Прыгающие клеточные автоматы. Обзор результатов

XIV конференция «РусКрипто’2012»

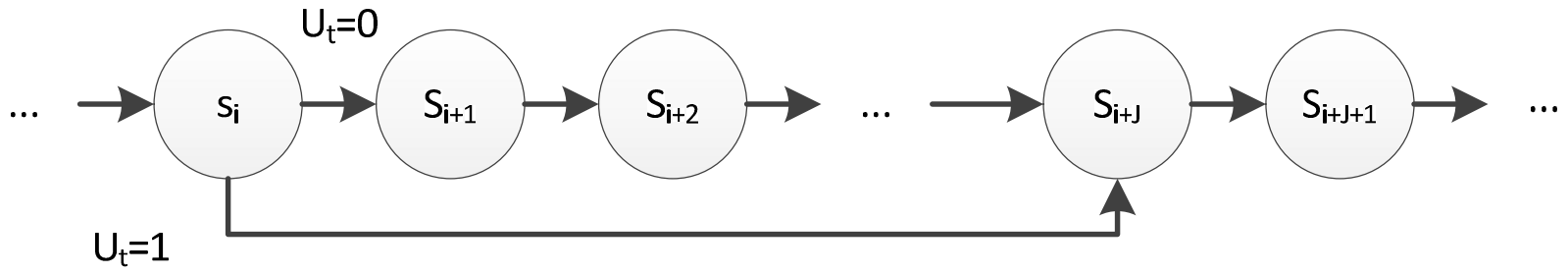
Дрелихов В.О.

к.ф.-м.н.

1. Нахождение характеристических многочленов с заданным индексом прыжка

Цель: гарантировать невозможность частичных перекрытий или пересечений различных траекторий состояний автомата на цикловой структуре.

Решение. Реализация прыжков по цикловой структуре для линейного автомата со специально подобранной матрицей перехода.



$\mathfrak{L}(A,l)$ - неавтономный линейный автомат,

$\{u_i\}$, , - знаки управляющей последовательности,

$\{y_i\}$ - знаки выходной последовательности,

$\{\vec{x}_i\}$ - векторы, задающие внутренние состояния линейного автомата

Закон функционирования

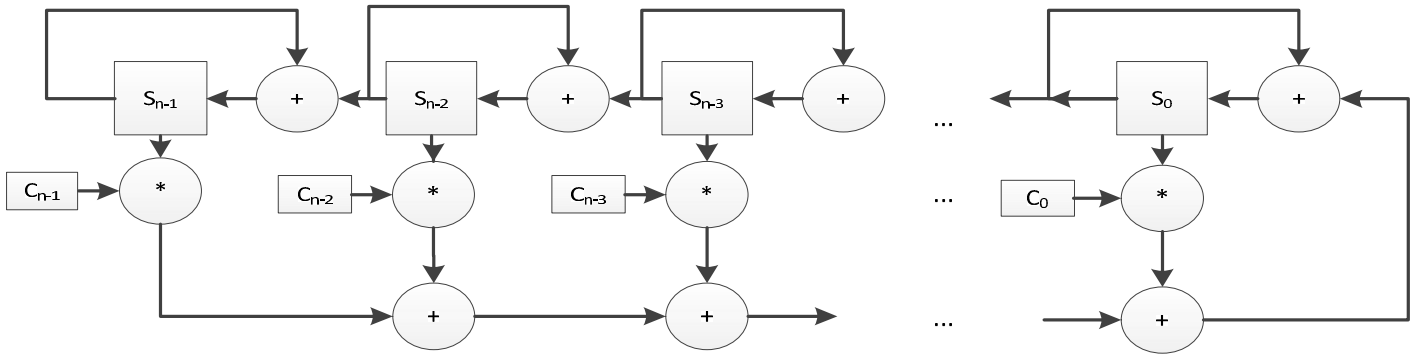
$$u_i \in \{0,1\},\ y_i = \vec{x}_i l^{\downarrow}$$

$$\overrightarrow{x_{i+1}} = \vec{x}_i A^{u_i J + (1-u_i)},\ i = 0,1,\ldots,$$

где $\vec{x}_i \in GF(q)^n$, $\overrightarrow{x_0}$ - вектор начального состояния автомата, A - матрица перехода, $A \in GF(q)_n$, $l^{\downarrow} \in GF(q)^n$ - вектор, задающий линейную функцию выхода автомата.

Если $A^J = A + E$, то вычислить $\vec{x}(A+E)$ проще чем $\vec{x}A^J$.

Прыжок по цикловой структуре **для линейного регистра сдвига**:



Матрица перехода $A + E = \begin{pmatrix} 1 & 0 & \cdots & 0 & c_{n-1} \\ 1 & 1 & \cdots & 0 & c_{n-2} \\ 0 & 1 & \cdots & 0 & c_{n-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_0 + 1 \end{pmatrix}$.

Как искать такие матрицы A?

В первую очередь, найдем $f(x) = \det(Ex - A)$?

Индекс J прыжка многочлена f: минимальный J, $J \in \mathbb{N}$

$$x^J \equiv x + 1 \bmod f(x)$$ (если такой J существует),

$f(x)$ - неприводимый многочлен.

Jansen C.J.A.: Partitions of polynomials: Stream ciphers based on jumping shift registers. In Cardinal J., Cerf N., Delgrange O., Markowitch O., eds.: 26th Symposium on Information Theory in the Benelux, Enschede, Werkgemeenschap voor Informatie en Communicatie theorie (2005) 277-284.

Jansen C.J.A.: Stream cipher design based on jumping finite state machines. (2005).

Построение примитивных $C(x)$, $\deg C = 2k$, $x^J \equiv x+1 \bmod C(x)$, $J = 2^k - \delta$, где δ небольшое натуральное число[1].

Если $C(x)$ существует, $C(x)$ делит $G_\delta(x)$, $\deg G_\delta(x) = (\delta+1)^2$:

$$G_\delta(x) = (x^{\delta+1} + x^\delta)^{\delta+1} + (x^{\delta+1} + x^\delta)^\delta + x.$$

Найти в разложении $G_\delta(x)$ примитивные сомножители $F(x)$, $\deg F = n$,

$$x^{2^k-\delta} + x + 1 \equiv 0 \bmod F(x).$$

Метод можно адаптировать для поиска многочленов заданной степени n с индексом прыжка J вида $J = 2^{an/b} \pm \delta$, где a, b, δ, $a < b$.

[1] *Babbage S, Dodd M.: Finding characteristic polynomials with jump indices. 2006.*

Каскады прыгающих линейных автоматов.

2^k полноцикловых линейных регистров сдвига с характеристическими многочленами $C(x)$ и «независимым» управлением

$$x^{2^{(n-k)/2}-\delta} \equiv x+1 \bmod C(x).$$

В каждый такт: либо один шаг, либо прыжок вперед на $2^{(n-k)/2}-\delta$ шагов.

Как искать такие $C(x)$?

$C(x)$ делит [2] многочлен$(x^{\delta+1}+x^{\delta})^{2^k(\delta+1)}+(x^{\delta+1}+x^{\delta})^{2^k\delta}+x.$

---

[2] *Колчин Д.А. Об одном методе построения каскадов «прыгающих» регистров сдвига, XVII всероссийская школа-коллоквиум по стохастическим методам, Кисловодск, 2010г.*

Начальное состояние каскада «прыгающих» регистров.

1. Начальное заполнение первого регистра ненулевое.
2. Начальное состояние $i+1$ регистра вырабатывается из начального состояния i регистра с использованием «прыжка» по цикловой структуре на $2^{n-k}-\delta^2$ шагов, $i=\overline{1,2^k-1}$.

Нет перекрытий в течение $2^{(n-k)/2}+\delta$ тактов работы.

Как реализовать прыжок на $2^{n-k}-\delta^2$ шагов?

$$A^{2^{n-k}-\delta^2}=(A+E)^{\delta+1}A^{\delta}+(A+E)^{\delta}.$$

многочлен от матрицы A степени $2\delta+1$.

Неудобство: искомый полноцикловый $C(x)$ содержит много слагаемых, он делит:

$(x^{\delta+1}+x^{\delta})^{\delta+1}+(x^{\delta+1}+x^{\delta})^{\delta}+x$ - для одного линейного автомата,

$(x^{\delta+1}+x^{\delta})^{2^k(\delta+1)}+(x^{\delta+1}+x^{\delta})^{2^k\delta}+x$ - для каскада линейных автоматов.

Сопровождающая матрица линейного регистра сдвига

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & c_{n-1} \\ 1 & 0 & 0 & \cdots & 0 & c_{n-2} \\ 0 & 1 & 0 & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \vdots & \ddots & 1 & 0 & c_1 \\ 0 & 0 & \cdots & 0 & 1 & c_0 \end{pmatrix}$$

Вопрос №2. Как найти просто реализуемую матрицу с заданным характеристическим многочленом?

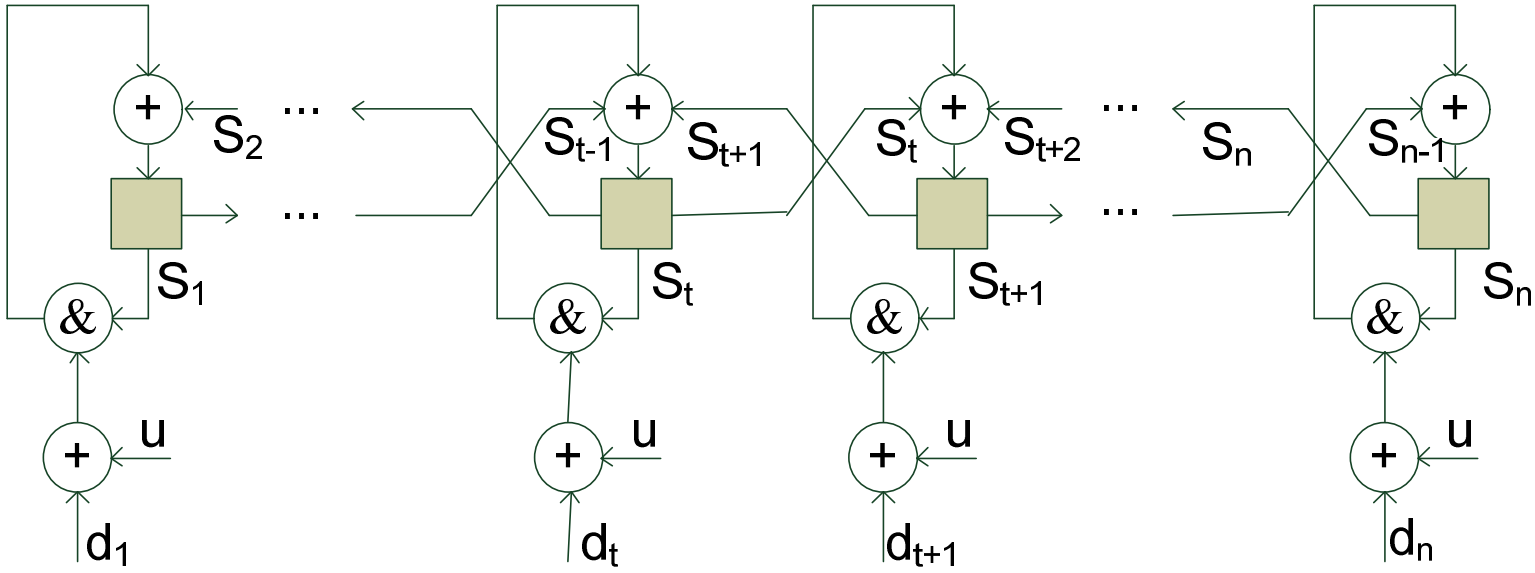
Примеры синтеза - криптографические алгоритмы Mickey, Mickey-128, Pomaranch.

$$\begin{pmatrix} d_n & 0 & 0 & \cdots & 0 & 1 \\ 1 & d_{n-1} & 0 & \cdots & 0 & t_{n-1} \\ 0 & 1 & d_{n-2} & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \vdots & \ddots & 1 & d_2 & t_2 \\ 0 & 0 & \cdots & 0 & 1 & d_1 + t_1 \end{pmatrix}$$

Характеристический многочлен:

$$C(x) = 1 + \sum_{i=0}^{n-1} t_i \prod_{j=i+1}^{n} (d_j + x), \text{ где } t_0 = 1.$$

Теория клеточных автоматов, позволяющая построить клеточный автомат с заданным характеристическим многочленом матрицы перехода.



сопровождающий вектор $[d_1, d_2, \ldots, d_n]$,

$$d_i = \begin{cases} 0, & \textit{инструкция}\ \text{"90"} \\ 1, & \textit{инструкция}\ \text{"150"} \end{cases}, \ 1 \le i \le n.$$

Матрицы переходов B и прыжков $B+E$ клеточного автомата имеют вид

$$B=\begin{pmatrix} d_n & 1 & 0 & \cdots & 0 \\ 1 & d_{n-1} & \ddots & \cdots & 0 \\ 0 & 1 & \cdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots & 1 \\ 0 & 0 & \cdots & 1 & d_1 \end{pmatrix},$$

$$B+E=\begin{pmatrix} d_n+1 & 1 & 0 & \cdots & 0 \\ 1 & d_{n-1}+1 & \ddots & \cdots & 0 \\ 0 & 1 & \cdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots & 1 \\ 0 & 0 & \cdots & 1 & d_1+1 \end{pmatrix}.$$

$$B+xE=\begin{pmatrix} d_n+x & 1 & 0 & \cdots & 0 \\ 1 & d_{n-1}+x & \ddots & \cdots & 0 \\ 0 & 1 & \cdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots & 1 \\ 0 & 0 & \cdots & 1 & d_1+x \end{pmatrix}$$

$\Delta_{r,s}(x)$, $1\le r\le s\le n$, минор матрицы $B+xE$, образованной строками и столбцами с номерами $r,r+1,...,s$, $\deg\Delta_{r,s}(x)=r-s+1$.

$$\Delta_{1,r}(x)=(x+d_{n-r+1})\Delta_{1,r-1}(x)+\Delta_{1,r-2}(x),\ r=n,n-1,...2,$$

$$\Delta_{1,2}(x)=(x+d_{n-1})\Delta_{1,1}(x)+1,\ \Delta_{1,1}(x)=x+d_n,$$

Алгоритм Эвклида: зная $\Delta_{1,n}(x)$ и $\Delta_{1,n-1}(x)$ найдем d_k, $1\le k\le n$.

Как найти $\Delta_{1,n-1}(x)$ для заданного характеристического многочлена $\Delta_{1,n}(x)$?

Многочлены $\Delta_{1,n-1}(x)$ и $\Delta_{2,n}(x)$ являются решением квадратного уравнения над полем $GF(2^n)$

$$g^2(x)+(x^2+x)\frac{\partial\Delta_{1,n}(x)}{\partial x}g(x)+1\equiv 0 \bmod \Delta_{1,n}(x),$$

где $\frac{\partial\Delta_{1,n}(x)}{\partial x}$ формальная производная.

Для неприводимого многочлена $g(x)$ над GF(2), всегда найдется матрица клеточного автомата с заданным $\Delta_{1,n}(x)=g(x)$.

Частное решение уравнения $A = P^{-1} \cdot B \cdot P$, где B - матрица клеточного автомата, A - сопровождающая матрица:

$$P = \begin{Bmatrix} \mathrm{Tr}(x\Delta_{1,0}) & \mathrm{Tr}(x^2\Delta_{1,0}) & \mathrm{Tr}(x^3\Delta_{1,0}) & \mathrm{Tr}(x^n\Delta_{1,0}) \\ \mathrm{Tr}(x\Delta_{1,1}) & \mathrm{Tr}(x^2\Delta_{1,1}) & \mathrm{Tr}(x^3\Delta_{1,1}) & \mathrm{Tr}(x^n\Delta_{1,1}) \\ \mathrm{Tr}(x\Delta_{1,2}) & \mathrm{Tr}(x^2\Delta_{1,2}) & \mathrm{Tr}(x^3\Delta_{1,2}) & \mathrm{Tr}(x^n\Delta_{1,2}) \\ \dots & \dots & \dots & \dots \\ \mathrm{Tr}(x\Delta_{1,n-1}) & \mathrm{Tr}(x^2\Delta_{1,n-1}) & \mathrm{Tr}(x^3\Delta_{1,n-1}) & \mathrm{Tr}(x^n\Delta_{1,n-1}) \end{Bmatrix},$$

где $\mathrm{Tr}(f(x)) = \sum_{j=1}^{n-1} f(x)^{2^j} \bmod g(x)$, $\Delta_{1,0} = 1$.

Cattell K. and Muzio J. C., An explicit similarity transform between cellular automata and LFSR matrices, 1998.

Другие результаты:

Cattell K. and Muzio J. C., Analysis of one-dimensional linear hybrid cellular automata over GF(q), 1996. - приведен недетерминированный алгоритм построения клеточного автомата над полем $GF(q)$ по заданному характеристическому многочлену

Sung-Jin Cho, Un-Sook Choi, Han-Doo Kim, Yoon-Hee Hwang, Jin-Gyoung Kim, and Seong-Hun Heo, New Synthesis of One-Dimensional 90/150 Linear Hybrid Group Cellular Automata, 2007 - детерминированный алгоритм с трудоемкостью $O(n^3)$, - модификация алгоритма Ланцоша приведения матрицы к трех-диагональному виду.

3. Явный вид решения уравнения подобия линейных автоматов с линейными функциями выхода

$\mathfrak{L}(A,l)$ линейный автомат,

$$\overrightarrow{x_{i+1}} = \vec{x_i}A,\ y_i = \vec{x_i}l^{\downarrow},\ i = 0,1,\ldots,$$

$$\vec{x_i} \in GF(q)^n,\ A \in GF(q)_n,\ l^{\downarrow} \in GF(q)^n.$$

Как найти базис, в котором автомат $\mathfrak{L}(A_1,l_1)$ будет представлен в виде автомата $\mathfrak{L}(A_2,l_2)$, для $A_1,A_2 \in GF(q)_n$, $l_1^{\downarrow},l_2^{\downarrow} \in GF(q)^n \setminus \{0^{\downarrow}\}$, A_1 и A_2 подобны?

$$A_2 = T^{-1} A_1 T,$$

$$\vec{l}_1 T = \vec{l}_2,$$

$$T \in GF(q)^n.$$

Матричное уравнение Сильвестра

$$AT + TB + Q = 0,$$

$$A \in GF(q)_n,\ T \in GF(q)_n,\ B \in GF(q)_n,\ Q \in GF(q)_n.$$

Зададим произвольный вектор $\vec{d} \in GF(q)^n$. Из системы уравнений следует, что матрица T удовлетворяет цепочке соотношений

$$TA_2 - A_1 T = 0 = d^{\downarrow}\vec{l}_2 - d^{\downarrow}\vec{l}_1 T,$$

$$(d^{\downarrow}\vec{l}_1 - A_1)T + TA_2 - d^{\downarrow}\vec{l}_2 = 0.$$

$$A = d^{\downarrow}\vec{l}_1 - A_1,\ \ B = A_2,\ \ Q = -d^{\downarrow}\vec{l}_2.$$

Явный вид решения $AT + TB + Q = 0$

Пусть матрицы A и $-B$ не имеют общих собственных значений,

$$p(t) = \sum_{s=0}^{n} p_s t^s = \det(A - xE).$$

Тогда

$$T = -p(-B)^{-1}\left(\sum_{s=0}^{n} p_s \sum_{k=1}^{s} (-1)^{k+1} A^{n-k} Q B^{k-1}\right), \text{ где } \sum_{k=1}^{0} A^{n-k} Q B^{k-1} = 0.$$

Условие для вектора $\vec{d} \in GF(q)^n$: характеристические многочлены матриц $A_1 - d^{\downarrow}\vec{l}_1$ и A_1 не имеют общих корней.

$\det(A_1 - Ex)$ неприводим то, достаточно, что бы выполнялось $(d, l_1) \neq 0$.

Спасибо за внимание!