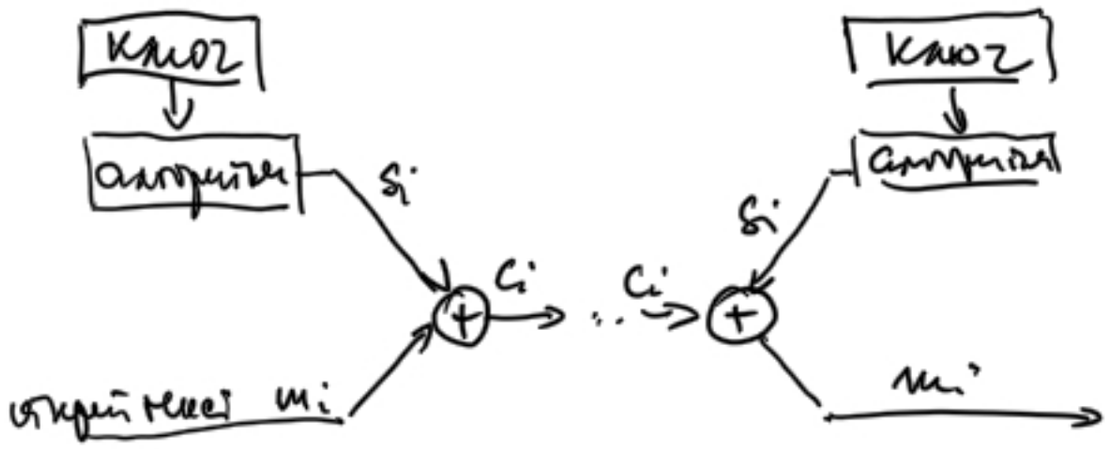
17.03.2021

Линейни рекурентни редици и линейни регистри

Обща схема



Бихме искали:

- $(s_i)_{i \geq 0}$ да изглежда като случайна редица
- да има нужда криптографски действия

Ще разглеждаме само двоични редици.

Идеята теория често се крепясва за редици над произволно крайно поле.

Def. • Казваме, че $(s_i)_{i\geq 0}$ е периодична, ако съществува естествено число m, за което

$$s_{i+m} = s_i \quad \forall i \geq 0.$$

• Най-малкото естествено число m с това свойство наричаме период.

• Казваме, че

$(s_t, s_{t+1}, \dots s_{t+k-1})$

е блок с дължина k, ако

$s_{t-1} \neq s_t = s_{t+1} = \dots = s_{t+k-1} \neq s_{t+k}$

е блок с дължина k

$0\underbrace{11\dots1}_{k}0$ – блок от единици

$1\underbrace{00\dots0}_{k}1$ – блок от нули

- Автокорелацията на периодична редица с период p (минималния период) наричаме величината

$$AC(k) = \frac{A - D}{p},$$

където

A = брят на съвпаденията в рамките на един период между (s_i) и (s_{i+k})

D = брят на несъвпаденията в рамките на един период между (s_i) и (s_{i+k})

$$A = \left| \{ 0 \le i < p \mid s_i = s_{i+k} \} \right|$$

$$D = \left| \{ 0 \le i < p \mid s_i \neq s_{i+k} \} \right|$$

Ако p / k фазова автокорелацията е 1.

Ако $p \nmid k$ нулафазова

$-1 \le AC \le 1$

Пример

(а) 1 1 1 0 0 0 0 1 1 1 0 0 0 0 . . . .

$p = 7$

AC(1)
1 1 1 0 0 0 0
1 1 0 0 0 0 1
$A = 5$ $D = 2$ $AC(1) = \frac{3}{7}$

AC(2)
1 1 1 0 0 0 0
1 0 0 0 0 1 1
$A = 3$ $D = 4$ $AC(2) = -\frac{1}{7}$

$AC(3) = -\frac{5}{7}$, $AC(4) = -\frac{5}{7}$, $AC(5) = -\frac{1}{7}$, $AC(6) = \frac{3}{7}$

(б) 1 1 0 1 0 0 0 1 1 0 1 0 0 0 . . . .

AC(1)
1 1 0 1 0 0 0
1 0 1 0 0 0 1
$A = 3$ $D = 4$ $AC(1) = -\frac{1}{7}$

AC(2)
1 1 0 1 0 0 0
0 1 0 0 0 1 1
$A = 3$ $D = 4$ $AC(2) = -\frac{1}{7}$

$AC(3) = AC(4) = AC(5) = AC(6) = -\frac{1}{7}$

Цифровизирана автокорелация е константа.

Постулати на Голомб

(G1) Броят на нулите и единиците в рамките на един период да е равен или да се различава с 1.

(G2) Половината от поднизите в рамките на един период да е дължина 1; една четвърт — да е дължина 2; една осма от поднизите — с дължина 3 и т.н. (докъдето има смисъл). Много повече — половината от поднизите с дадена дължина са поднизи от нули и половината — поднизи от единици.

(G3) Мултифазовата автокорелация $AC(k)$, $\phi \neq k$, е константа.

Def. Редица, удовлетворяваща (G1 – G3) наричаме *псевдослучайна*, PN-редица (pseudo-noise sequence).

Теорема Нека (s_i) е PN-редица. Тогава за всяко *период* p

k, което не се дели на p:

$$AC(k) = \begin{cases} -\frac{1}{p-1} & p\text{-четно} \\ -\frac{1}{p} & p\text{-нечетно} \end{cases}$$

Док.

$$\begin{matrix} s_0 & s_1 & s_2 & \cdots & s_{p-1} \\ s_1 & s_2 & s_3 & \cdots & s_0 \\ s_2 & s_3 & s_4 & \cdots & s_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{p-1} & s_0 & s_1 & \cdots & s_{p-2} \end{matrix}$$

Броим двете съвпадения заедно
двойно несъвпадение на ред 0
с всеки от останалите
редове.

От една за нулевия и кой да е
друг ред това число е $p.AC(k)$

$$A - D = p.AC(k)$$

$\Rightarrow$ сумата е $p(p-1)AC(k)$

От друга страна

(а) p-четно всеки стълб дава

$$\left(\frac{p}{2}-1\right) - \frac{p}{2} = -1$$

$$\Rightarrow p(p-1)AC(k) = p.(-1)$$

$$AC(k) = -\frac{1}{p-1}$$

(б) p-нечетно

за $\frac{p+1}{2}$ стълба: $\frac{p-1}{2} - \frac{p-1}{2} = 0$

за $\frac{p-1}{2}$ стълба: $\frac{p-3}{2} - \frac{p+1}{2} = -2$

$$\Rightarrow p(p-1)\,Ac(k) = \frac{p+1}{2}\cdot 0 + \frac{p-1}{2}\cdot(-2)$$

$$Ac(k) = -\frac{1}{p}$$

□

Допълнителни изисквания
(от криптографско естество)

(C1) голям период

(C2) лесни за генериране

(C3) устойчивост на криптоанализ
(знанието на относително
малка част от изходната
редица не позволява
генерирането на цялата
редица)

LFSR

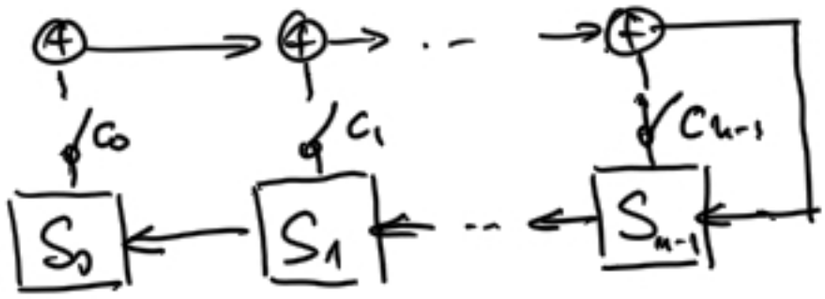
n - дължина на регистъра

$(S_0, S_1 \ldots S_{n-1})$ състояние на регистъра

$f: \{0,1\}^n \to \{0,1\}$ булева функция

Ако f е линейна - линеен регистър

$$\begin{cases} S_i(t+1) = S_{i+1}(t) & i = 0, \ldots, n-2 \\ S_{n-1}(t+1) = f(S_0(t), \ldots S_{n-1}(t)) \end{cases}$$



$$f(x_0, x_1 \ldots x_{n-1}) = c_0 x_0 + c_1 x_1 + \ldots + c_{n-1} x_{n-1}$$
$$c_i \in \{0,1\}$$

Линейните регистри поражда редици, които се нарекли рекурентни редици (S_i)

$$S_{k+n} = C_0 S_k + C_1 S_{k+1} + \dots + C_{n-1} S_{k+n-1}$$

$$S_i = S_0(t=i)$$

Б.О.О. можем да дешифрираме във уравнението

$$C_0 S_k + C_1 S_{k+1} + \dots + C_{n-1} S_{k+n-1} + \underset{\|}{C_n} S_{k+n} = 0$$
$$1$$

Ще считаме, че $\underline{C_0 = 1}$, $\underline{C_n = 1}$

Ако $C_0 = 0$ отпада редица без първия член се генерира от по-ниския регистър.

$\underline{S}^{(i)} = (S_i, S_{i+1}, \dots S_{i+n-1})$ – вектор из состояний в i-ый момент

$$\underline{S}^{(k+n)} = C_0\underline{S}^{(k)} + C_1\underline{S}^{(k+1)} + \dots + C_{n-1}\underline{S}^{(k+n-1)}$$

$$C_0\underline{S}^{(k)} + C_1\underline{S}^{(k+1)} + \dots + C_{n-1}\underline{S}^{(k+n-1)} + C_n\underline{S}^{(k+n)} = \underline{0}$$

$C_0 = 1$ по допущению

$C_n = 1$ по определению

$$\boxed{f(x) = C_n x^n + C_{n-1}x^{n-1} + \dots + C_1 x + C_0}$$

характеристический полином из регистра (S_i), задающий с горизонтальной линией уравнение.

Def $\Omega(f) = \{(s_i) \mid s_i$ удовлетворяват $(*)\}$

$(*)$ $c_0 s_k + c_1 s_{k+1} + \dots c_{n-1} s_{k+n-1} + c_n s_{k+n} = 0$

Thm. $\Omega(f)$ е ~~линейно~~ векторно пространство с размерност n.

Док.

Да се провери, че ако (s_i) и (t_i) удовлетворяват $(*)$, то и $(s_i + t_i)$ удовлетворява $(*)$.

Базис: редиците с нагоре отсъстващи

$$(0\ 0 \dots \underbrace{1}_{i}\ 0 \dots 0) \qquad i = 0, 1, \dots, n-1$$

n

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$$

$$f^*(x) = x^n f\left(\frac{1}{x}\right) = c_0 x^n + c_1 x^{n-1} + \dots + c_{n-1} + c_n$$

$$\deg f - \deg f^* = n$$

$$(s_i) \in \Omega(f) \Rightarrow S(x) \in \Omega(f)$$

$$S(x) = s_0 + s_1 x + s_2 x^2 + \dots = \sum_{i \geq 0} s_i x^i$$

(За формалните редове – виж приложението)

Thm Нехай $(s_i) \in Q(f)$, нехай
$f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_0$
Тоді
$$S(x) = \frac{\tau(x)}{f^*(x)},$$
де $\tau(x) = \sum_{j=0}^{n-1}{}' \left(\sum_{l=0}^{j}{}' c_{n-l} s_{j-l} \right) x^j$

В частності $\deg \tau(x) < n$

Дов. $S(x) f^*(x) = \left(\sum_{i=0}^{\infty}{}' s_i x^i \right) \left(\sum_{l=0}^{n}{}' c_{n-l} x^l \right)$

$$= \sum_{j=0}^{\infty}{}' \left(\sum_{l=0}^{\min(j,n)}{}' s_{j-l} c_{n-l} \right) x^j$$

$$= \sum_{j=0}^{n-1}{}' \left(\sum_{l=0}^{j}{}' s_{j-l} c_{n-l} \right) x^j + \sum_{j=n}^{\infty}{}' \underbrace{\left(\sum_{l=0}^{n}{}' s_{j-l} c_{n-l} \right)}_{0 \ (*)} x^j$$

Следствие

$$\Omega(f) = \left\{ \frac{i(x)}{f^*(x)} \;\middle|\; \deg i < n \right\}$$

Лемма 1. Пусть $(s_i) \in \Omega(f)$, а $(t_i) \in \Omega(g)$. Тогда $(s_i + t_i) \in \Omega(h)$ где $h = \operatorname{lcm}(f,g) = [f,g]$ (fork)

Док-во. $S(x) = \dfrac{\alpha(x)}{f^*(x)}$ $\deg \alpha < \deg f$

$T(x) = \dfrac{\beta(x)}{g^*(x)}$ $\deg \beta < \deg g$

$h(x) = u(x) \cdot f(x) = v(x) \cdot g(x)$

$$S(x) + T(x) = \frac{\alpha(x)}{f^*(x)} + \frac{\beta(x)}{g^*(x)}$$

$$= \frac{\alpha(x) g^*(x) + \beta(x) f^*(x)}{f^*(x) g^*(x)}$$

$$= \frac{\alpha(x) u^*(x) + \beta(x) v^*(x)}{h^*(x)}$$

Използваме, че

$$h^* = u^* f^* = v^* g^* .$$

$$\left.\begin{array}{l} \deg \alpha(x) u^*(x) < \deg h \\ \deg \beta(x) v^*(x) < \deg h \end{array}\right\} \Rightarrow$$

$$S(x) + T(x) \in \Omega(h)$$

□

Факти.

A. $\forall f(x) \in \mathbb{F}_2[x]$, $f(0) = 1$ съществува ест. число m : $f(x) \mid x^m - 1 = x^m + 1$
Най-малкото такова m : ord(f)

B. Ако f е неразложим. то
ord $f \mid 2^n - 1$
Ако ord $f = 2^n - 1$, то f се нарича примитивен.

C. Брят на примитивните полиноми е $\varphi(2^n - 1)/n$.

Лемма 2. Пусть $\deg f = n$ n
$\operatorname{ord} f = m$

Пусть $(s_i) \in \Omega(f)$. Тогда
период p на (s_i) равен m.

Док. $\exists g(x) : f(x) g(x) = x^m + 1$ $(\mathbb{F}_2)$

$\deg g(x) = m - n$

$f^*(x) \cdot g^*(x) = (x^m+1)^* = x^m + 1$

$\exists r(x)$, $\deg r < n$

$$S(x) = \frac{r(x)}{f^*(x)} = \frac{r(x) g^*(x)}{x^m+1} =$$

$$= r(x) f^*(x) \left(1 + x^m + x^{2m} + \dots\right)$$

$$\frac{1}{1+x^m} = 1 + x^m + x^{2m} + x^{3m} + \dots$$

$$(1+b^m)(1 + b^m + b^{2m} + \dots) = 1 + b^m + b^{2m} + \dots$$
$$x^m + x^{2m} + \dots$$

$$= 1$$

$\deg \tau g^* < m$

$\underline{\tau(x) g^*(x)} + \underline{x^m \tau(x) g^*(x)} + \underline{x^{2m} \tau(x) g^*(x)}$

$\Rightarrow$ $S(x)$ има период който дели m (m е кратно на периода).

∎

Лема 3. Нека $\deg f = n$, $\operatorname{ord} f = m$ и f - неразложим. Ако $(s_i) \in \Omega(f)$, то тази редица е с период равен на m.

Док. Нека p е периодът на (s_i). Отпреди знаем, че $p \mid m$

$$S(x) = \frac{u(x)}{1+x^p}, \quad \deg u < p$$

$$= u(x) + x^p u(x) + x^{2p} u(x) + \cdots$$

$$S(x) = \frac{\tau(x)}{f^*(x)}, \quad \deg \tau < n$$

$$(1+x^p)\,\tau(x) = u(x)\, f^*(x)$$

$$(1+x^p)\,\tau^*(x) = u^*(x)\, f(x)$$

Но f є незвідним і

$\deg \tau^* < \deg f = n$

$\Rightarrow f \mid 1+x^p$

$\Rightarrow \operatorname{ord} f = m \mid p$

$\Rightarrow m = p$

□

Лема 4. Нека $\deg f(x) = n$, нека $(s_i) \in \Omega(f)$ и нека (s_i) е PN-редица с период $2^n - 1$. Тогава f е неразложим.

Док. Нека $f = f_1 f_2$ $\deg f_i = n_i > 0$

$\frac{1}{f_1^x} \in \Omega(f_1) \Rightarrow$ периодът на $\frac{1}{f_1^x}$ дели $2^{n_1} - 1$

$\frac{1}{f_1^x} = \frac{f_2^x}{f^x} \in \Omega(f) \to \frac{1}{f_1^x}$ е с период $2^n - 1$

$\Rightarrow 2^n - 1 \;/\; 2^{n_1} - 1 \Rightarrow n_1 = n$

$\to f = f_1$, противоречие ($\deg f_2 = 0$).

□

Thm Редица, получена от LFSR с характеристичен полином f (от ген. рек. уравнение (*) с хар. пол. f) има период $2^n - 1$ тогава и само тогава, когато f е примитивен.

Док.: Леми 1–4.

Броят на линейните регистри, които пораждат редица с макс. период $2^n - 1$ е

$$\frac{\varphi(2^n - 1)}{n}.$$

В каква степен се удовлетворяват постулатите на Голомб

G1. Най-левият бит на всяко състояние (всеки ненулев вектор) излиза на изхода

$\Rightarrow$ #единици $= 2^{n-1}$; #нули $= 2^{n-1} - 1$

G2: За всяко $k = 0, \ldots, n-2$:

Съществуват 2^{n-k-2} състояния, чиито най-леви $k+2$ координати са от вида $0\underbrace{1\ldots1}_{k}0$ или $1\underbrace{0\ldots0}_{k}1$

(и половината са блокове от нули, а половината блокове от единици)

$0\underbrace{1\ldots11}_{n-1}$ се появява точно веднъж с наследник

$\underbrace{11\ldots11}_{n}$ с наследник

$\underbrace{11\ldots1}_{n-1}0$

=> или блок от единици с дължина $n-1$
или точно един блок от
единици с дължина n

Аналогично:

или точно един блок от нули с
дължина $n-1$
или блок от нули с дължина n

(G2) се изпълнява в удовлетворяващия
смисъл

(G3) $(\delta_i) \in \Omega(f)$ $(\delta_{i+k}) \in \Omega(f)$
$(\delta_i + \delta_{i+k}) \in \Omega(f)$

=> # съвпадения в (δ_i) и (δ_{i+k}) =
брой нули в $(\delta_i + \delta_{i+k})$
несъвпадения в $(\delta_i) + (\delta_{i+k})$ =
брой единици в $(\delta_i + \delta_{i+k})$

$$AC(k) = \frac{(2^{n-1} - 1) - 2^{n-1}}{2^n - 1} = -\frac{1}{2^n - 1}.$$

Криптографски изисквания:

(С1) Период $2^n - 1$ – колкото да бъде невъзможно да бъде намерен.

(С2) Удовлетворява статистическите изисквания

(С3) NB! Знаейки $2n$ последователни бита трябва невъзможно да определим c_i $i = 0, 1, \ldots, n-1$.

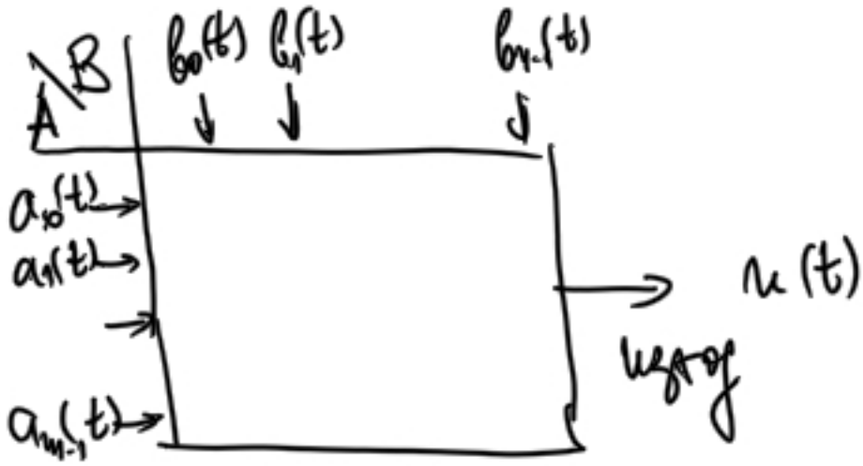
$$\begin{pmatrix} s_k & s_{k+1} & \cdots & s_{k+n-1} \\ s_{k+1} & s_{k+2} & \cdots & s_{k+n} \\ \cdots & & & \\ s_{k+n-1} & s_{k+n} & \cdots & s_{k+2n-2} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} s_{k+n} \\ s_{k+n+1} \\ \vdots \\ s_{k+2n-1} \end{pmatrix}$$

Ако се нарушат: $s_k, s_{k+1}, \ldots, s_{k+2n-1}$

всеки n последователни членове са линейно независими (защо?)

$\Rightarrow$ можем да намерим $c_0, \ldots c_{n-1}$ единствено.

Мултиплексер



- В този случай A определя адрес в B
- Този адрес сочи кутия съответната клетка в B.

Пример

1) Два LFSR с дължини съответно m и n с примитивни характеристични полиноми и с ненулеви начални състояния

2) Избиране h различни ел. от $\{0,1,\dots m-1\}$ и им подреждане

$$0 \le i_1 < i_2 < \dots < i_h \le m-1$$

$$(a_{i_1}(t), \dots a_{i_h}(t)) \to N(t) = \sum_{j=1}^{h} a_{i_j}(t) 2^{j-1}$$

3) τ - инжективно

$$\tau: \{0,1,\dots 2^h - 1\} \to \{0,1,\dots n-1\}$$

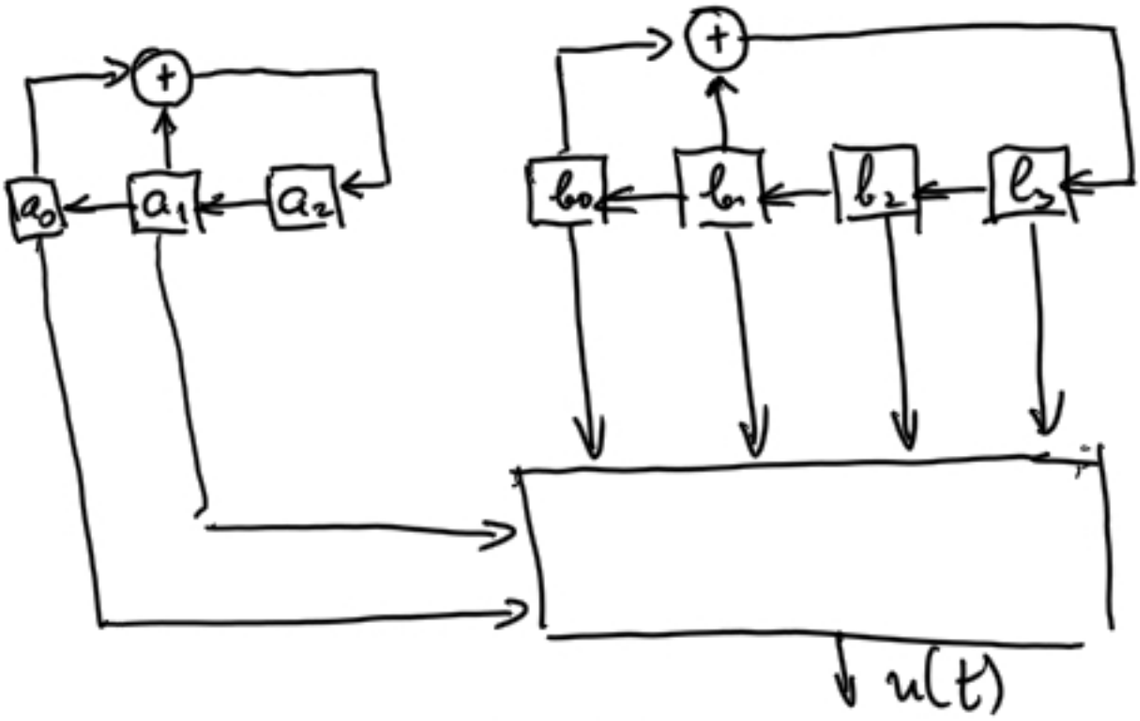
4) Изход:

$$u(t) = b_{\tau(N(t))}(t)$$

Пример $m=3, n=4, k=2, i_1=0, i_2=1$

$\tau(0)=3, \tau(1)=2, \tau(2)=0, \tau(3)=1$

$N=a_0+2a_1$



t	a_0	a_1	a_2	N(t)	$\tau(N)$	b_0	b_1	b_2	b_3	u(t
0	1	0	0	1	2	1	0	(0)	0	0
1	0	0	1	0	3	0	0	0	(1)	1
2	0	1	0	2	0	(0)	0	1	0	0
3	1	0	1	1	2	0	1	(0)	0	0
4	0	1	1	2	0	(1)	0	0	1	1
5	1	1	1	3	1	0	(0)	1	1	0
6	1	1	0	3	1	0	(1)	1	0	1
7	1	0	0	1	3	1	1	0	(1)	1

Пим Ако $(m,n) = 1$ то
циклическата редица $u(t)$
е с период $(2^m-1)(2^n-1)$.