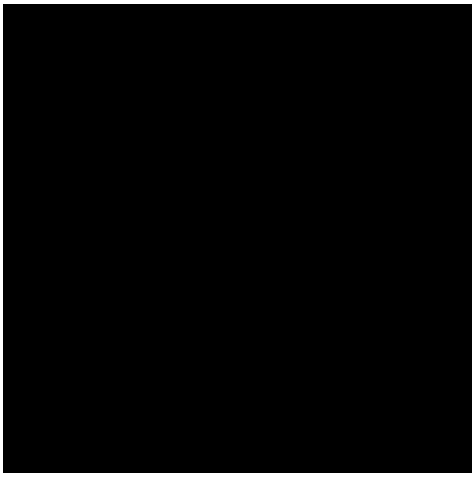
Ehhez elengedhetetlen, hogy maguk a fedő téglalapok maximálisak legyenek tartalmazásra nézve:

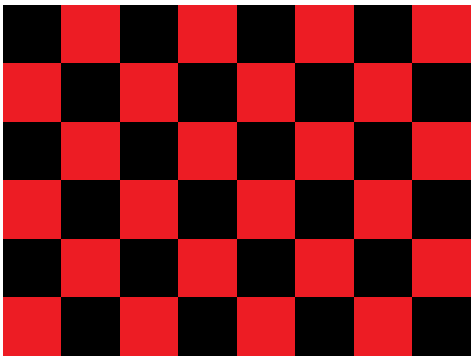
$$\forall i \nexists t' = \{a', a'+1, \ldots, b'\} \times \{c', c'+1, \ldots, d'\} \supsetneq t_i$$

$$\forall (x, y), (z, w) \in t' \; e_{x,y} = e_{z,w}$$

Eloszlás

A tesztstatisztikához szükségünk van a várható értékre és a szórásra; becsüljük meg egy $n \times k$-as független azonos eloszlású $\xi_{i,j}$ valószínűségi változókból származó bitekkel feltöltött rács futamainak számának (x) eloszlásfüggvényét. Szemléltetésül az szélsőséges esetek:





Egyetlen futam	$\mathrm{P}(x = 1) = \dfrac{2}{2^{nk}}$
nk futam	$\mathrm{P}(x = 1) = \dfrac{2}{2^{nk}}$

Az egy dimenziós (véletlen sorozat) tesztnél láttuk, hogy a futamok száma helyett a különböző bitpárok számát venni, így ugyanis eggyel kisebb elem-

számra vonatkozó binomiális eloszlást kapunk. Csakugyan: lerögzítjük az első bitet, a szomszédja pedig attól függően növeli a futamok számát vagy sem, hogy ugyanaz-e, mint az utolsó bit; ezt fejezi ki a különböző bit pár tulajdonság. Ebből adódik azonban a becslés hibája is.

1 futam	2 futam	3 futam	4 futam	5 futam	
1					-féleképpen fordulhat elő $n = 1$-re
1	1				-féleképpen fordulhat elő $n = 2$-re
1	2	1			-féleképpen fordulhat elő $n = 3$-re
1	3	3	1		-féleképpen fordulhat elő $n = 4$-re
1	4	6	4	1	-féleképpen fordulhat elő $n = 5$-re

n elemre $k + 1$ futam tehát

$$\binom{n}{k}$$

-féleképpen fordulhat elő, ami

$$\mathrm{P}\,(n \text{ elem}, k \text{ futam}) = \frac{\binom{n}{k}}{2^n}$$

valószínűséget jelent.

Ismerjük fel a Pascal-háromszöget: attól függően, hogy az új bit növeli-e a futamok számát vagy sem, adódik hozzá az alatta lévő (ugyanannyi futam), vagy a jobb alsó szomszédjához (eggyel több futam).

Ha megszorítanánk, hogy az $n \times k$-as rácsban csak 1 magasságú téglalapokkal fedünk, k darab binomiális eloszlás összegét kapnánk. Ez ismét binomiális eloszlású lenne.

$$\begin{aligned} X_i &\sim B(n, 50\%) \\ \sum X_i &\sim kB(n, 50\%) \\ \sum X_i &\sim B(kn, 50\%) \end{aligned}$$

Vegyük észre, hogy egy $n \times k$-as és egy $n \times 1$-es rács egyesítése után a futamok száma akkor és csak akkor csökken az összeghez képest, ha az $n \times k$-as rács érintkező $n \times 1$-es rácsában és az egyesítendő $n \times 1$-es rácsban van egy-egy egyforma futam pont egymás alatt. Tehát például

1	0	**1**	0	1	1
0	0	**1**	0	0	0

Ebben a 6×2-es rácsban 7 futam van, ami eggyel kevesebb, mint a felső 6×1-esben található 5 futam és az alsóban található 3-é, hiszen pontosan egy olyan futam van, ami ugyanabból a bitből áll, ugyanannyiadik helyen kezdődik és fejeződik be mindkét rácsban.

Az alábbi ellenpéldákban látszik, hogy csak ezekben az esetekben csökken a futamok száma.

1	1	**0**	**0**	1	1
1	0	**1**	**1**	0	1

1	1	1	0	**1**	**1**
1	**1**	0	0	0	0

1	1	1	0	**1**	**1**
1	1	0	1	**1**	**1**

1	1	**0**	**0**	1	1
0	0	0	0	0	0
0	1	**0**	**0**	1	1

Ha az új $n \times 1$-es rács éppen megegyezik az alatta levő $n \times 1$-essel, akkor az új rács minden futamára kiterjeszthetjük a régi futamait. Ekkor a futamok száma annyi lesz, mint a régi $n \times k$-asban, ez azt jelenti, hogy az összeg akár az új $n \times 1$-esben lévő összes futam számával is csökkenhet.

0	**1**	**1**	**0**	**0**	**0**
0	**1**	**1**	**0**	**0**	**0**
1	1	1	1	1	1

Nyilvánvalóan nem lehet kevesebb a futamok száma az egyesített $n \times k + 1$-es rácsban, mint bármelyik részében. Általában igaz tehát, hogy ha A összefüggő $n' \times k'$ részrácsa B $n \times k$-as rácsnak, akkor A-ban nem lehet több futam, mint B-ben, azaz

$$A \preceq B \Rightarrow \#\text{futam}\,(A) \leq \#\text{futam}\,(B)$$

Indukcióval tegyük fel, a $n \times k$-as rácsokon már ismerjük a futamok számának eloszlását, azaz a

futam#	1	2	...	nk
darab#	2	$2n^2k^2$	...	2

függvényt, és az $(n+1) \times k$-as rács futamainak számára vagyunk kíváncsiak (ugyanez a módszer működne az $n \times (k+1)$-asra is).

Tekintsük az alábbi rácsot

0	1	1	0	1
0	1	1	0	1
1	0	1	1	1
0	1	0	0	0
0	0	1	1	1

Alakítsuk ezt át a következő formára:

- Az első elemet hagyjuk meg
- Az első oszlopban (az első elemet kivéve) írjunk - jelet (vízszintes fal), ha nem egyezik meg az alatta levő bittel, hagyjuk üresen egyébként
- A többi sorban írjunk | jelet (függőleges fal), ha nem egyezik meg a tőle balra levő bittel, hagyjuk üresen egyébként

Így az alábbi átalakított rácshoz jutunk

	|		|	|
-	|		|	|
-	|	|		
	|	|		
0		|		

Használjuk az indukciós feltevést, hogy a $(n-1) \times k$-as rácsokon már ismerjük a futamok számának eloszlását, tehát ha az $n \times k$-as rácsok futamainak számának eloszlására vagyunk kíváncsiak, derítsük ki, hogyan változik az eloszlás az n-edik sor hozzávételével. Jelen példában a futamok számának változásában csak a nem *-ozott elemek játszanak szerepet

	|		|	|
*	|		|	|
*	*	*	*	*
*	*	*	*	*
*	*	*	*	*

Oszloponként haladva határozzuk meg, hány új futam keletkezik. Az első oszlop különleges, itt

+0	+1
	-

A többi oszlopot már négy lehetséges módon tölthetjük ki:

+0	+0	?	+1
	|		|
	|	|	

A ? eset általában +0-nak számít, kivéve, ha éppen ez az első különbség az alsó és a felső futam között, azaz

|		|			|			
|	|	|		|	|			|

...

*	|	*		|	*			|

...

-		-			-			
*	|	*		|	*			|

...

Így a második oszlop is kivételes: itt a ? egyértelmű:

+0	+0	+1	+1
	|		|
	|	|	

Az i-edik oszlopban pedig ?

$$\left(\frac{1}{4}\right)^{i-2} + \frac{1}{4} + \left(\frac{1}{4}\right)^{2} + \left(\frac{1}{4}\right)^{3} + \cdots + \left(\frac{1}{4}\right)^{i-2}$$

Erre alkalmazva a mértani sor összegképletét

$$\left(\frac{1}{4}\right)^{i-2} + \frac{1}{4}\frac{\left(\frac{1}{4}\right)^{i-2} - 1}{\frac{1}{4} - 1}$$

Egyszerűsítve

$$\frac{1}{3} - 2\left(\frac{1}{4}\right)^{i-3}$$

Hangsúlyozzuk (ami a képletből is látszik):

$$i \geq 3$$

Összegezzük mindezt:

- Az új sor első mezejébe írt bit x_1 :=50% eséllyel növeli a futamok számát
- A második mezőbe szintén x_2 :=50%-kal

- Innentől kezdve viszont csak

$$
\begin{aligned}
x_i : &= \frac{1}{3} - 2\left(\frac{1}{4}\right)^{i-3} \\
y_i &:= 1 - x_i = \frac{2}{3} + 2\left(\frac{1}{4}\right)^{i-3}
\end{aligned}
$$

$x_3 = 50\%$ továbbra is, de $i > 3$-ra $x_i < 50\%$.

Így adódik, hogy a k hosszú új sor hozzávétele a futamok számát az alábbi eloszlás szerint növeli

	$+0$	$+1$	$+2$	$\sum$
$+0$	$\prod_{i=3}^{k} y_i$	0	0	$\frac{1}{4}\prod_{i=3}^{k} y_i$
$+1$	$\sum_{i_1=3}^{k} x_{i_1} \prod_{\substack{i=3 \\ i\neq i_1}}^{k} y_i$	$\prod_{i=3}^{k} y_i$	0	$\frac{1}{4}\sum_{i_1=3}^{k} x_{i_1} \prod_{\substack{i=3 \\ i\neq i_1}}^{k} y_i + \frac{1}{2}\prod_{i=3}^{k} y_i$
$+2$	$\vdots$	$\sum_{i_1=1}^{k} x_{i_1} \prod_{\substack{i=1 \\ i\neq i_1}}^{k} y_i$	$\prod_{i=1}^{k} y_i$	$\vdots$
$+3$	$\vdots$	$\vdots$	$\sum_{i_1=1}^{k} x_{i_1} \prod_{\substack{i=1 \\ i\neq i_1}}^{k} y_i$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$+k-2$	$\prod_{i=3}^{k} x_i$	$\vdots$	$\vdots$	$\vdots$
$+k-1$	0	$\prod_{i=3}^{k} x_i$	$\vdots$	$\vdots$
$+k$	0	0	$\prod_{i=3}^{k} x_i$	$\frac{1}{4}\prod_{i=3}^{k} x_i$

Táblázatok

Ding, Helleseth és Shan megmutatta[16], hogy

$$s_i = \begin{cases} \left[\frac{1+\left(\frac{i}{p}\right)}{2}\right] & \text{,ha } p \nmid i \\ 0 & \text{,ha } p \mid i \end{cases}$$

végtelen 0-1 sorozat ($i \geq 0$) lineáris komplexitása:

$p \equiv -1$	mod 8	$\frac{p+1}{2}$
$p \equiv 1$	mod 8	$\frac{p-1}{2}$
$p \equiv 3$	mod 8	p
$p \equiv -3$	mod 8	$p-1$

Ha csak az első néhány (n) elemét vizsgáltam a fenti (s_i) sorozatnak, p mod 8 értékétől függetlenül nagyjából $\frac{n}{2}$ lineáris komplexitás adódott.

Az alábbi táblázatok a modulo p kvadratikus maradékokon alapuló n elemű pszeudovéletlen sorozatok lineáris komplexitását elemzik. Ezek a sorozatok

$$\left(\frac{f(1)}{p}\right), \left(\frac{f(2)}{p}\right), \left(\frac{f(3)}{p}\right), \ldots, \left(\frac{f(n)}{p}\right)$$

valamilyen f polinom pozitív egész helyeken felvett értékeinek Legendre-szimbóluma modulo egy p prímszám. Megjegyzés: valójában

$0-1$-ekre kódoljuk át a Legendre szimbólumokat, és ha $p \mid f(i)$ adódna, úgy a Legendre-szimbólumot helyettesítjük 1-gyel.

A táblázatokban a lineáris komplexitás $\left\lfloor \frac{n}{2} \right\rfloor$-től vett különbséget adjuk meg (S-sel jelölve).

Ha f az identitás, az első néhány 100-nál nagyobb p prímre az így elkészített $p-1$ elemű sorozatok nagyon jó pszeudovéletlen tulajdonságot mutatnak:

p	$f(x)$	n	S
101	x	100	0
103	x	102	1
107	x	106	1
109	x	108	1
113	x	112	0
127	x	126	1
131	x	130	1
137	x	136	0
139	x	138	1
149	x	148	1
151	x	150	1
157	x	156	1
163	x	162	1
167	x	166	1
173	x	172	1
179	x	178	1
181	x	180	1
191	x	190	1
193	x	192	0
197	x	196	0
199	x	198	1

p	$f(x)$	n	S
211	x	210	1
223	x	222	1
227	x	226	1
229	x	228	0
233	x	232	0
239	x	238	1
241	x	240	0
251	x	250	1
257	x	256	0
263	x	262	1
269	x	268	0
271	x	270	1
277	x	276	1
281	x	280	0
283	x	282	1
293	x	292	1

p	$f(x)$	n	S
307	x	306	1
311	x	310	1
313	x	312	0
317	x	316	1
331	x	330	1
337	x	336	0
347	x	346	1
349	x	348	0
353	x	352	0
359	x	358	1
367	x	366	1
373	x	372	0
379	x	378	1
383	x	382	1
389	x	388	0
397	x	396	0

p	$f(x)$	n	S
401	x	400	0
409	x	408	0
419	x	418	1
421	x	420	0
431	x	430	1
433	x	432	0
439	x	438	1
443	x	442	1
449	x	448	0
457	x	456	0
461	x	460	1
463	x	462	1
467	x	466	1
479	x	478	1
487	x	486	1
491	x	490	1
499	x	498	1

p	$f(x)$	n	S
503	x	502	1
509	x	508	1
521	x	520	0
523	x	522	1
541	x	540	1
547	x	546	1
557	x	556	0
563	x	562	1
569	x	568	0
571	x	570	1
577	x	576	0
587	x	586	1
593	x	592	0
599	x	598	1

p	$f(x)$	n	S
601	x	600	0
607	x	606	1
613	x	612	0
617	x	616	0
619	x	618	1

Kezdőszeletek lineáris komplexitása kevésbé pontosan, de lényegében szintén $\frac{n}{2}$. Modulo 101 vizsgáltuk az x^2+1 polinommal generált $1, 2, 3, \ldots, 100$ hosszú sorozatok lineáris komplexitását.

p	$f(x)$	n	S
101	x^2+1	1	0
101	x^2+1	2	-1
101	x^2+1	3	1
101	x^2+1	4	-2
101	x^2+1	5	0
101	x^2+1	6	-3
101	x^2+1	7	-1
101	x^2+1	8	-4
101	x^2+1	9	-2
101	x^2+1	10	-5
101	x^2+1	11	3
101	x^2+1	12	-6
101	x^2+1	13	2
101	x^2+1	14	6
101	x^2+1	15	1
101	x^2+1	16	5
101	x^2+1	17	0
101	x^2+1	18	4
101	x^2+1	19	1
101	x^2+1	20	3

p	$f(x)$	n	S
101	x^2+1	21	0
101	x^2+1	22	2
101	x^2+1	23	-1
101	x^2+1	24	1
101	x^2+1	25	-2
101	x^2+1	26	0
101	x^2+1	27	-3
101	x^2+1	28	-1
101	x^2+1	29	-4
101	x^2+1	30	1
101	x^2+1	31	5
101	x^2+1	32	0
101	x^2+1	33	4
101	x^2+1	34	0
101	x^2+1	35	3
101	x^2+1	36	-1
101	x^2+1	37	2
101	x^2+1	38	1
101	x^2+1	39	1
101	x^2+1	40	0

p	$f(x)$	n	S
101	x^2+1	41	0
101	x^2+1	42	-1
101	x^2+1	43	1
101	x^2+1	44	1
101	x^2+1	45	0
101	x^2+1	46	0
101	x^2+1	47	1
101	x^2+1	48	0
101	x^2+1	49	0
101	x^2+1	50	0
101	x^2+1	51	1
101	x^2+1	52	-1
101	x^2+1	53	0
101	x^2+1	54	-2
101	x^2+1	55	-1
101	x^2+1	56	-3
101	x^2+1	57	2
101	x^2+1	58	3
101	x^2+1	59	1
101	x^2+1	60	2

p	$f(x)$	n	S
101	x^2+1	61	0
101	x^2+1	62	1
101	x^2+1	63	-1
101	x^2+1	64	0
101	x^2+1	65	-2
101	x^2+1	66	0
101	x^2+1	67	-3
101	x^2+1	68	0
101	x^2+1	69	4
101	x^2+1	70	-1
101	x^2+1	71	3
101	x^2+1	72	1
101	x^2+1	73	2
101	x^2+1	74	0
101	x^2+1	75	1
101	x^2+1	76	0
101	x^2+1	77	0
101	x^2+1	78	0
101	x^2+1	79	1
101	x^2+1	80	-1

p	$f(x)$	n	S
101	x^2+1	81	0
101	x^2+1	82	-2
101	x^2+1	83	1
101	x^2+1	84	-3
101	x^2+1	85	0
101	x^2+1	86	-4
101	x^2+1	87	-1
101	x^2+1	88	-5
101	x^2+1	89	-2
101	x^2+1	90	5
101	x^2+1	91	-3
101	x^2+1	92	4
101	x^2+1	93	-4
101	x^2+1	94	3
101	x^2+1	95	5
101	x^2+1	96	2
101	x^2+1	97	4
101	x^2+1	98	1
101	x^2+1	99	3
101	x^2+1	100	0

$f(x)$-nek van többszörös gyöke (de nem teljes négyzet)

p	$f(x)$	n	S
101	x^3+2x^2+x	1	0
101	x^3+2x^2+x	2	-1
101	x^3+2x^2+x	3	-1
101	x^3+2x^2+x	4	1
101	x^3+2x^2+x	5	2
101	x^3+2x^2+x	6	0
101	x^3+2x^2+x	7	1
101	x^3+2x^2+x	8	-1
101	x^3+2x^2+x	9	0
101	x^3+2x^2+x	10	1
101	x^3+2x^2+x	11	-1
101	x^3+2x^2+x	12	0
101	x^3+2x^2+x	13	-2
101	x^3+2x^2+x	14	-1
101	x^3+2x^2+x	15	-3
101	x^3+2x^2+x	16	-2
101	x^3+2x^2+x	17	-4
101	x^3+2x^2+x	18	2
101	x^3+2x^2+x	19	-5
101	x^3+2x^2+x	20	1

p	$f(x)$	n	S
101	x^3+2x^2+x	21	6
101	x^3+2x^2+x	22	0
101	x^3+2x^2+x	23	5
101	x^3+2x^2+x	24	0
101	x^3+2x^2+x	25	4
101	x^3+2x^2+x	26	0
101	x^3+2x^2+x	27	3
101	x^3+2x^2+x	28	0
101	x^3+2x^2+x	29	2
101	x^3+2x^2+x	30	-1
101	x^3+2x^2+x	31	1
101	x^3+2x^2+x	32	-2
101	x^3+2x^2+x	33	0
101	x^3+2x^2+x	34	2
101	x^3+2x^2+x	35	-1
101	x^3+2x^2+x	36	1
101	x^3+2x^2+x	37	-2
101	x^3+2x^2+x	38	0
101	x^3+2x^2+x	39	-3
101	x^3+2x^2+x	40	0

p	$f(x)$	n	S
101	x^3+2x^2+x	41	4
101	x^3+2x^2+x	42	0
101	x^3+2x^2+x	43	3
101	x^3+2x^2+x	44	0
101	x^3+2x^2+x	45	2
101	x^3+2x^2+x	46	-1
101	x^3+2x^2+x	47	1
101	x^3+2x^2+x	48	1
101	x^3+2x^2+x	49	0
101	x^3+2x^2+x	50	0
101	x^3+2x^2+x	51	1
101	x^3+2x^2+x	52	-1
101	x^3+2x^2+x	53	0
101	x^3+2x^2+x	54	1
101	x^3+2x^2+x	55	-1
101	x^3+2x^2+x	56	0
101	x^3+2x^2+x	57	-2
101	x^3+2x^2+x	58	-1
101	x^3+2x^2+x	59	-3
101	x^3+2x^2+x	60	-2

p	$f(x)$	n	S
101	x^3+2x^2+x	61	-4
101	x^3+2x^2+x	62	2
101	x^3+2x^2+x	63	-5
101	x^3+2x^2+x	64	1
101	x^3+2x^2+x	65	6
101	x^3+2x^2+x	66	0
101	x^3+2x^2+x	67	5
101	x^3+2x^2+x	68	-1
101	x^3+2x^2+x	69	4
101	x^3+2x^2+x	70	1
101	x^3+2x^2+x	71	3
101	x^3+2x^2+x	72	0
101	x^3+2x^2+x	73	2
101	x^3+2x^2+x	74	0
101	x^3+2x^2+x	75	1
101	x^3+2x^2+x	76	0
101	x^3+2x^2+x	77	0
101	x^3+2x^2+x	78	-1
101	x^3+2x^2+x	79	-1
101	x^3+2x^2+x	80	1

p	$f(x)$	n	S
101	$x^3 + 2x^2 + x$	81	-2
101	$x^3 + 2x^2 + x$	82	0
101	$x^3 + 2x^2 + x$	83	3
101	$x^3 + 2x^2 + x$	84	0
101	$x^3 + 2x^2 + x$	85	2
101	$x^3 + 2x^2 + x$	86	0
101	$x^3 + 2x^2 + x$	87	1
101	$x^3 + 2x^2 + x$	88	0
101	$x^3 + 2x^2 + x$	89	0
101	$x^3 + 2x^2 + x$	90	-1
101	$x^3 + 2x^2 + x$	91	-1
101	$x^3 + 2x^2 + x$	92	1
101	$x^3 + 2x^2 + x$	93	-2
101	$x^3 + 2x^2 + x$	94	0
101	$x^3 + 2x^2 + x$	95	-3
101	$x^3 + 2x^2 + x$	96	0
101	$x^3 + 2x^2 + x$	97	4
101	$x^3 + 2x^2 + x$	98	0
101	$x^3 + 2x^2 + x$	99	3
101	$x^3 + 2x^2 + x$	100	-1

2 nem primitív gyök modulo p, $f(x)$-nek van többszörös gyöke, mégis jó

p	$f(x)$	n	S
127	x^3+2x^2+x	1	0
127	x^3+2x^2+x	2	-1
127	x^3+2x^2+x	3	-1
127	x^3+2x^2+x	4	-2
127	x^3+2x^2+x	5	2
127	x^3+2x^2+x	6	-3
127	x^3+2x^2+x	7	1
127	x^3+2x^2+x	8	3
127	x^3+2x^2+x	9	0
127	x^3+2x^2+x	10	2
127	x^3+2x^2+x	11	1
127	x^3+2x^2+x	12	1
127	x^3+2x^2+x	13	0
127	x^3+2x^2+x	14	0
127	x^3+2x^2+x	15	1
127	x^3+2x^2+x	16	-1
127	x^3+2x^2+x	17	0
127	x^3+2x^2+x	18	-2
127	x^3+2x^2+x	19	-1
127	x^3+2x^2+x	20	-3

p	$f(x)$	n	S
127	x^3+2x^2+x	21	-2
127	x^3+2x^2+x	22	-4
127	x^3+2x^2+x	23	-3
127	x^3+2x^2+x	24	-5
127	x^3+2x^2+x	25	4
127	x^3+2x^2+x	26	-6
127	x^3+2x^2+x	27	3
127	x^3+2x^2+x	28	6
127	x^3+2x^2+x	29	2
127	x^3+2x^2+x	30	5
127	x^3+2x^2+x	31	1
127	x^3+2x^2+x	32	4
127	x^3+2x^2+x	33	0
127	x^3+2x^2+x	34	3
127	x^3+2x^2+x	35	-1
127	x^3+2x^2+x	36	2
127	x^3+2x^2+x	37	-2
127	x^3+2x^2+x	38	1
127	x^3+2x^2+x	39	-3
127	x^3+2x^2+x	40	0

p	$f(x)$	n	S
127	x^3+2x^2+x	41	-4
127	x^3+2x^2+x	42	-1
127	x^3+2x^2+x	43	-5
127	x^3+2x^2+x	44	-2
127	x^3+2x^2+x	45	6
127	x^3+2x^2+x	46	-3
127	x^3+2x^2+x	47	5
127	x^3+2x^2+x	48	-4
127	x^3+2x^2+x	49	4
127	x^3+2x^2+x	50	-5
127	x^3+2x^2+x	51	3
127	x^3+2x^2+x	52	5
127	x^3+2x^2+x	53	2
127	x^3+2x^2+x	54	4
127	x^3+2x^2+x	55	1
127	x^3+2x^2+x	56	3
127	x^3+2x^2+x	57	0
127	x^3+2x^2+x	58	2
127	x^3+2x^2+x	59	1
127	x^3+2x^2+x	60	1

p	$f(x)$	n	S
127	x^3+2x^2+x	61	0
127	x^3+2x^2+x	62	0
127	x^3+2x^2+x	63	-1
127	x^3+2x^2+x	64	-1
127	x^3+2x^2+x	65	-2
127	x^3+2x^2+x	66	-2
127	x^3+2x^2+x	67	-3
127	x^3+2x^2+x	68	-3
127	x^3+2x^2+x	69	4
127	x^3+2x^2+x	70	-4
127	x^3+2x^2+x	71	3
127	x^3+2x^2+x	72	4
127	x^3+2x^2+x	73	2
127	x^3+2x^2+x	74	3
127	x^3+2x^2+x	75	1
127	x^3+2x^2+x	76	2
127	x^3+2x^2+x	77	0
127	x^3+2x^2+x	78	1
127	x^3+2x^2+x	79	-1
127	x^3+2x^2+x	80	0

p	$f(x)$	n	S
127	x^3+2x^2+x	81	2
127	x^3+2x^2+x	82	-1
127	x^3+2x^2+x	83	1
127	x^3+2x^2+x	84	1
127	x^3+2x^2+x	85	0
127	x^3+2x^2+x	86	0
127	x^3+2x^2+x	87	1
127	x^3+2x^2+x	88	0
127	x^3+2x^2+x	89	0
127	x^3+2x^2+x	90	-1
127	x^3+2x^2+x	91	1
127	x^3+2x^2+x	92	-2
127	x^3+2x^2+x	93	0
127	x^3+2x^2+x	94	-3
127	x^3+2x^2+x	95	-1
127	x^3+2x^2+x	96	3
127	x^3+2x^2+x	97	-2
127	x^3+2x^2+x	98	2
127	x^3+2x^2+x	99	3
127	x^3+2x^2+x	100	1

p	$f(x)$	n	S
127	x^3+2x^2+x	101	2
127	x^3+2x^2+x	102	0
127	x^3+2x^2+x	103	1
127	x^3+2x^2+x	104	-1
127	x^3+2x^2+x	105	0
127	x^3+2x^2+x	106	-2
127	x^3+2x^2+x	107	-1
127	x^3+2x^2+x	108	2
127	x^3+2x^2+x	109	2
127	x^3+2x^2+x	110	1
127	x^3+2x^2+x	111	1
127	x^3+2x^2+x	112	0
127	x^3+2x^2+x	113	0
127	x^3+2x^2+x	114	-1
127	x^3+2x^2+x	115	-1
127	x^3+2x^2+x	116	1
127	x^3+2x^2+x	117	-2
127	x^3+2x^2+x	118	0
127	x^3+2x^2+x	119	-3
127	x^3+2x^2+x	120	-1

p	$f(x)$	n	S
127	$x^3 + 2x^2 + x$	121	-4
127	$x^3 + 2x^2 + x$	122	-2
127	$x^3 + 2x^2 + x$	123	-5
127	$x^3 + 2x^2 + x$	124	-3
127	$x^3 + 2x^2 + x$	125	-6
127	$x^3 + 2x^2 + x$	126	-4

A legnagyobb ismert prímre is jó

p	$f(x)$	n	S
$2^{57885151}-1$	x^2-1	1	0
$2^{57885151}-1$	x^2-1	2	1
$2^{57885151}-1$	x^2-1	3	1
$2^{57885151}-1$	x^2-1	4	0
$2^{57885151}-1$	x^2-1	5	1
$2^{57885151}-1$	x^2-1	6	0
$2^{57885151}-1$	x^2-1	7	0
$2^{57885151}-1$	x^2-1	8	1
$2^{57885151}-1$	x^2-1	9	1
$2^{57885151}-1$	x^2-1	10	0
$2^{57885151}-1$	x^2-1	11	1
$2^{57885151}-1$	x^2-1	12	0
$2^{57885151}-1$	x^2-1	13	0
$2^{57885151}-1$	x^2-1	14	-1
$2^{57885151}-1$	x^2-1	15	-1
$2^{57885151}-1$	x^2-1	16	-2
$2^{57885151}-1$	x^2-1	17	-2
$2^{57885151}-1$	x^2-1	18	-3
$2^{57885151}-1$	x^2-1	19	-3
$2^{57885151}-1$	x^2-1	20	-4

p	$f(x)$	n	S
$2^{57885151}-1$	x^2-1	21	-4
$2^{57885151}-1$	x^2-1	22	5
$2^{57885151}-1$	x^2-1	23	5
$2^{57885151}-1$	x^2-1	24	4
$2^{57885151}-1$	x^2-1	25	4
$2^{57885151}-1$	x^2-1	26	3
$2^{57885151}-1$	x^2-1	27	3
$2^{57885151}-1$	x^2-1	28	2
$2^{57885151}-1$	x^2-1	29	2
$2^{57885151}-1$	x^2-1	30	1
$2^{57885151}-1$	x^2-1	31	1
$2^{57885151}-1$	x^2-1	32	0
$2^{57885151}-1$	x^2-1	33	1
$2^{57885151}-1$	x^2-1	34	0
$2^{57885151}-1$	x^2-1	35	0
$2^{57885151}-1$	x^2-1	36	-1
$2^{57885151}-1$	x^2-1	37	2
$2^{57885151}-1$	x^2-1	38	1
$2^{57885151}-1$	x^2-1	39	1
$2^{57885151}-1$	x^2-1	40	0

p	$f(x)$	n	S
$2^{57885151}-1$	x^2-1	41	1
$2^{57885151}-1$	x^2-1	42	0
$2^{57885151}-1$	x^2-1	43	1
$2^{57885151}-1$	x^2-1	44	0
$2^{57885151}-1$	x^2-1	45	1
$2^{57885151}-1$	x^2-1	46	0
$2^{57885151}-1$	x^2-1	47	1
$2^{57885151}-1$	x^2-1	48	0
$2^{57885151}-1$	x^2-1	49	0
$2^{57885151}-1$	x^2-1	50	-1
$2^{57885151}-1$	x^2-1	51	-1
$2^{57885151}-1$	x^2-1	52	2
$2^{57885151}-1$	x^2-1	53	2
$2^{57885151}-1$	x^2-1	54	1
$2^{57885151}-1$	x^2-1	55	1
$2^{57885151}-1$	x^2-1	56	0
$2^{57885151}-1$	x^2-1	57	1
$2^{57885151}-1$	x^2-1	58	0
$2^{57885151}-1$	x^2-1	59	1
$2^{57885151}-1$	x^2-1	60	0

p	$f(x)$	n	S
$2^{57885151}-1$	x^2-1	61	0
$2^{57885151}-1$	x^2-1	62	-1
$2^{57885151}-1$	x^2-1	63	-1
$2^{57885151}-1$	x^2-1	64	2
$2^{57885151}-1$	x^2-1	65	2
$2^{57885151}-1$	x^2-1	66	1
$2^{57885151}-1$	x^2-1	67	1
$2^{57885151}-1$	x^2-1	68	0
$2^{57885151}-1$	x^2-1	69	1
$2^{57885151}-1$	x^2-1	70	0
$2^{57885151}-1$	x^2-1	71	1
$2^{57885151}-1$	x^2-1	72	0
$2^{57885151}-1$	x^2-1	73	1
$2^{57885151}-1$	x^2-1	74	0
$2^{57885151}-1$	x^2-1	75	1
$2^{57885151}-1$	x^2-1	76	0
$2^{57885151}-1$	x^2-1	77	0
$2^{57885151}-1$	x^2-1	78	-1
$2^{57885151}-1$	x^2-1	79	2
$2^{57885151}-1$	x^2-1	80	1

p	$f(x)$	n	S
$2^{57885151}-1$	x^2-1	81	1
$2^{57885151}-1$	x^2-1	82	0
$2^{57885151}-1$	x^2-1	83	1
$2^{57885151}-1$	x^2-1	84	0
$2^{57885151}-1$	x^2-1	85	0
$2^{57885151}-1$	x^2-1	86	-1
$2^{57885151}-1$	x^2-1	87	-1
$2^{57885151}-1$	x^2-1	88	2
$2^{57885151}-1$	x^2-1	89	2
$2^{57885151}-1$	x^2-1	90	1
$2^{57885151}-1$	x^2-1	91	1
$2^{57885151}-1$	x^2-1	92	0
$2^{57885151}-1$	x^2-1	93	0
$2^{57885151}-1$	x^2-1	94	-1
$2^{57885151}-1$	x^2-1	95	-1
$2^{57885151}-1$	x^2-1	96	2
$2^{57885151}-1$	x^2-1	97	2
$2^{57885151}-1$	x^2-1	98	1
$2^{57885151}-1$	x^2-1	99	1

p	$f(x)$	n	S
101	$7x^{10} - 8x^7 + 3x^5 - 14$	100	0
103	$7x^{10} - 8x^7 + 3x^5 - 14$	102	0
107	$7x^{10} - 8x^7 + 3x^5 - 14$	106	1
109	$7x^{10} - 8x^7 + 3x^5 - 14$	108	0
113	$7x^{10} - 8x^7 + 3x^5 - 14$	112	0
127	$7x^{10} - 8x^7 + 3x^5 - 14$	126	0
131	$7x^{10} - 8x^7 + 3x^5 - 14$	130	1
137	$7x^{10} - 8x^7 + 3x^5 - 14$	136	1
139	$7x^{10} - 8x^7 + 3x^5 - 14$	138	0
149	$7x^{10} - 8x^7 + 3x^5 - 14$	148	1
151	$7x^{10} - 8x^7 + 3x^5 - 14$	150	1
157	$7x^{10} - 8x^7 + 3x^5 - 14$	156	1
163	$7x^{10} - 8x^7 + 3x^5 - 14$	162	0
167	$7x^{10} - 8x^7 + 3x^5 - 14$	166	0
173	$7x^{10} - 8x^7 + 3x^5 - 14$	172	-3
179	$7x^{10} - 8x^7 + 3x^5 - 14$	178	0
181	$7x^{10} - 8x^7 + 3x^5 - 14$	180	0
191	$7x^{10} - 8x^7 + 3x^5 - 14$	190	0
193	$7x^{10} - 8x^7 + 3x^5 - 14$	192	1
197	$7x^{10} - 8x^7 + 3x^5 - 14$	196	0
199	$7x^{10} - 8x^7 + 3x^5 - 14$	198	0
211	$7x^{10} - 8x^7 + 3x^5 - 14$	210	0
223	$7x^{10} - 8x^7 + 3x^5 - 14$	222	0

p	$f(x)$	n	S
227	$7x^{10} - 8x^7 + 3x^5 - 14$	226	-1
229	$7x^{10} - 8x^7 + 3x^5 - 14$	228	-1
233	$7x^{10} - 8x^7 + 3x^5 - 14$	232	0
239	$7x^{10} - 8x^7 + 3x^5 - 14$	238	0
241	$7x^{10} - 8x^7 + 3x^5 - 14$	240	1
251	$7x^{10} - 8x^7 + 3x^5 - 14$	250	0
257	$7x^{10} - 8x^7 + 3x^5 - 14$	256	0
263	$7x^{10} - 8x^7 + 3x^5 - 14$	262	1
269	$7x^{10} - 8x^7 + 3x^5 - 14$	268	1
271	$7x^{10} - 8x^7 + 3x^5 - 14$	270	1
277	$7x^{10} - 8x^7 + 3x^5 - 14$	276	0
281	$7x^{10} - 8x^7 + 3x^5 - 14$	280	0
283	$7x^{10} - 8x^7 + 3x^5 - 14$	282	0
293	$7x^{10} - 8x^7 + 3x^5 - 14$	292	1
307	$7x^{10} - 8x^7 + 3x^5 - 14$	306	-2
311	$7x^{10} - 8x^7 + 3x^5 - 14$	310	-1
313	$7x^{10} - 8x^7 + 3x^5 - 14$	312	0
317	$7x^{10} - 8x^7 + 3x^5 - 14$	316	0
331	$7x^{10} - 8x^7 + 3x^5 - 14$	330	3
337	$7x^{10} - 8x^7 + 3x^5 - 14$	336	0
347	$7x^{10} - 8x^7 + 3x^5 - 14$	346	1
349	$7x^{10} - 8x^7 + 3x^5 - 14$	348	1

p	$f(x)$	n	S
353	$7x^{10} - 8x^7 + 3x^5 - 14$	352	1
359	$7x^{10} - 8x^7 + 3x^5 - 14$	358	0
367	$7x^{10} - 8x^7 + 3x^5 - 14$	366	0
373	$7x^{10} - 8x^7 + 3x^5 - 14$	372	1
379	$7x^{10} - 8x^7 + 3x^5 - 14$	378	3
383	$7x^{10} - 8x^7 + 3x^5 - 14$	382	0
389	$7x^{10} - 8x^7 + 3x^5 - 14$	388	0
397	$7x^{10} - 8x^7 + 3x^5 - 14$	396	0
401	$7x^{10} - 8x^7 + 3x^5 - 14$	400	2
409	$7x^{10} - 8x^7 + 3x^5 - 14$	408	0
419	$7x^{10} - 8x^7 + 3x^5 - 14$	418	0
421	$7x^{10} - 8x^7 + 3x^5 - 14$	420	0
431	$7x^{10} - 8x^7 + 3x^5 - 14$	430	0
433	$7x^{10} - 8x^7 + 3x^5 - 14$	432	0
439	$7x^{10} - 8x^7 + 3x^5 - 14$	438	1
443	$7x^{10} - 8x^7 + 3x^5 - 14$	442	0
449	$7x^{10} - 8x^7 + 3x^5 - 14$	448	0
457	$7x^{10} - 8x^7 + 3x^5 - 14$	456	0
461	$7x^{10} - 8x^7 + 3x^5 - 14$	460	0
463	$7x^{10} - 8x^7 + 3x^5 - 14$	462	0
467	$7x^{10} - 8x^7 + 3x^5 - 14$	466	-1
479	$7x^{10} - 8x^7 + 3x^5 - 14$	478	0

p	$f(x)$	n	S
487	$7x^{10} - 8x^7 + 3x^5 - 14$	486	0
491	$7x^{10} - 8x^7 + 3x^5 - 14$	490	0
499	$7x^{10} - 8x^7 + 3x^5 - 14$	498	-1
503	$7x^{10} - 8x^7 + 3x^5 - 14$	502	1
509	$7x^{10} - 8x^7 + 3x^5 - 14$	508	0
521	$7x^{10} - 8x^7 + 3x^5 - 14$	520	0
523	$7x^{10} - 8x^7 + 3x^5 - 14$	522	0
541	$7x^{10} - 8x^7 + 3x^5 - 14$	540	0
547	$7x^{10} - 8x^7 + 3x^5 - 14$	546	1
557	$7x^{10} - 8x^7 + 3x^5 - 14$	556	1
563	$7x^{10} - 8x^7 + 3x^5 - 14$	562	0
569	$7x^{10} - 8x^7 + 3x^5 - 14$	568	1
571	$7x^{10} - 8x^7 + 3x^5 - 14$	570	1
577	$7x^{10} - 8x^7 + 3x^5 - 14$	576	-1
587	$7x^{10} - 8x^7 + 3x^5 - 14$	586	0
593	$7x^{10} - 8x^7 + 3x^5 - 14$	592	-1
599	$7x^{10} - 8x^7 + 3x^5 - 14$	598	-1
601	$7x^{10} - 8x^7 + 3x^5 - 14$	600	0
607	$7x^{10} - 8x^7 + 3x^5 - 14$	606	1
613	$7x^{10} - 8x^7 + 3x^5 - 14$	612	3
617	$7x^{10} - 8x^7 + 3x^5 - 14$	616	1
619	$7x^{10} - 8x^7 + 3x^5 - 14$	618	-1

p	$f(x)$	n	S
101	$7x^{10} - 8x^7 + 3x^5 - 14$	50	-2
103	$7x^{10} - 8x^7 + 3x^5 - 14$	51	0
107	$7x^{10} - 8x^7 + 3x^5 - 14$	53	1
109	$7x^{10} - 8x^7 + 3x^5 - 14$	54	0
113	$7x^{10} - 8x^7 + 3x^5 - 14$	56	0
127	$7x^{10} - 8x^7 + 3x^5 - 14$	63	1
131	$7x^{10} - 8x^7 + 3x^5 - 14$	65	1
137	$7x^{10} - 8x^7 + 3x^5 - 14$	68	0
139	$7x^{10} - 8x^7 + 3x^5 - 14$	69	1
149	$7x^{10} - 8x^7 + 3x^5 - 14$	74	-1
151	$7x^{10} - 8x^7 + 3x^5 - 14$	75	0
157	$7x^{10} - 8x^7 + 3x^5 - 14$	78	0
163	$7x^{10} - 8x^7 + 3x^5 - 14$	81	1
167	$7x^{10} - 8x^7 + 3x^5 - 14$	83	1
173	$7x^{10} - 8x^7 + 3x^5 - 14$	86	0
179	$7x^{10} - 8x^7 + 3x^5 - 14$	89	-1
181	$7x^{10} - 8x^7 + 3x^5 - 14$	90	1
191	$7x^{10} - 8x^7 + 3x^5 - 14$	95	1
193	$7x^{10} - 8x^7 + 3x^5 - 14$	96	0
197	$7x^{10} - 8x^7 + 3x^5 - 14$	98	1
199	$7x^{10} - 8x^7 + 3x^5 - 14$	99	1
211	$7x^{10} - 8x^7 + 3x^5 - 14$	105	1
223	$7x^{10} - 8x^7 + 3x^5 - 14$	111	1

p	$f(x)$	n	S
227	$7x^{10} - 8x^7 + 3x^5 - 14$	113	1
229	$7x^{10} - 8x^7 + 3x^5 - 14$	114	0
233	$7x^{10} - 8x^7 + 3x^5 - 14$	116	0
239	$7x^{10} - 8x^7 + 3x^5 - 14$	119	1
241	$7x^{10} - 8x^7 + 3x^5 - 14$	120	2
251	$7x^{10} - 8x^7 + 3x^5 - 14$	125	1
257	$7x^{10} - 8x^7 + 3x^5 - 14$	128	2
263	$7x^{10} - 8x^7 + 3x^5 - 14$	131	1
269	$7x^{10} - 8x^7 + 3x^5 - 14$	134	1
271	$7x^{10} - 8x^7 + 3x^5 - 14$	135	2
277	$7x^{10} - 8x^7 + 3x^5 - 14$	138	1
281	$7x^{10} - 8x^7 + 3x^5 - 14$	140	-3
283	$7x^{10} - 8x^7 + 3x^5 - 14$	141	0
293	$7x^{10} - 8x^7 + 3x^5 - 14$	146	3
307	$7x^{10} - 8x^7 + 3x^5 - 14$	153	1
311	$7x^{10} - 8x^7 + 3x^5 - 14$	155	1
313	$7x^{10} - 8x^7 + 3x^5 - 14$	156	0
317	$7x^{10} - 8x^7 + 3x^5 - 14$	158	-1
331	$7x^{10} - 8x^7 + 3x^5 - 14$	165	-2
337	$7x^{10} - 8x^7 + 3x^5 - 14$	168	-1
347	$7x^{10} - 8x^7 + 3x^5 - 14$	173	1
349	$7x^{10} - 8x^7 + 3x^5 - 14$	174	0
353	$7x^{10} - 8x^7 + 3x^5 - 14$	176	-1

p	$f(x)$	n	S
359	$7x^{10} - 8x^7 + 3x^5 - 14$	179	-2
367	$7x^{10} - 8x^7 + 3x^5 - 14$	183	-1
373	$7x^{10} - 8x^7 + 3x^5 - 14$	186	-1
379	$7x^{10} - 8x^7 + 3x^5 - 14$	189	2
383	$7x^{10} - 8x^7 + 3x^5 - 14$	191	1
389	$7x^{10} - 8x^7 + 3x^5 - 14$	194	0
397	$7x^{10} - 8x^7 + 3x^5 - 14$	198	2
401	$7x^{10} - 8x^7 + 3x^5 - 14$	200	3
409	$7x^{10} - 8x^7 + 3x^5 - 14$	204	1
419	$7x^{10} - 8x^7 + 3x^5 - 14$	209	-3
421	$7x^{10} - 8x^7 + 3x^5 - 14$	210	0
431	$7x^{10} - 8x^7 + 3x^5 - 14$	215	1
433	$7x^{10} - 8x^7 + 3x^5 - 14$	216	1
439	$7x^{10} - 8x^7 + 3x^5 - 14$	219	1
443	$7x^{10} - 8x^7 + 3x^5 - 14$	221	0
449	$7x^{10} - 8x^7 + 3x^5 - 14$	224	0
457	$7x^{10} - 8x^7 + 3x^5 - 14$	228	-1
461	$7x^{10} - 8x^7 + 3x^5 - 14$	230	0
463	$7x^{10} - 8x^7 + 3x^5 - 14$	231	0
467	$7x^{10} - 8x^7 + 3x^5 - 14$	233	0
479	$7x^{10} - 8x^7 + 3x^5 - 14$	239	1
487	$7x^{10} - 8x^7 + 3x^5 - 14$	243	1
491	$7x^{10} - 8x^7 + 3x^5 - 14$	245	1

p	$f(x)$	n	S
499	$7x^{10} - 8x^7 + 3x^5 - 14$	249	3
503	$7x^{10} - 8x^7 + 3x^5 - 14$	251	1
509	$7x^{10} - 8x^7 + 3x^5 - 14$	254	0
521	$7x^{10} - 8x^7 + 3x^5 - 14$	260	1
523	$7x^{10} - 8x^7 + 3x^5 - 14$	261	1
541	$7x^{10} - 8x^7 + 3x^5 - 14$	270	1
547	$7x^{10} - 8x^7 + 3x^5 - 14$	273	-1
557	$7x^{10} - 8x^7 + 3x^5 - 14$	278	0
563	$7x^{10} - 8x^7 + 3x^5 - 14$	281	1
569	$7x^{10} - 8x^7 + 3x^5 - 14$	284	2
571	$7x^{10} - 8x^7 + 3x^5 - 14$	285	1
577	$7x^{10} - 8x^7 + 3x^5 - 14$	288	1
587	$7x^{10} - 8x^7 + 3x^5 - 14$	293	2
593	$7x^{10} - 8x^7 + 3x^5 - 14$	296	0
599	$7x^{10} - 8x^7 + 3x^5 - 14$	299	1
601	$7x^{10} - 8x^7 + 3x^5 - 14$	300	0
607	$7x^{10} - 8x^7 + 3x^5 - 14$	303	5
613	$7x^{10} - 8x^7 + 3x^5 - 14$	306	1
617	$7x^{10} - 8x^7 + 3x^5 - 14$	308	1
619	$7x^{10} - 8x^7 + 3x^5 - 14$	309	1

Következtetés:

Teljes négyzet vagy annak konstansszorosa nyilván nem jó, hiszen ezek mindig kvadratikus maradékot (esetleg p többszörösét) adják. Ezt leszámítva minden polinom jó pszeudovéletlen tulajdonságot mutatott a teszteken minden vizsgált prímre és hosszra (hosszra, azaz a generált bitek számára — elképzelhető, hogy egy hosszú bitsorozat lineáris komplexitása ugyan magas, de valamely kezdőszeletéé alacsony; a vizsgált esetekben szerencsére nem ez a helyzet). Érdekes, hogy bár ± 3 modulo 8 alakú p prímekre a lineáris komplexitás [16] alapján p körüli, mégis az n hosszú kezdőszeletekre csak $\frac{n}{2}$ körüli értékeket tapasztalunk (0 körüli S).

Irodalomjegyzék

[1] R. Ahlswede, C. Mauduit, A. Sárközy, *Large families of Pseudorandom sequences of k symbols and their complexity - Part I*, Information Transfer and Combinatorics, LNCS 4123, pp. 293–307, 2006.

[2] J. Cassaigne, C. Mauduit, A. Sárközy, *On finite pseudorandom sequences VII: The measures of pseudoranomness*, Acta Arithmetica 103.2 (2002)

[3] L. Goubin, C. Mauduit, A. Sárközy, *Construction of pseudorandom binary sequences*, Journal of Number Theory 106 (2004) 56–69

[4] K. Gyarmati, *Measures of pseudorandomess*, Finite Fields and Their Applications: Character Sums and Polynomials edited by Pascale Charpin, Alexander Pott, Arne Winterhof

[5] K. Gyarmati, C. Mauduit, A. Sárközy, *On linear complexity of binary lattices*, Ramanujan J (2014) 34:237–263

[6] K. Gyarmati, A. Pethő, A. Sárközy, *On linear recursion and pseudorandomness*, Acta Mathematica 118.4 (2005)

[7] K. Gyarmati, A. Sárközy, *Pszeudovéletlenség*, egyetemi jegyzet

[8] K. Gyarmati, A. Sárközy, C. Stewart, *On Legendre symbol lattices*, Uniform Distribution Theory 4 (2009), no.1, 81–95

[9] P. Hubert, C. Mauduit, A. Sárközy, *On pseudorandom binary lattices*, Acta Arithmetica 125.1 (2006)

[10] C. Mauduit, A. Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arithmetica LXXXII.4 (1997)

[11] C. Mauduit, A. Sárközy, *On finite pseudorandom binary sequences of k symbols*, Indag. Mathem., N.S., 13 (1), 89-101

[12] A. Menezes, P. Oorschot, S. Vanstone, *Handbook of applied cryptography*

[13] National Institute of Standards and Technology, *A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications*, http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html

[14] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, V. Rödl, *Measures of pseudorandomness for finite sequences: Minimal Values,* Combinatorics, Probability and Computing, 15, pp 1-29 (2006)

[15] D. K. Nyberg, *Fundamentals of Cryptography*, lectures notes, 2014

[16] C. Ding, T. Helleseth, W. Shan, *On the Linear Complexity of Legendre Sequences*, 1276 IEEE Transactions on information theory, vol. 44, no. 3, May 1998

[17] J. Neumann, V*arious techniques used in connection with random digits*, Notes by G E Forsythe, National Bureau of Standards Applied Math Series, 12 (1951) pp 36-38

[18] K. Gyarmati, C. Maudit, A. Sárközy, *On finite pseudorandom binary lattices*, Discrete Applied Mathematics (2014)