The paper investigates the multipurpose search in the design based on the approaches inspired by the natural systems. Innovative and modified search architecture containing multilevel evolution is suggested in the given paper. So the decision process is parallelized and the problem of the algorithm preliminary convergence is partly eliminated. The fundamental difference of the suggested method is the division of the search process into two stages and various algorithms for each of them. Tests and experiments show the application perspectiveness for the developed architectures. The time complexity of algorithms is ≈O(nlogn) in the best case and $O(n^3)$ in the worst case.

Key words: combined search, design, evolutionary computation.

УДК 519.716.32+519.854

О ПЕРИОДИЧЕСКИХ СВОЙСТВАХ ОДНОГО ВАРИАЦИОННО-КООРДИНАТНО ЛИНЕЙНОГО (ВКЛ-) ГЕНЕРАТОРА НАД КОЛЬЦОМ ВЫЧЕТОВ

***Мирослав Владимирович Заец**, сотрудник ФГУП «НИИ КВАНТ»,*
Тел.:(916) 475-31-06, e-mail: mirzaets@hotmail.com
http://www.rdi-kvant.ru

В данной статье рассматриваются периодические свойства последовательностей над примарным кольцом вычетов $\mathbf{Z}_{2^m}$, вырабатываемых автономным регистром сдвига, у которого функция обратной связи принадлежит одному классу функций, названных в настоящей статье «функции с вариационно-координатной линейностью». Регистр с такой функцией обратной связи также назван ВКЛ-генератором. Интерес в изучении данного класса функций обуславливается тем, что он содержит не полиномиальные функции, однако, имеет схожие свойства с классом полиномиальных.

Ключевые слова: период, линейные функции, линейная рекуррентная последовательность (ЛРП), вариационно-координатно линейные (ВКЛ) функции.


М.В. Заец

Введение

Одним из простейших способов выработки псевдослучайных последовательностей над произвольным коммутативным кольцом с единицей R является использование рекуррентного соотношения вида

$$u(i+1) = f(u(i)), i \geq 0,$$

где $f : R \to R$ преобразование кольца R. В этом случае первым возникающим вопросом является вопрос о длине подхода (дефекте) и периоде последовательности u. Наиболее изученным в этом плане случаем, является полиномиальный генератор, т.е. случай, когда функция f полиномиальна над R. При различных кольцах он довольно подробно рассматривался в работах [1; 2; 3] и др. В настоящей статье будут изучаться периодические свойства одного генератора над кольцом вычетов $\mathbf{Z}_{2^m}$, в котором используется функции с вариационно-координатной линейностью. Такой генератор будем называть ВКЛ-генератором. Функции с вариационно-координатной линейностью являются частным случаем функций с вариационно-координатной полиномиальностью [4; 5], которые в свою очередь в определенном смысле обобщают полиномиальные функции. Поэтому представляет интерес изучения генераторов с вариационно-координатно полиномиальными функциями.

Будем далее использовать следующие обозначения:

$F_{2^m}(n)$ - класс всех функций n переменных над кольцом вычетов $\mathbf{Z}_{2^m}$;

$P_{2^m}(n)$ - класс всех полиномиальных функций от n переменных над кольцом вычетов $\mathbf{Z}_{2^m}$;

$L_{2^m}(n)$ - класс всех линейных функций от n переменных над кольцом вычетов $\mathbf{Z}_{2^m}$;

$L_P(f(x))$ - множество всех линейных рекуррентных последовательностей (ЛРП-семейство) над полем $P = \mathbf{Z}_2$ с характеристическим многочленом $f(x)$;

$T(u), \Lambda(u)$ - период и длина подхода ЛРП u соответственно;

$v[\overline{s,k}]$ - отрезок значений ЛРП v, т.е. вектор $(v(s), v(s+1)..., v(k))$;

$(a,b), [a,b]$ - НОД и НОК соответственно целых чисел (либо многочленов) a и b;

$m_v(x)$ - минимальный многочлен ЛРП v.

Рассмотрим автономный регистр сдвига, изображенный на рисунке, имеющий множество состояний - $\mathbf{Z}_{2^m}^n, n, m \in \mathbf{N}$, $m > 1$, множество выходов - $\mathbf{Z}_{2^m}$ и функцией обратной связи $f(x,y) \in F_{2^m}(2)$. При этом $(u(0),...,u(n-1))$ – начальное состояние автомата и $u(i), i \geq n$ – его выходная последовательность. Регистр функционирует по закону:

$$u(i+n) = f(u(i), u(i+1)), i \geq 0.$$

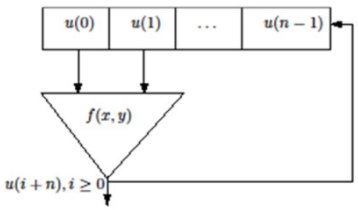

Рис. Регистр сдвига

Получаемая таким образом выходная последовательность является, очевидно, периодической в силу автономности регистра. В данной работе будет изучаться вопрос об оценке периода последовательности $\{u(i)\}$ в случае, когда функция обратной связи $f(x,y)$ принадлежит некоторому классу функций над кольцом $\mathbf{Z}_{2^m}$.

Если $a \in \mathbf{Z}_{2^m}$ обозначим через $\gamma_i(a) = a^{(i)}, i = 0,..., m-1,$ - i-ую двоичную координату a в двоичном разложении:

$$a = a^{(0)} + 2 \cdot a^{(1)} + ... + 2^{m-1} \cdot a^{(m-1)}.$$

Определение 1. *Функцию $f(x_1,...,x_n) \in F_{2^m}(n)$ будем называть вариационно-координатно линейной (ВКЛ-функцией) если для любого $i \in \{0,...,m-1\}$ существует линейная функция $p_i(x_1,...,x_n) \in L_{2^m}(n)$ такая, что при всех $\alpha \in \mathbf{Z}_{2^m}^n$ выполняется равенство:*

$$\gamma_i(f(\alpha)) = \gamma_i(p_i(\alpha)).$$

В таком случае $p_i(x_1,...,x_n)$ будем называть i-тым координатным многочленом ВКЛ-функции $f(x_1,...,x_n)$.

Класс всех ВКЛ-функций от n переменных над кольцом вычетов $\mathbf{Z}_{2^m}$ обозначим через $CL_{2^m}(n)$. В следующей теореме сформулируем без доказательства некоторые интересные свойства введенного класса функций.

Теорема 1. *Любая ВКЛ-функция $f \in CL_{2^m}(n)$ сохраняет отношение сравнимости по любому делителю 2^m, т.е. если $a_i \equiv b_i (\mathrm{mod}\, 2^k), i = 1,...,n, k \in \{1,...,m-1\}$, то*

$$f(a_1,...,a_n) \equiv f(b_1,...,b_n) (\mathrm{mod}\, 2^k).$$

Кроме того справедливо включение: $L_{2^m}(n) \subseteq CL_{2^m}(n)$ *и при* $m \geq 3$ *класс ВКЛ-функций* $CL_{2^m}(n)$ *содержит функции, не лежащие в классе полиномиальных* $P_{2^m}(n)$.

В данной работе будем использовать свойства линейных рекуррентных последовательностей над конечным полем, которые можно найти в [6]. Свойства полиномиальных функций, а также свойства так называемых ВКП-функций, которые являются обобщением ВКЛ-функций можно найти в работах [4; 5].

Определение 2. *Пусть* $\{u(i)\}$ *последовательность над кольцом* $\mathbf{Z}_{2^m}$. *Последовательность* $v_j(i) = \gamma_j(u(i))$, *где* $j \in \{0,...,m-1\}$, *будем называть j-ой координатной последовательностью последовательности* u.

В нашем случае выходная последовательность u – периодическая, поэтому и все ее координатные последовательности так же являются периодическими над полем $\mathbf{Z}_2$, а, следовательно, являются линейными рекуррентными последовательностями над указанным полем.

Следующая простая теорема устанавливает связи периодов и длин подхода координатных последовательностей $v_j, j = 0,...,m-1,$ с периодом и длиной подхода последовательности u.

Теорема 2. $T(u) = [T(v_0),...,T(v_{m-1})], \Lambda(u) = \max\{\Lambda(v_0),...,\Lambda(v_{m-1})\}$.

Следствие. *Для любого* $j \in \{0,...,m-1\}$: $T(v_j) \mid T(u)$.

Утверждение 3. *Пусть* $p(x,y) = x + by, b \in \mathbf{Z}_{2^m}$, *тогда, если* $2^j \mid b, j \in \{1,...,m-1\}$, *то:*

$$\gamma_j(p_j(x,y)) = x^{(j)} + b^{(j)}y^{(0)}.$$

В данной статье будем рассматривать случай, когда $f(x,y) \in CL_{2^m}(2)$, тогда ее координатные многочлены имеют вид:

$$\begin{cases} p_0(x,y) = a_0x + b_0y, \\ \vdots \\ p_{m-1}(x,y) = a_{m-1}x + b_{m-1}y, \end{cases}$$

где $a_i, b_i \in \mathbf{Z}_{2^m}, i = 0,...,m-1,$ при этом также будем считать, что они обладают свойством, описанным в утверждении 3. Это означает, что для любого $i \in \{1,...,m-1\}$ либо $a_i = 1, 2^i \mid b_i$ либо $b_i = 1, 2^i \mid a_i$.

Сформулируем и докажем теорему о виде ЛРП-семейств координатных последовательностей $v_j, j = 0,...,m-1,$ последовательности u, получаемой из регистра сдвига с ВКЛ-функцией $f(x,y)$ обратной связи указанного вида.

Теорема 4. *Пусть* $f(x,y) \in CL_{2^m}(2)$ *и имеет координатные многочлены* $p_j(x,y) = a_jx + b_jy, j = 0,...,m-1$. *Справедливы утверждения:*

1. $v_0 \in L_P(f_0(x)), f_0(x) = x^n + b_0^{(0)}x + a_0^{(0)}$;

2. если $a_j = 1, 2^j \mid b_j, j \in \{1,...,m-1\}$, *тогда:*

а) если $b_j^{(j)} = 0$ *или* $v_0[\overline{0,n-1}] = (0,...,0)$, *то* $v_j \in L_P(x^n + 1)$;

б) если $b_j^{(j)} = 1$, *то* $v_j \in L_P((x^n + 1)f_0(x))$

3. если $b_j = 1, 2^j \mid a_j, j \in \{1,...,m-1\}$, *тогда:*

а) если $a_j^{(j)} = 0$ *или* $v_0[\overline{0,n-1}] = (0,...,0)$, *то* $v_j \in L_P(x^n + x)$;

б) если $a_j^{(j)} = 1$, *то* $v_j \in L_P((x^n + x)f_0(x))$.

Доказательство.

1. Рассмотрим последовательность нулевой координаты v_0. Запишем согласно определению 2:

$$v_0(i+n) = \gamma_0(u(i+n)) = \gamma_0(f(u(i),u(i+1))) = \gamma_0(p_0(u(i),u(i+1))) =$$
$$= a_0^{(0)}\gamma_0(u(i)) + b_0^{(0)}\gamma_0(u(i+1)) = a_0^{(0)}v_0(i) + b_0^{(0)}v_0(i+1).$$

Следовательно:

$$v_0(i+n) = b_0^{(0)}v_0(i+1) + a_0^{(0)}v_0(i).$$

А значит, $v_0 \in L_P(f_0(x)), f_0(x) = x^n + b_0^{(0)}x + a_0^{(0)}$. В частности, это означает, что v_0 - ЛРП порядка *n*. Поэтому, если $v[\overline{0,n-1}] = (0,...,0)$, то $v_0 = 0$.

2. Пусть $a_j = 1,2^j \mid b_j, j \in \{1,...,m-1\}$, тогда:

$$v_j(i+n) = \gamma_j(u(i+n)) = \gamma_j(f(u(i),u(i+1))) = \gamma_j(p_j(u(i),u(i+1))) =$$
$$= \gamma_j(u(i)) + b_j^{(j)}\gamma_0(u(i+1)) = v_j(i) + b_j^{(j)}v_0(i+1).$$

И таким образом

$$v_j(i+n) = b_j^{(j)}v_0(i+1) + v_j(i), i \geq 0.$$

Следовательно:

$$(x^n+1)v_j = b_j^{(j)}x \cdot v_0$$

Отсюда, если $b_j^{(j)} = 0$, то $(x^n+1)v_j = 0$, а, значит, $v_j \in L_P(x^n+1)$. Если же $v_0[\overline{0,n-1}] = (0,...,0)$, то, как было отмечено выше, $v_0 = 0$, значит $(x^n+1)v_j = 0$ и тогда $v_j \in L_P(x^n+1)$.

Если $b_j^{(j)} = 1$, то:

$$f_0(x)(x^n+1)\cdot v_j = f_0(x)\cdot x \cdot v_0.$$

А так как $v_0 \in L_P(f_0(x))$, то $f_0(x)\cdot v_0 = 0$. Поэтому имеем:

$$f_0(x)(x^n+1)\cdot v_j = 0.$$

Отсюда, $v_j \in L_P((x^n+1)f_0(x))$.

3. Пусть $b_j = 1,2^j \mid a_j, j \in \{1,...,m-1\}$, тогда:

$$v_j(i+n) = \gamma_j(u(i+n)) = \gamma_j(f(u(i),u(i+1))) = \gamma_j(p_j(u(i),u(i+1))) =$$
$$= a_j^{(j)}\gamma_0(u(i)) + \gamma_j(u(i+1)) = a_j^{(j)}v_0(i) + v_j(i+1).$$

И имеем

$$v_j(i+n) = a_j^{(j)}v_0(i) + v_j(i+1), i \geq 0.$$

Откуда получим

$$(x^n+x)v_j = a_j^{(j)}v_0.$$

И аналогично пункту 2: если $a_j^{(j)} = 0$ или $v_0[\overline{0,n-1}] = (0,...,0)$, то $v_j \in L_P(x^n+x)$ и если $a_j^{(j)} = 1$, то $v_j \in L_P((x^n+x)f_0(x))$. □

Следствие. *В условиях теоремы 4 верны следующие утверждения:*

1. $T(v_0) \mid T(f_0(x))$

2. пусть $a_j = 1,2^j \mid b_j, j \in \{1,...,m-1\}$, *тогда если* $b_j^{(j)} = 0$ *или* $v_0[\overline{0,n-1}] = (0,...,0)$, *то* $T(v_j) \mid n$

3. пусть $b_j = 1, 2^j \mid a_j, j \in \{1,...,m-1\}$, *тогда если* $a_j^{(j)} = 0$ *или* $v_0[\overline{0,n-1}] = (0,...,0)$, *то* $T(v_j) \mid n-1$.

Приведем без доказательства утверждения, которые уточняют ЛРП-семейства координатных последовательностей в случае, когда многочлен нулевой координаты ВКЛ-функции имеет вид $p_0(x,y) = x + y$.

Утверждение 5. *Пусть* $f(x,y) \in CL_{2^m}(2)$ *и имеет координатные многочлены* $p_j(x,y) = a_j x + b_j y, j = 1,...,m-1, p_0(x,y) = x + y$. *Тогда:*

1. если $a_j = 1, 2^j \mid b_j, j \in \{1,...,m-1\}$, *то:*

$$v_j \in L_P(x^n + 1) \Leftrightarrow b_j^{(j)} = 0 \text{ или } v_0[\overline{0,n-1}] = (0,...,0).$$

2. если $b_j = 1, 2^j \mid a_j, j \in \{1,...,m-1\}$, *то:*

$$v_j \in L_P(x^n + x) \Leftrightarrow a_j^{(j)} = 0 \text{ или } v_0[\overline{0,n-1}] = (0,...,0).$$

Утверждение 6. *Пусть* $p_0(x,y) = x + y$ *и для некоторого* $j \in \{1,...,m-1\}$ *выполняется одно из условий:*

а) $p_j(x,y) = x + b_j y$, *где* $2^j \mid b_j, b_j^{(j)} = 1$;

б) $p_j(x,y) = a_j x + y$, *где* $2^j \mid a_j, a_j^{(j)} = 1$.

Тогда:

$$v_j \in L_P(x^n + x + 1) \Leftrightarrow v_j[\overline{0,n-1}] = v_0[\overline{0,n-1}].$$

Напомним, что согласно следствию к теореме 2: $T(v_0) \mid T(u)$, и следствию к теореме 4: $T(v_0) \mid T(f_0(x)), f_0(x) = x^n + b_0^{(0)} x + a_0^{(0)}$, поэтому чтобы обеспечить нижнюю границу для периода $T(u)$, будем всюду далее считать, что многочлен $f_0(x)$ является примитивным многочленом степени $n \geq 2$ над полем $\mathbf{Z}_2$, поскольку в этом случае (если $v_0[\overline{0,n-1}] \neq (0,...,0)$)

$$T(v_0) = T(f_0(x)) = 2^n - 1.$$

И тогда, $2^n - 1 \mid T(u)$. Также отметим, что при таком предположении $f_0(x) = x^n + x + 1$. А значит, всюду далее можно без ограничения общности считать, что $p_0(x,y) = x + y$.

Лемма 7. *Пусть* $a,b,d \in \mathrm{N}u$ $(a,b) = 1$, *тогда*

$$[[a,d],[b,d]] = a'b'd,$$

где $a' = \dfrac{a}{(a,d)}, b' = \dfrac{b}{(b,d)}$.

Докажем теорему об оценках периода и длины подхода ЛРП u, вырабатываемой ВКЛ-генератором при сказанных ранее предложениях.

Теорема 8. *Пусть* $f(x,y) \in CL_{2^m}(2)$ *и имеет координатные многочлены* $p_j(x,y) = a_j x + b_j y, j = 1,...,m-1, p_0(x,y) = x + y$, *при этом* $f_0(x) = x^n + x + 1$ *является примитивным многочленом над* $\mathbf{Z}_2$ *и* $v_0[\overline{0,n-1}] \neq (0,...,0)$. *Тогда справедливы утверждения:*

1. если для всех $j \in \{1,...,m-1\} : a_j = 1, 2^j \mid b_j$, *то:*

$$\Lambda(u) = 0, 2^n - 1 \mid T(u) \mid [n, 2^n - 1]$$

2. если для всех $j \in \{1,...,m-1\} : b_j = 1, 2^j \mid a_j$, *то:*

$$\Lambda(u) \le 1,2^n - 1 \mid T(u) \mid [n-1,2^n - 1]$$

3. если существуют $i, j \in \{1,...,m-1\}$ *такие, что* $a_i = 1,2^i \mid b_i$ *и* $b_j = 1,2^j \mid a_j$, *то:*

$$\Lambda(u) \le 1,2^n - 1 \mid T(u) \mid n_1 n_2 (2^n - 1),$$

где $n_1 = \dfrac{n}{(n,2^n - 1)}, n_2 = \dfrac{n-1}{(n-1,2^n - 1)}$.

Доказательство.

1. Пусть для любого $j \in \{1,...,m-1\} : a_j = 1,2^j \mid b_j$, тогда $v_j \in L_P((x^n + 1) f_0(x))$. А значит, $T(v_j) \mid T((x^n + 1) f_0(x))$ и $\Lambda(v_j) \le \Lambda((x^n + 1) f_0(x)), j = 1,...,m-1$. Заметим, что $\Lambda((x^n + 1) f_0(x)) = 0$, следовательно, $\Lambda(v_j) = 0, j = 1,...,m-1$.

Поскольку $f_0(x)$ неприводим над $\mathbf{Z}_2$, то $(x^n + 1, f_0(x)) = 1$. Отсюда

$$T((x^n + 1) f_0(x)) = [T(x^n + 1), T(f_0(x))] = [n, 2^n - 1].$$

Таким образом, для любого $j \in \{1,...,m-1\}$ $T(v_j) \mid [n, 2^n - 1]$ А стало быть, и $[T(v_0),...,T(v_{m-1})] \mid [n, 2^n - 1]$. Теперь, вспомним, что согласно теореме 2: $T(u) = [T(v_0),...,T(v_{m-1})], \Lambda(u) = \max\{\Lambda(v_0),...,\Lambda(v_{m-1})\}$, поэтому:

$$\Lambda(u) = 0,2^n - 1 \mid T(u) \mid [n, 2^n - 1].$$

2. Доказывается аналогично п. 1.

3. Условие данного пункта означает, что для всех $j \in \{1,...,m-1\}$: либо $a_j = 1,2^j \mid b_j$ либо $b_j = 1,2^j \mid a_j$. Поэтому в силу п. 1, 2, для всех $j \in \{1,...,m-1\}$: либо $T(v_j) \mid [n, 2^n - 1], \Lambda(v_j) = 0$ либо $T(v_j) \mid [n-1, 2^n - 1], \Lambda(v_j) \le 1$. Отсюда:

$$T(u) = [T(v_0),...,T(v_{m-1})] \mid [[n, 2^n - 1], [n-1, 2^n - 1]], \Lambda(u) = \max\{\Lambda(v_0),...,\Lambda(v_{m-1})\} \le 1$$

И тогда, воспользовавшись леммой 7, получим:

$$[[n, 2^n - 1], [n-1, 2^n - 1]] = n_1 n_2 (2^n - 1),$$

где $n_1 = \dfrac{n}{(n,2^n - 1)}, n_2 = \dfrac{n-1}{(n-1,2^n - 1)}$. □

Итак, данная теорема говорит о верхней и нижней оценках периода вырабатываемой последовательности u, в предположении, что последовательность нулевой координаты v_0 является ЛРП максимального периода над полем $\mathbf{Z}_2$ (или что то же самое, $f_0(x)$ является примитивным многочленом и v_0 имеет ненулевое начальное заполнение). Соответственно интересным представляется вопрос о нахождении достаточных условий достижения верхней границы для периода $T(u)$. Для этого введем некоторые обозначения.

Пусть $\mathbf{v} = (a_0,...,a_{n-1}) \in P^n, P = \mathbf{Z}_2$. Обозначим через $f_{\mathbf{v}}(x)$ многочлен степени не выше $n-1$, определяемый по формуле:

$$f_{\mathbf{v}}(x) = \sum_{i=0}^{n-1} a_i x^{n-1-i}.$$

Заметим отсюда очевидное свойство: для любых векторов $\mathbf{v}, \mathbf{w} \in P^n$

$$f_{\mathbf{v}+\mathbf{w}}(x) = f_{\mathbf{v}}(x) + f_{\mathbf{w}}(x).$$

Обозначим также, через $RS(\mathbf{v})$ - вектор, полученный из вектора $\mathbf{v}$ циклическим сдвигом влево на одну координату, то есть вектор:

$$RS(\mathbf{v}) = (a_1,...,a_{n-1},a_0).$$

Лемма 9. *Пусть* $v \in L_P(x^m+1), m \in \mathbf{N}$ *и* e^{x^m+1} *- импульсная последовательность данного семейства, тогда:*

$$v = f_{\mathbf{v}}(x) \cdot e^{x^m+1},$$

где $\mathbf{v} = v[\overline{0,m-1}]$.

Теорема 10. *Пусть* $f(x,y) \in CL_{2^m}(2)$ *и имеет координатные многочлены* $p_j(x,y) = a_j x + b_j y, j = 1,...,m-1, p_0(x,y) = x + y$, *при этом* $f_0(x) = x^n + x + 1$ *является примитивным многочленом над* $\mathbf{Z}_2$ *и* $v_0[\overline{0,n-1}] \neq (0,...,0)$. *Тогда справедливы утверждения:*

1. если для $j \in \{1,...,m-1\} : a_j = 1, 2^j \mid b_j$ *и* $b_j^{(j)} = 1$, *верно:*

$$(x^n + 1, f_{RS(\mathbf{v}_j)}(x) + f_{RS(\mathbf{v}_0)}(x)) = 1,$$

где $\mathbf{v}_j = v_j[\overline{0,n-1}], \mathbf{v}_0 = v_0[\overline{0,n-1}]$, *то*

$$T(v_j) = [n, 2^n - 1].$$

2. если для $j \in \{1,...,m-1\} : b_j = 1, 2^j \mid a_j$ *и* $a_j^{(j)} = 1$, *верно:*

$$(x^{n-1} + 1, f_{\mathbf{v}_j}(x) + f_{\mathbf{v}_0}(x)) = 1,$$

где $\mathbf{v}_j = v_j[\overline{0,n-1}], \mathbf{v}_0 = v_0[\overline{0,n-1}]$, *то:*

$$T(v_j) = [n-1, 2^n - 1].$$

Доказательство. Пусть выполнены условия пункта 1, докажем, что тогда $T(v_j) = [n, 2^n - 1]$. Рассмотрим последовательность:

$$w = (x^n + x + 1)v_j.$$

В соответствии с теоремой 4: $w \in L_P(x^n + 1)$, а значит, w является ЛРП порядка n. Используя рассуждения, аналогичные доказательству теоремы 4, легко показать, что при этом:

$$w(i) = v_j(i+1) + v_0(i+1), i \geq 0.$$

Следовательно, $w[\overline{0,n-1}] = (v_j(1) + v_0(1),..., v_j(n) + v_0(n))$.

Согласно доказанному в теореме 4: $v_j(n) = v_j(0) + v_0(1)$, и так как $v_0(n) = v_0(1) + v_0(0)$, то:

$$v_j(n) + v_0(n) = v_j(0) + v_0(0).$$

Поэтому

$$w[\overline{0,n-1}] = (v_j(1) + v_0(1),..., v_j(n-1) + v_0(n-1), v_j(0) + v_0(0)).$$

Пусть e^{x^n+1} - импульсная последовательность ЛПР-семейства $L_P(x^n + 1)$, тогда согласно лемме 9 последовательность w может быть представлена следующим образом:

$$w = f_{\mathbf{w}}(x) \cdot e^{x^n+1},$$

где $\mathbf{w} = w[\overline{0,n-1}]$. Теперь заметим, что вектор $\mathbf{w}$ можно представить в виде суммы двух векторов:

$$\mathbf{w} = (v_j(1),..., v_j(n-1), v_j(0)) + (v_0(1),..., v_0(n-1), v_0(0)),$$

при этом:

$$(v_j(1),..., v_j(n-1), v_j(0)) = RS(v_j(0),..., v_j(n-1)) = RS(\mathbf{v}_j),$$

$$(v_0(1),..., v_0(n-1), v_0(0)) = RS(v_0(0),..., v_0(n-1)) = RS(\mathbf{v}_0),$$

где $\mathbf{v}_j = v_j[\overline{0,n-1}], \mathbf{v}_0 = v_0[\overline{0,n-1}]$. Поэтому $f_{\mathbf{w}}(x) = f_{RS(\mathbf{v}_j)}(x) + f_{RS(\mathbf{v}_0)}(x)$, и тогда из условия следует, что $(x^n+1, f_{\mathbf{w}}(x)) = 1$. А значит:

$$m_w(x) = \frac{m_{e^{x^n+1}}(x)}{(m_{e^{x^n+1}}(x), f_{\mathbf{w}}(x))} = \frac{x^n+1}{(x^n+1, f_{\mathbf{w}}(x))} = x^n+1.$$

Таким образом, имеем, что для последовательности w в условиях теоремы $m_w(x) = x^n+1$. При этом:

• $w = (x^n+x+1)v_j \neq 0$, в силу утверждения 6, поскольку $b_j^{(j)} = 1$ и $v_j[\overline{0,n-1}] \neq v_0[\overline{0,n-1}]$ (последнее верно, так как в противном случае $f_{\mathbf{w}}(x) = 0$ и $(x^n+1, f_{\mathbf{w}}(x)) \neq 1$);

• $\left(x^n+1\right)v_j \neq 0$, в силу утверждения 5, поскольку $b_j^{(j)} \neq 0$ и $v_0[\overline{0,n-1}] \neq (0,...,0)$;

• многочлен x^n+x+1 неприводим над $\mathbf{Z}_2$.

Следовательно, $x^n+x+1 \mid m_{v_j}(x)$. С другой стороны:

$$m_w(x) = \frac{m_{v_j}(x)}{(x^n+x+1, m_{v_j}(x))},$$

а значит:

$$m_{v_j}(x) = m_w(x) \cdot \left(x^n+x+1, m_{v_j}(x)\right) = m_w(x)(x^n+x+1) = (x^n+1)(x^n+x+1).$$

Итак, имеем: $m_{v_j}(x) = (x^n+1)(x^n+x+1)$ и отсюда следует, что

$$T(v_j) = T(m_{v_j}(x)) = [n, 2^n-1].$$

Пункт 2 теоремы доказывается аналогичным образом. □

Следствие. *Пусть* $f(x,y) \in CL_{2^m}(2)$ *и имеет координатные многочлены* $p_j(x,y) = a_j x + b_j y, j = 1,...,m-1, p_0(x,y) = x+y$, *при этом* $f_0(x) = x^n+x+1$ *является примитивным многочленом над* $\mathbf{Z}_2$ *и* $v_0[\overline{0,n-1}] \neq (0,...,0)$. *Тогда справедливы утверждения:*

1. если для всех $j \in \{1,...,m-1\} : a_j = 1, 2^j \mid b_j$ *и хотя бы для одной из координатных последовательностей выполняется п. 1 теоремы 10, то:*

$$T(u) = [n, 2^n-1].$$

2. если для всех $j \in \{1,...,m-1\} : b_j = 1, 2^j \mid a_j$, *и хотя бы для одной из разрядных последовательностей выполняется п. 2 теоремы 10, то:*

$$T(u) = [n-1, 2^n-1].$$

3. если существуют две такие координатные последовательности, что для одной из них выполнено условие 1 теоремы, а для другой условие 2, то

$$T(u) = n_1 n_2 (2^n-1),$$

где $n_1 = \frac{n}{(n, 2^n-1)}, n_2 = \frac{n-1}{(n-1, 2^n-1)}$.

Заключение

Автор считает, что в данной работе новыми являются следующие положения и результаты: оценка периода и длины подхода линейных рекуррент, вырабатываемых вариационно-координатно линейным (ВКЛ-) генератором, достаточные условия достижимости верхней оценки периода. Изучение функций с вариационно-координатной

полиномиальностью (ВКП-функций) в работах [4; 5], позволило обобщить некоторые свойства полиномиальных функций. Это привело к задаче обобщения результатов о полиномиальных генераторах на случай таких функций. В представленной работе впервые был рассмотрен генератор, в котором используются вариационно-координатно линейные функции – частный случай ВКП-функций, у которых координатные многочлены являются линейными. Интерес к данной задаче заключает также и в том, что в классе всех ВКЛ-функций содержатся и неполиномиальные функции, что заведомо позволяет дать некоторое обобщение полиномиального случая.

Литература

1. *Ермилов Д.М. Козлитин О.А.* Цикловая структура полиномиального генератора над кольцом Галуа // Матем. вопр. Криптографии. 2013. Т. 4. № 1. С. 27–57.

2. *Козлитин О.А.* Полиномиальные преобразования GEO-кольца простой характеристики // Дискретная математика. 2004. Т. 16. Вып. 3. С. 105-117.

3. *Нечаев А.А.* Полиномиальные преобразования конечных коммутативных локальных колец главных идеалов // Мат. заметки. 1980. Т. 27, Вып. 6. С. 885-899.

4. Заец М.В., Никонов В.Г., Шишков А.Б. Функции с вариационно-координатной полиномиальностью и их свойства. // Открытое образование. 2012. № 3. С. 57-61.

5. *Заец М.В., Никонов В.Г., Шишков А.Б.* Класс функций с вариационно-координатной полиномиальностью над кольцом $\mathbb{Z}_{2^m}$ и его обобщение // Матем. вопр. криптографии. 2013. Т. 4. № 3. С. 19-45.

6. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра. Т. 2. – М.: Гелиос-АРВ, 2003. – 414 с.

About periodic properties of one variative-coordinate linear(vcl-) generator over ring of residues $\mathbf{Z}_{2^m}$

***Miroslav Vladimirovich Zayets**, Associate*
Federal Sate Unitary Enterprise Kvant Research Institute

The article considers periodic properties of sequences over primary ring of residues $\mathbf{Z}_{2^m}$, generated by autonomous shift register, which feedback function belongs to one class of functions, called in the present article «functions with variative-coordinate linearity». The register with such feedback function is also called VCL-generator. The interest in studying the given class of functions is based on that it doesn't contain polynomial functions, but has some similar properties.

Key words: period, linear functions, linear recurrent sequence, variative-coordinate linear (VCL) functions.

УДК: 378.162.3

МАШИННОЕ ОБУЧЕНИЕ В ЭКСПЕРТНЫХ СИСТЕМАХ: ПОДГОТОВКА СПЕЦИАЛИСТОВ

***Александр Викторович Шмид**, д-р.техн.наук, профессор,*
председатель правления
Тел.: +7(495) 319-58-09, e-mail: ashmid@ec-leasing.ru
***Кирилл Анатольевич Лычагин**, начальник сектора*
Тел.: +7 (495) 781-22-12, e-mail: klychagin@ec-leasing.ru
ЗАО «ЕС-лизинг»
http://www.ec-leasing.ru