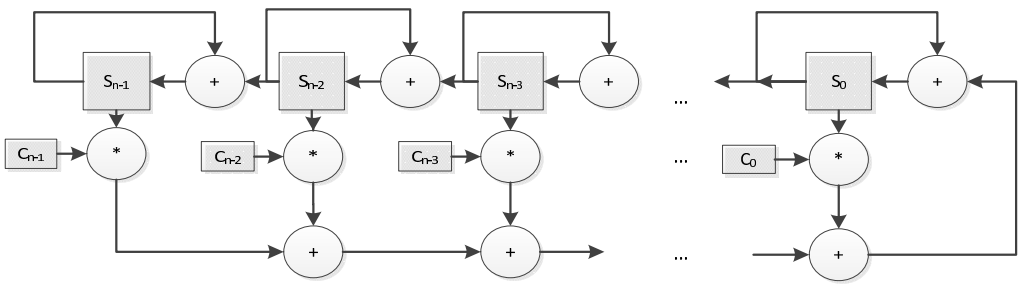
Прыгающие клеточные автоматы. Обзор результатов

1. Нахождение характеристических многочленов с заданным индексом прыжка

При синтезе неавтономных автоматов в некоторых случаях возникает необходимость гарантировать невозможность частичных перекрытий или пересечений различных траекторий состояний автомата на цикловой структуре. Одним из путей решения данной задачи является реализация прыжков по цикловой структуре для линейного автомата со специально подобранной матрицей перехода.

Пусть A - матрица перехода некоторого линейного автомата, не обязательно регистра сдвига, $f(x)$ - её характеристический многочлен, $f(x) = \det(Ex - A)$. Предположим, что для матрицы A выполнено соотношение $A^J = A + E$ для заданного значения J. Нетрудно заметить, что для такой матрицы A гораздо проще вычислить умножение вектора на матрицу $A + E$, чем последовательно J раз умножать матрицу A на вектор.

Метод прыжков по цикловой структуре может использоваться для синтеза блоков выработки псевдослучайных последовательностей, основанных на неавтономных линейных автоматах. Выбор закона сдвига определяется битом управляющей последовательности, в зависимости от которого в каждый такт работы реализуется сдвиг по цикловой структуре автомата либо на один шаг вперед, либо прыжок по цикловой структуре сразу на J шагов. Нетрудно убедиться, что для линейного регистра сдвига реализация прыжка по цикловой структуре имеет вид:



Матрица перехода в этом случае имеет вид:

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

Основной вопрос – как искать такие матрицы A?

Ниже будут рассмотрены, в основном, линейные преобразования над полем $GF(2)$, отметим, однако, что многие приведенные результаты, будут справедливы для произвольного конечного поля.

Определение ([13,14]**).** Пусть $f(x)$ - неприводимый многочлен над $GF(2)$. Индексом J прыжка многочлена f называется минимальный J, $J \in \mathbb{N}$, удовлетворяющий уравнению $x^J \equiv x+1 \bmod f(x)$, если такой J существует.

Замечание. Индекс прыжка всегда существует для примитивных многочленов. Для неприводимых трехчленов вида $x^n + x + 1$ индекс прыжка равен n.

Метод построения примитивных многочленов $C(x)$ степени $n = 2k$ имеющих индекс прыжка J, $J = 2^k - \delta$, где δ небольшое натуральное число описан в [3,4]. Установлено, что многочлен $C(x)$, если он существует, должен быть делителем многочлена $G_\delta(x)$ степени $(\delta+1)^2$:

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

Для нахождения характеристического многочлена матрицы A может быть использован следующий алгоритм:

- разложить на множители над полем $GF(2)$ многочлен $G_\delta(x)$, выделить его неприводимый сомножитель $F(x)$ заданной степени n;

- для выбранного $F(x)$ проверить его примитивность и выполнимость сравнения $x^{2^k-\delta} + x + 1 \equiv 0 \bmod F(x)$;

- если указанные условия выполнены, то искомый многочлен найден, $C(x) = F(x)$. Если условия не выполнены, то из разложения многочлена $G_\delta(x)$ нужно выбрать другой неприводимый сомножитель $F(x)$ степени n и повторить проверку. В случае, если все неприводимые сомножители $F(x)$ степени n были рассмотрены, нужно изменить δ и повторить вычисления.

Там же в [3] кратко сформулировано, что используемый метод можно адаптировать для поиска многочленов заданной степени n с индексом прыжка J вида $J = 2^{an/b} \pm \delta$, где a, b, δ, $a < b$ небольшие натуральные числа.

С целью увеличения количества вырабатываемых в каждый такт работы знаков псевдослучайной последовательности в [1] предложено использовать в качестве генератора псевдослучайной последовательности каскад из 2^k независимо «прыгающих» полноцикловых линейных регистров сдвига длины n с одинаковыми характеристическими многочленами. В каждый такт работы каждый регистр сдвига осуществляет либо шаг вперед по цикловой структуре, либо совершает прыжок вперед на $2^{(n-k)/2} - \delta$ шагов, при этом сопровождающая матрица A удовлетворяет условию $A + E = A^{2^{(n-k)/2} - \delta}$. Показано, что в этом случае характеристический многочлен полноциклового регистра сдвига делит многочлен

$$(x^{\delta+1} + x^\delta)^{2^k(\delta+1)} + (x^{\delta+1} + x^\delta)^{2^k \delta} + x, \qquad (1.1)$$

предложен способ выбора начального состояния каскада «прыгающих» регистров с гарантированным отсутствием повторов их внутренних состояний в течение $2^{(n-k)/2} + \delta$ тактов работы. Для этого начальное заполнение первого регистра должно быть ненулевым, начальное состояние $i+1$ регистра вырабатывается из начального состояния i регистра с использованием «прыжка» по цикловой структуре на $2^{n-k} - \delta^2$ шагов, $i = \overline{1, 2^k - 1}$. Способ вычисления указанного прыжка основан на равенстве

$$A^{2^{n-k} - \delta^2} = (A + E)^{\delta+1} A^\delta + (A + E)^\delta. \qquad (1.2)$$

Как замечено в [1], поскольку правая часть равенства (1.2) представляет собой многочлен от матрицы A степени $2\delta+1$, то для вычисления заполнения регистра сдвига через $2^{n-k}-\delta^2$ тактов, потребуется проработка регистра в течение $2\delta+1$ тактов с подсуммированием, в некоторые такты работы, заполнения регистра в массив памяти.

2. Методы синтеза просто реализуемых линейных автоматов с заданным характеристическим многочленом

Сомножители, получаемые из разложений многочленов

$G_\delta(x)=(x^{\delta+1}+x^\delta)^{\delta+1}+(x^{\delta+1}+x^\delta)^\delta+x$, либо $(x^{\delta+1}+x^\delta)^{2^k(\delta+1)}+(x^{\delta+1}+x^\delta)^{2^k\delta}+x$,

как правило, содержат большое количество слагаемых, не позволяющее эффективно реализовать сдвиг и прыжок соответствующего линейного регистра сдвига. Используются различные методы выбора просто реализуемых линейных преобразований, имеющих заданный характеристический многочлен ([4,6,9,11]). В качестве примера рассмотрим криптографические алгоритмы Mickey, Mickey-128 [4], Pomaranch [11] для которых с помощью указанного метода были найдены характеристический многочлен заданной степени с заданным индексом прыжка. Матрицы перехода линейного автомата имеют вид

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

Характеристический многочлен указанной выше матрицы имеет вид

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

В работах [7,8,9,15,16] развита теория клеточных автоматов, позволяющая построить клеточный автомат с заданным характеристическим

многочленом матрицы перехода. Клеточные автоматы являются частным случаем автоматов, и задаются одномерным массивом клеток, которые могут взаимодействовать только с соседними клетками. Для каждой клетки можно задать $2^{2^3} = 256$ различных инструкций выработки её состояния в следующий такт в зависимости от её состояния и состояния соседних клеток, однако, если рассматривать только регулярные автоматы, в поле зрения остаются только линейные инструкции «90» и «150». Числа 90 и 150 являются численным представлением таблицы истинности соответствующих функций от 3 переменных: в соответствии с инструкцией «90» состояние клетки в такт $t+1$ является суммой по модулю 2 состояний её двух соседей в такт t работы клеточного автомата. В соответствии с инструкцией «150» состояние клетки в такт $t+1$ есть сумма её состояния и состояний её соседей в такт t.

Введем сопровождающий вектор $[d_1, d_2, \ldots, d_n]$ для представления клеточного автомата, где d_i равны 0, если клетка i использует инструкцию «90», либо 1, если клетка i использует инструкцию «150», $1 \le i \le n$. В этих обозначениях матрицы переходов B и прыжков $B+E$ клеточного автомата имеют вид

$$B = \begin{pmatrix} d_n & 1 & 0 & \cdots & 0 \\ 1 & d_{n-1} & \ddots & \cdots & 0 \\ 0 & 1 & \cdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots & 1 \\ 0 & 0 & \cdots & 1 & d_1 \end{pmatrix}, \qquad (2.1)$$

$$B+E = \begin{pmatrix} d_n+1 & 1 & 0 & \cdots & 0 \\ 1 & d_{n-1}+1 & \ddots & \cdots & 0 \\ 0 & 1 & \cdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots & 1 \\ 0 & 0 & \cdots & 1 & d_1+1 \end{pmatrix}, \qquad (2.2)$$

Хорошо известно, что существует взаимно-однозначное соответствие между регистрами сдвига с линейной обратной связью и их характеристическими многочленами. В тоже время, нетрудно видеть, что

характеристические многочлены матриц перехода B с управляющими векторами $(d_1, d_2, \ldots, d_n)$ и $(d_n, d_{n-1}, \ldots, d_1)$ совпадают, другими словами, для клеточных автоматов аналогичное взаимно-однозначное соответствие не выполнено.

Обозначим через $\Delta_{r,s}(x)$, $1 \le r \le s \le n$, многочлен степени $s-r+1$, представляющий собой минор матрицы $B + x \cdot E$, образованной строками и столбцами с номерами $r, r+1, ..., s$. Из соотношений

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

$$\Delta_{1,2}(x) = (x + d_{n-1})\Delta_{1,1}(x) + 1, \;\; \Delta_{1,1}(x) = x + d_n, \qquad (2.3)$$

следует, что, зная многочлены $\Delta_{1,n}(x)$ и $\Delta_{1,n-1}(x)$, с помощью алгоритма Эвклида можно вычислить все значения d_k, $1 \le k \le n$. Задача нахождения $\Delta_{1,n-1}(x)$ для заданного характеристического многочлена $\Delta_{1,n}(x)$ решена в работе [9], где показано, что многочлены $\Delta_{1,n-1}(x)$ и $\Delta_{2,n}(x)$ являются решением квадратного уравнения над полем $GF(2^n)$

$$g^2(x) + (x^2 + x)\frac{\partial \Delta_{1,n}(x)}{\partial x} g(x) + 1 \equiv 0 \bmod \Delta_{1,n}(x), \qquad (2.4)$$

где $\dfrac{\partial \Delta_{1,n}(x)}{\partial x}$ формальная производная многочлена $\Delta_{1,n}(x)$. Там же установлено, что для неприводимого многочлена $g(x)$ над полем GF(2), $\deg g = n$ всегда найдется матрица вида (2.1), такая что $\Delta_{1,n}(x) = g(x)$. В [10] описан метод решения квадратных уравнений над полем GF(2^n) с трудоемкостью $O(n^7)$.

В [7] получено частное решение уравнения подобия $A = P^{-1} \cdot B \cdot P$, где B - матрица вида (2.1), A - сопровождающая матрица для многочлена g:

$$P = \begin{Bmatrix} \mathrm{Tr}(x\Delta_{1,0}) & \mathrm{Tr}(x^2\Delta_{1,0}) & \mathrm{Tr}(x^3\Delta_{1,0}) & \mathrm{Tr}(x^n\Delta_{1,0}) \\ \mathrm{Tr}(x\Delta_{1,1}) & \mathrm{Tr}(x^2\Delta_{1,1}) & \mathrm{Tr}(x^3\Delta_{1,1}) & \mathrm{Tr}(x^n\Delta_{1,1}) \\ \mathrm{Tr}(x\Delta_{1,2}) & \mathrm{Tr}(x^2\Delta_{1,2}) & \mathrm{Tr}(x^3\Delta_{1,2}) & \mathrm{Tr}(x^n\Delta_{1,2}) \\ \ldots & \ldots & \ldots & \ldots \\ \mathrm{Tr}(x\Delta_{1,n-1}) & \mathrm{Tr}(x^2\Delta_{1,n-1}) & \mathrm{Tr}(x^3\Delta_{1,n-1}) & \mathrm{Tr}(x^n\Delta_{1,n-1}) \end{Bmatrix}, \qquad (2.5)$$

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

В [8] рассматривались методы построения клеточного автомата для заданного неприводимого многочлена в случае произвольного конечного поля. Приведен недетерминированный алгоритм построения клеточного автомата над полем $GF(q)$ по заданному характеристическому многочлену. В [19] предложен вероятностный алгоритм с трудоемкостью $O(n^3)$, являющийся модификацией алгоритма Ланцоша приведения матрицы к трех диагональному виду и позволяющий выполнять преобразование линейного регистра сдвига в клеточный автомат для достаточно больших n, например, для $n \sim 10^4$.

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

Пусть $\mathfrak{L}(A,l)$ линейный автомат, вырабатывающий знаки $\{y_i\}$ псевдослучайной последовательности в соответствии с соотношениями:

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

$$y_i = \vec{x_i} l^{\downarrow},\ i = 0,1,\ldots, \qquad (3.1)$$

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

Рассмотрим задачу нахождения линейного преобразования пространства $GF(q)^n$, отображающего автомат $\mathfrak{L}(A_1,l_1)$ в автомат $\mathfrak{L}(A_2,l_2)$, где l_1, l_2 - заданные ненулевые векторы длины n над полем $GF(q)$, A_1 и A_2 заданные матрицы размера $n \times n$, причем A_1 и A_2 подобны. Нахождение линейного преобразования эквивалентно решению системы матричных уравнений

$$A_2 = T^{-1} A_1 T,\quad \vec{l_1} T = \vec{l_2}, \qquad (3.2)$$

относительно неизвестной матрицы T, $T \in GF(q)^n$.

Систему (3.2) можно свести к матричному уравнению Сильвестра

$$AT + TB + Q = 0, \tag{3.3}$$

где $A \in GF(q)_n$, $T \in GF(q)_n$, $B \in GF(q)_n$, $Q \in GF(q)_n$, следующим образом. Зададим произвольный вектор $\vec{d} \in GF(q)^n$. Из системы уравнений (3.2) следует, что матрица T удовлетворяет цепочке соотношений

$$TA_2 - A_1T = 0 = d^{\downarrow}\vec{l}_2 - d^{\downarrow}\vec{l}_1T,$$

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

Последнее соотношение является матричным уравнением Сильвестра (3.3), где $A = d^{\downarrow}\vec{l}_1 - A_1$, $B = A_2$, $Q = -d^{\downarrow}\vec{l}_2$.

В работах [2, 5, 12, 13] предложен способ нахождения в явном виде решение матричного уравнения $AT + TB + Q = 0$ над полем действительных чисел или над конечным полем.

Утверждение [2]. Пусть матрицы A и $-B$ не имеют общих собственных значений, $p(t) = \sum_{s=0}^{n} p_s t^s$ характеристический многочлен матрицы A над полем P. Тогда решение уравнения (3.3) имеет вид

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

Следует заметить, что условие, что матрицы A и $-B$ не имеют общих собственных значений необходимо для обеспечения невырожденности матрицы $p(-B)$. С учетом данного замечания вектор $\vec{d} \in GF(q)^n$ должен выбираться таким образом, чтобы характеристические многочлены матриц $A_1 - d^{\downarrow}\vec{l}_1$ и A_1 не имели общих корней. В частности, данное условие будет выполнено, если $(d, l_1) \neq 0$ и характеристический многочлен матрицы A_1 неприводим.

Автор: Дрелихов Владимир Олегович

ЛИТЕРАТУРА

1. Колчин Д.А. Об одном методе построения каскадов «прыгающих» регистров сдвига, XVII всероссийская школа-коллоквиум по стохастическим методам. Посвящается 80-летию академика Ю.В. Прохорова. XI всероссийский симпозиум по прикладной и промышленной математике. Кисловодск. 1-8 мая 2010г. http://www.tvp.ru/conferen/vsppm11/kidag151.pdf
2. Шестопал В. Е., Решение матричного уравнения AX—XB=C, М. «Наука», 1976 г., Математические заметки, т. 19, № 3 (1976), 449—451.
3. Babbage S, Dodd M.: Finding characteristic polynomials with jump indices. (2006).
4. Babbage S.H., Dodd M.W., Streamciphers MICKEY and MICKEY-128, http://www.ecrypt.eu.org/stream.
5. Bartels R. H., Stewart G. W., Solution of the matrix equation AX + XB = C, Comm. ACM, 15 (1972), pp. 820 – 826.
6. Boaz Tsaban, Efficient Linear Feedback Shift Registers with Maximal Period, Finite Fields and Their Applications 8, 256-267 (2002)
7. Cattell K. and Muzio J. C., An explicit similarity transform between cellular automata and LFSR matrices, Finite Fields Their Appl.,vol.4, no. 3, pp. 239–251, Jul. 1998.
8. Cattell K. and Muzio J. C., Analysis of one-dimensional linear hybrid cellular automata over GF(q), IEEE Trans. Comput., vol. 45, no. 7, pp. 782–792, Jul. 1996.
9. Cattell K. and Muzio J.C., Synthesis of one-dimensional linear hybrid cellular automata," IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., vol.15, no.3. pp.325-335, 1996.
10. Chen C.L. Formulas for Solutions of Quadratic Equations over GF(2^m), IEEE Trans. Inform. Theory. 1982. V.28. №5. P.792-794.

11. Cid C., Gilbert H. , Johansson T., "Cryptanalysis of Pomaranch", ECRYPT Stream Cipher Project Report 2005/060. 2005, http://www.ecrypt.eu.org/stream/
12. Er-Chieh Ma, A finite series solution of the matrix equation AX −XB = C, S.I.A.M. J. on Appl. Math., 14 (1966) pp. 490-495.
13. 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.
14. Jansen C.J.A.: Stream cipher design based on jumping finite state machines. (2005).
15. Serra M. and Slater T., A Lanczos algorithm in a finite field and its application, J. Comb. Math. Comb. Comput., vol. 7, pp. 11–32,1990.
16. Serra M., Cattell K., Zhang S., Muzio J.C., Miller D.M., One-Dimensional Linear Hybrid Cellular Automata: Their Synthesis, Properties and Applications to Digital Circuits Testing Dept. of Computer Science University of Victoria. Victoria, B.C., Canada January 27, 2009
17. 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, IEEE trans. on computer-aided design of integrated circuits and systems, vol. 26, no. 9, pp. 1720-1724, Sep., 2007.