

О СЛОЖНОСТИ МЕТОДА ФОРМАЛЬНОГО КОДИРОВАНИЯ ПРИ АНАЛИЗЕ ГЕНЕРАТОРА С ПОЛНОЦИКЛОВОЙ ФУНКЦИЕЙ ПЕРЕХОДОВ¹

В. М. Фомичёв

Институт проблем информатики РАН, г. Москва, Россия

E-mail: fomichev@nm.ru

Исследованы генераторы гаммы (автономные автоматы), множество состояний которых есть пространство двоичных n -мерных векторов, и функция переходов реализует полноцикловую подстановку множества состояний. Оценивается сложность T_n решения системы уравнений гаммообразования (без ограничения на число уравнений) относительно неизвестного начального состояния методом формального кодирования. Оценка получена с помощью определения линейной сложности и порядка множества мономов для последовательности выходных функций генератора. Показано, что $TL(2^{n-1}) < T_n < TL(2^n)$, где $TL(m)$ — сложность решения над $GF(2)$ системы из m линейных уравнений от m неизвестных. Данный класс генераторов порождает, в частности, нормальные рекуррентные последовательности над полем $GF(2)$ (последовательности де Брёйна).

Ключевые слова: *моном, аннулирующий полином, линейная оболочка.*

1. Характеристики, определяющие сложность решения систем уравнений методом формального кодирования

Метод формального кодирования [1] применим для решения любой системы уравнений над конечным полем [2]. Вместе с тем трудоемкость метода меньше трудоемкости метода полного перебора только для частных классов систем уравнений. Определим характеристики системы уравнений, важные для оценки сложности ее решения методом формального кодирования.

Обозначим: M_n — множество всех мономов, зависящих от переменных $x_1, \dots, x_n$; $M_{n,d}$ — его подмножество всех мономов степени d , $0 \leq d \leq n$. Отсюда $M_n = \bigcup_{d=0}^n M_{n,d}$, где $M_{n,0} = \{1\}$ и при $d \geq 1$

$$M_{n,d} = \{x_{j_1} \dots x_{j_d} : \{j_1, \dots, j_d\} \subseteq \{1, \dots, n\}, j_1 < \dots < j_d\}.$$

Определим на M_n частичный порядок: $x_{j_1} \dots x_{j_d} \leq x_{s_1} \dots x_{s_\ell} \Leftrightarrow \{j_1, \dots, j_d\} \subseteq \{s_1, \dots, s_\ell\}$. Заметим, что M_n — решётка, изоморфная решётке V_n булевых векторов длины n , где вектору $\delta = (\delta_1, \dots, \delta_n)$ из V_n биективно соответствует моном $x^\delta = x_1^{\delta_1} \dots x_n^{\delta_n}$ из M_n , при этом для $j = 1, \dots, n$

$$x_j^{\delta_j} = \begin{cases} x_j, & \delta_j = 1, \\ 1, & \delta_j = 0. \end{cases}$$

Единицей и нулём решётки V_n являются соответственно векторы $e_n = (1, \dots, 1)$ и $u_n = (0, \dots, 0)$, единицей и нулём решётки M_n — мономы $x^{e_n} = x_1 \dots x_n$ и $x^{u_n} = 1$.

¹Результаты работы докладывались на Международной конференции с элементами научной школы для молодёжи, г. Омск, 7–12 сентября 2009 г.

3. Размерность линейной оболочки системы выходных функций

Пусть r — натуральное число, $W = \{w_i\}$ — чисто периодическая последовательность над V_r с длиной периода $2\tau = 2^t$, где $\tau > 1$, $m_W(\lambda)$ — минимальный многочлен (над $\text{GF}(2)$) последовательности W . Длину периода периодической последовательности W обозначим $\text{per } W$.

Последовательность W назовём *компенсированной*, если $w_1 \oplus \dots \oplus w_{2\tau} = u_r$, где u_r — нуль пространства V_r .

Теорема 1.

а) $m_W(\lambda) = (\lambda \oplus 1)^s$, где $\tau + 1 \leq s \leq 2\tau - \varepsilon(W)$ и

$$\varepsilon(W) = \begin{cases} 0, & \text{если } W \text{ не компенсированная,} \\ 1, & \text{если } W \text{ компенсированная;} \end{cases}$$

при этом $s = \tau + 1$, если $w_i \oplus w_{i+\tau} = \alpha$ при некотором $\alpha \neq u_r$ и при всех $i = 1, \dots, \tau$.

б) Если многочлен $\psi(\lambda) = p_0 \oplus p_1\lambda \oplus \dots \oplus p_k\lambda^k$ аннулирует последовательность W и $k < 2\tau$, то вес $wp(\psi(\lambda))$ чётен и выполнены равенства: $p_j = p_{j+\tau}$, $j = 0, 1, \dots, k - \tau$; $p_j = 0$, $j = k - \tau + 1, \dots, \tau - 1$.

Доказательство.

а) По условию длина периода последовательности W равна 2τ ; следовательно, W аннулируется многочленом $\lambda^{2\tau} \oplus 1$, каноническое разложение которого на неприводимые множители есть $(\lambda \oplus 1)^{2\tau}$. Так как $m_W(\lambda)$ делит $(\lambda \oplus 1)^{2\tau}$, то $m_W(\lambda) = (\lambda \oplus 1)^s$, где $s \leq 2\tau$. Вместе с тем $s > \tau$, так как иначе последовательность W аннулируется многочленом $(\lambda \oplus 1)^\tau$, где $(\lambda \oplus 1)^\tau = \lambda^\tau \oplus 1$. Последнее означало бы, что длина периода последовательности W не больше τ , что противоречит условию.

Для компенсированной последовательности W верхнюю оценку линейной сложности можно уточнить: W аннулируется многочленом $1 \oplus \lambda \oplus \dots \oplus \lambda^{2\tau-1}$, каноническое разложение которого на неприводимые множители есть $(\lambda \oplus 1)^{2\tau-1}$. Следовательно, в этом случае $m_W(\lambda) = (\lambda \oplus 1)^s$, где $s \leq 2\tau - 1$.

При условии $w_i \oplus w_{i+\tau} = \alpha$ нижняя оценка для s достигается, так как при всех $i = 1, \dots, 2\tau$ выполняется

$$w_{i+\tau+1} \oplus w_{i+\tau} \oplus w_{i+1} \oplus w_i = (w_{i+\tau+1} \oplus w_{i+1}) \oplus (w_{i+\tau} \oplus w_i) = \alpha \oplus \alpha = u_r.$$

Отсюда многочлен $\lambda^{\tau+1} \oplus \lambda^\tau \oplus \lambda \oplus 1$, разложение которого на неприводимые множители есть $(\lambda \oplus 1)^{\tau+1}$, аннулирует последовательность W и является минимальным многочленом для W в соответствии с доказанной нижней оценкой для s .

б) Из утверждения а) теоремы следует: $m_W(\lambda) = (\lambda^\tau \oplus 1)(\lambda \oplus 1)^{s-\tau}$, где $\tau + 1 \leq s < 2\tau$. Любой многочлен $\psi(\lambda)$, аннулирующий последовательность W , кратен многочлену $m_W(\lambda)$, то есть $\psi(\lambda) = m_W(\lambda)\varphi(\lambda)$ при некотором ненулевом многочлене $\varphi(\lambda)$. Поэтому если $\deg \psi(\lambda) = k \leq 2\tau - 1$, то

$$\psi(\lambda) = (\lambda^\tau \oplus 1)q(\lambda), \quad (2)$$

где $\deg q(\lambda) = k - \tau$ и $q(\lambda) = (\lambda \oplus 1)^{s-\tau}\varphi(\lambda)$. Если $q(\lambda) = q_0 \oplus q_1\lambda \oplus \dots \oplus q_{k-\tau}\lambda^{k-\tau}$, то из (2) следует, что $p_j = p_{j+\tau} = q_j$, $j = 0, 1, \dots, k - \tau$; $p_j = 0$, $j = k - \tau + 1, \dots, \tau - 1$.

Из (2) следует также, что $wp(\psi(\lambda)) = 2wp(q(\lambda))$, поэтому $wp(\psi(\lambda))$ чётен. ■

Следствие. Для последовательности выходных функций автомата A выполнено

$$2\tau \geq \dim \langle F_{2\tau, n} \rangle \geq \tau + 1.$$

Доказательство. Последовательность $\{f_i(x_1, \dots, x_n)\}$ выходных функций автомата чисто периодическая, поэтому ее линейная оболочка совпадает с $\langle F_{2\tau, n} \rangle$ — с линейной оболочкой ее периода. По теореме 7.1 [3] $\dim \langle F_{2\tau, n} \rangle = \deg m_f(\lambda)$, где $m_f(\lambda)$ — минимальный многочлен последовательности $\{f_i(x_1, \dots, x_n)\}$. В соответствии с утверждением а теоремы $2\tau \geq \deg m_f(\lambda) \geq \tau + 1$. Следовательно, $2\tau \geq \dim \langle F_{2\tau, n} \rangle \geq \tau + 1$. ■

4. Свойства системы полиномов выходных функций автомата

Для автомата A обозначим чисто периодические последовательности: $W(h) = \{h^i(u_n)\}$ — последовательность состояний при начальном состоянии u_n ; $f(W(h)) = \{f(h^i(u_n))\}$ — соответствующая ей выходная последовательность; $H = \{h^i\}$ — последовательность степеней подстановки h ; $f(H) = \{f(h^i)\}$ — соответствующая ей последовательность выходных функций, $i = 0, 1, 2, \dots$. Заметим, что период последовательности H совпадает с циклической группой подстановок $\langle h \rangle$ порядка 2^n .

Отметим свойства этих последовательностей:

- 1) $\text{per } W(h) = \text{per } H = 2^n$;
- 2) $\text{per } f(W(h)) = \text{per } f(H) = 2\tau$, где $1 < \tau \leq 2^{n-1}$;
- 3) $m_{W(h)}(\lambda) = m_H(\lambda)$;
- 4) $m_{f(W(h))}(\lambda) = m_{f(H)}(\lambda)$;
- 5) $M(f(H)) = M(F_{2\tau, n})$.

Обозначим: $M_d(f(H)) = M_{n,d} \cap M(f(H))$ — множество всех мономов степени d , содержащихся в совокупности полиномов выходных функций из последовательности $f(H)$, $0 \leq d \leq n$. Отсюда

$$M(f(H)) = \bigcup_{d=1}^n M_d(f(H)).$$

На периоде последовательности $W(h)$ определим порядковый номер вектора $\gamma \in V_n$ (обозначим его $n(\gamma)$): $n(u_n) = 0$, $n(\gamma)$ — наименьшее натуральное число t , такое, что $h^t(u_n) = \gamma$.

Для монома x^δ степени $d > 0$, где $\delta \in V_n$, определим многочлен $\psi_\delta(\lambda)$ над $\text{GF}(2)$, зависящий от функций h и f автомата A :

$$\psi_\delta(\lambda) = \bigoplus_{\gamma \leq \delta} \lambda^{\nu(\gamma)}, \quad (3)$$

где $\nu(\gamma)$ — наименьший неотрицательный вычет числа $n(\gamma)$ по $\text{mod}(2\tau)$; символом $\leq$ обозначено стандартное отношение частичного порядка на решётке V_n . Многочлен $\psi_\delta(\lambda)$ назовем A -многочленом монома x^δ .

Отметим некоторые свойства A -многочленов мономов:

- 1) $\deg \psi_\delta(\lambda) < 2\tau$;
- 2) $wp(\psi_\delta(\lambda)) \leq 2^d$ и является чётным;
- 3) $wp(\psi_\delta(\lambda)) = 2^d \Leftrightarrow$ в последовательности $W(h)$ номера любых двух не превосходящих δ векторов не сравнимы по $\text{mod}(2\tau)$;
- 4) $wp(\psi_\delta(\lambda)) = 0 \Leftrightarrow$ множество $\{n(\gamma) : \gamma \leq \delta\}$ есть совокупность 2^{d-1} пар чисел, где числа в каждой паре сравнимы по модулю 2τ .

Обозначим: $g = h^\tau$. Заметим, что подстановка g состоит из τ циклов длины $2^n/\tau$.

Лемма 1.

а) Моном x^δ степени $d > 0$ не содержится в $M(f(H)) \Leftrightarrow A$ -многочлен монома x^δ либо нулевой, либо аннулирующий для последовательности $f(H)$.

б) Если $\psi_\delta(\lambda)$ аннулирует последовательность $f(H)$ и $\gamma \leq \delta$ для $\gamma, \delta \in V_n$, то и $g(\gamma) \leq \delta$.

Доказательство.

а) В полиноме Жегалкина булевой функции φ коэффициент $a_\delta(\varphi)$ при мономе x^δ равен булевой сумме 2^d элементов её табличного задания [3], формула (3.16):

$$a_\delta(\varphi) = \bigoplus_{\gamma \leq \delta} \varphi(\gamma).$$

Преобразуем это равенство, используя порядковые номера векторов:

$$a_\delta(\varphi) = \bigoplus_{\gamma \leq \delta} \varphi(h^{n(\gamma)}(u_n)).$$

Отсюда имеем, в частности, равенства для коэффициентов выходных функций f_i , $i = 0, 1, 2, \dots$:

$$a_\delta(f_i) = \bigoplus_{\gamma \leq \delta} f(h^i(h^{n(\gamma)}(u_n))) = \bigoplus_{\gamma \leq \delta} f(h^{i+n(\gamma)}(u_n)).$$

Так как $\text{per } f(W(h)) = 2\tau$, то $f(h^{i+n(\gamma)}) = f(h^{i+\nu(\gamma)})$, $i = 0, 1, 2, \dots$, следовательно,

$$a_\delta(f_i) = \bigoplus_{\gamma \leq \delta} f(h^{i+\nu(\gamma)}(u_n)). \quad (4)$$

По определению $x^\delta \notin M(f(H)) \Leftrightarrow a_\delta(f_i) = 0$, $i = 0, 1, 2, \dots$. Отсюда в соответствии с (3) следует, что $x^\delta \notin Mf(H) \Leftrightarrow A$ -многочлен монома x^δ либо является нулевым, либо аннулирует последовательность $f(H)$ (а также и $f(W(h))$), так как $m_{f(W(h))}(\lambda) = m_{f(H)}(\lambda)$.

б) В соответствии с определением подстановки g номера $n(\gamma)$ и $n(g(\gamma))$ сравнимы по модулю τ и не сравнимы по модулю 2τ , поэтому $\nu(\gamma)$ и $\nu(g(\gamma))$ также сравнимы по модулю τ . Отсюда если многочлен $\psi_\delta(\lambda)$ аннулирует последовательность $f(H)$ (а также $f(W(h))$), где $\deg \psi_\delta(\lambda) < 2\tau$, то из утверждения б) теоремы 1 и равенства (3) вытекает, что если $\lambda^{\nu(\gamma)}$ — моном многочлена $\psi_\delta(\lambda)$, то и $\lambda^{\nu(g(\gamma))}$ также моном многочлена $\psi_\delta(\lambda)$. По построению многочлена $\psi_\delta(\lambda)$ это равносильно тому, что если $\gamma \leq \delta$, то и $g(\gamma) \leq \delta$. ■

Для монома x^δ обозначим

$$U_n(x^\delta) = \{\xi \in M_n : x^\delta \leq \xi\}; \quad \bar{U}_n(x^\delta) = M_n \setminus U_n(x^\delta).$$

При любом δ из V_n множество $\bar{U}_n(x^\delta)$ не содержит монома x^{e_n} и множество $U_n(x^\delta)$ не пусто и образует в M_n подрешётку, изоморфную решётке $M_{n-\|\delta\|}$, где $\|\delta\|$ — вес двоичного вектора δ .

Обозначим также: $M_n(\gamma, \beta) = (U_n(x^\gamma) \cap \bar{U}_n(x^\beta)) \cup (U_n(x^\beta) \cap \bar{U}_n(x^\gamma))$, где $\gamma, \beta \in V_n$.

Теорема 2.

а) Множество $M(f(H))$ содержит $M(f(x_1, \dots, x_n))$ и все мономы степени $d > 0$ из $\bigcup_{\gamma \in V_n} M_n(\gamma, g(\gamma))$ с ненулевым A -многочленом.

б) Моном $x^{e_n} \in M(f_i(x_1, \dots, x_n))$, $i = 1, 2, \dots \Leftrightarrow x^{e_n} \in M(f(H)) \Leftrightarrow \|f\|$ нечетен.

Доказательство.

а) Последовательность H содержит тождественную подстановку, поэтому последовательность $f(H)$ содержит функцию $f(x_1, \dots, x_n)$. Следовательно, $M(f(x_1, \dots, x_n)) \subseteq M(f(H))$.

При любом $\gamma \in V_n$ для векторов γ и $g(\gamma)$ не выполнены одновременно отношения $\gamma \leq g(\gamma)$ и $g(\gamma) \leq \gamma$, так как $\gamma \neq g(\gamma)$ в соответствии с определением подстановки g . Пусть, например, не выполнено отношение $g(\gamma) \leq \gamma$, тогда из определения множества $M_n(\gamma, g(\gamma))$ следует, что множество $U_n(x^\gamma) \cap \bar{U}_n(x^{g(\gamma)})$ содержит моном x^γ и, следовательно, не пусто. Если $x^\delta \in U_n(x^\gamma) \cap \bar{U}_n(x^{g(\gamma)})$ при некоторых $\delta, \gamma \in V_n$, то $x^\delta \in U_n(x^\gamma)$ и $x^\delta \in \bar{U}_n(x^{g(\gamma)})$. Отсюда следует, что $\gamma \leq \delta$ в силу определения множества $U_n(x^\gamma)$ и отношение $g(\gamma) \leq \delta$ не выполнено в силу определения множества $\bar{U}_n(x^{g(\gamma)})$.

Если для монома x^δ степени $d > 0$ A -многочлен $\psi_\delta(\lambda)$ ненулевой и $x^\delta \notin M(f(H))$, то по утверждению *a* леммы 1 $\psi_\delta(\lambda)$ аннулирует последовательность $f(H)$ и по утверждению *б* леммы 1 если $\gamma \leq \delta$, то и $g(\gamma) \leq \delta$, что противоречит условию. Значит, если $\psi_\delta(\lambda)$ — ненулевой многочлен, то $x^\delta \in M(f(H))$.

Включение $x^\delta \in M(f(H))$ для монома x^δ из $U_n(x^{g(\gamma)}) \cap \bar{U}_n(x^\gamma)$ (если не выполнено отношение $\gamma \leq g(\gamma)$) доказывается аналогично. Заметим, что рассуждения верны для произвольного вектора γ .

б) В полиноме булевой функции коэффициент при мономе x^{e_n} равен $1 \Leftrightarrow$ вес функции нечетен (теорема 3.11 [3]). Осталось заметить, что веса всех выходных функций автомата равны $\|f\|$ в силу эквивалентности этих функций относительно группы подстановок $\langle h \rangle$. ■

Замечание. Если векторы γ и $g(\gamma)$ сравнимы, например $\gamma \leq g(\gamma)$, то $U_n(x^{g(\gamma)}) \cap \bar{U}_n(x^\gamma) = \emptyset$ и $M_n(\gamma, g(\gamma)) = U_n(x^\gamma) \cap \bar{U}_n(x^{g(\gamma)})$.

Следствие 1. Если $g(u_n) = \beta$, то $M(f(H))$ содержит все мономы из $\bar{U}_n(x^\beta)$ с ненулевым A -многочленом; если при этом $\|\beta\| = r$ и каждый моном из $\bar{U}_n(x^\beta)$ имеет ненулевой A -многочлен, то

$$|M_d(f(H))| \geq \begin{cases} C_n^d, & 1 \leq d < r, \\ C_n^d - C_{n-r}^{d-r}, & r \leq d < n. \end{cases} \quad (5)$$

Доказательство. Так как $u_n \leq \beta$, то $M_n(u_n, \beta) = U_n(x^{u_n}) \cap \bar{U}_n(x^\beta)$ в силу замечания к теореме 2. При этом $U_n(x^{u_n}) = M_n$, значит, $M_n(u_n, \beta) = \bar{U}_n(x^\beta)$, и по утверждению *a* теоремы 2 если моном x^δ из $\bar{U}_n(x^\beta)$ имеет ненулевой A -многочлен, то $x^\delta \in M(f(H))$.

По определению $\bar{U}_n(x^\beta) = M_n \setminus U_n(x^\beta)$. Поэтому если все мономы из $\bar{U}_n(x^\beta)$ имеют ненулевые A -многочлены, то по утверждению *a* теоремы 2 $|M_d(f(H))|$ оценивается снизу числом мономов степени d , которые не больше монома x^β степени r . К таким мономам относятся все мономы степени d , если $d < r$, и если $d \geq r$, — все мономы степени d за исключением тех, которые превосходят фиксированный моном x^β степени r . ■

Следствие 2. Если $g(e_n) = \alpha$, то $M(f(H))$ содержит все мономы из $U_n(x^\alpha) \setminus \{x^{e_n}\}$ с ненулевым A -многочленом; если при этом $\|\alpha\| = r$ и каждый моном из $U_n(x^\alpha) \setminus \{x^{e_n}\}$ имеет ненулевой A -многочлен, то

$$|M_d(f(H))| \geq \begin{cases} 0, & 1 \leq d < r, \\ C_{n-r}^{d-r}, & r \leq d < n. \end{cases} \quad (6)$$

Доказательство. Так как $\alpha \leq e_n$, то $M_n(\alpha, e_n) = U_n(x^\alpha) \cap \bar{U}_n(x^{e_n})$ в силу замечания к теореме 2. При этом $\bar{U}_n(x^{e_n}) = M_n \setminus \{x^{e_n}\}$, значит, $M_n(\alpha, e_n) = U_n(x^\alpha) \setminus \{x^{e_n}\}$, и по утверждению *a* теоремы 2 если моном x^δ из $U_n(x^\alpha) \setminus \{x^{e_n}\}$ имеет ненулевой A -многочлен, то $x^\delta \in M(f(H))$.

Если все мономы x^δ из $U_n(x^\alpha) \setminus \{x^{e_n}\}$ имеют ненулевые A -многочлены, то по утверждению a теоремы 2 $|M_d(f(H))|$ оценивается снизу числом мономов степени d , которые не меньше монома x^α степени r , где $d \geq r$. ■

Из следствий 1 и 2 теоремы 2 получаем оценку множества $M(f(H))$. Обозначим для $\alpha, \beta \in V_n$:

$$M_n(\beta/u, \alpha/e) = \overline{U}_n(x^\beta) \cup U_n(x^\alpha) \setminus \{x^{e_n}\}.$$

Заметим, $M_n(\beta/u, \alpha/e) = M_n \setminus \{x^{e_n}\}$ при $\alpha \leq \beta$.

Следствие 3. Если $g(u_n) = \beta$, $g(e_n) = \alpha$, то $M(f(H))$ содержит все мономы из $M_n(\beta/u, \alpha/e)$ с ненулевым A -многочленом.

Теорема 3. Если $\text{per } f(H) = 2^n$, то:

а) $|M(f(H))| \geq 2^{n-1}$;

б) при случайном равновероятном выборе h из класса всех полноцикловых подстановок

$$E|M(f(H))| \geq 2^n - (1,5)^n + (1,25)^n,$$

где $E\zeta$ — математическое ожидание случайной величины ζ .

Доказательство.

а) Для любой полноцикловой подстановки h подстановка g не содержит единичных циклов, поэтому $\|g(u_n)\| \geq 1$. Пусть $g(u_n) = \beta = (\beta_1, \dots, \beta_n)$ и для определённости $\beta_1 = 1$.

Если $\text{per } f(H) = 2^n$, то любой моном степени $d > 0$ имеет ненулевой A -многочлен, и при указанном векторе β множество $\overline{U}_n(x^\beta)$ содержит все мономы, не зависящие от x_1 . Следовательно, $|M_n(\alpha/e, \beta/u)| \geq |\overline{U}_n(x^\beta)| \geq 2^{n-1}$. Отсюда $|M(f(H))| \geq 2^{n-1}$ в соответствии со следствием 3 теоремы 2.

б) При случайном равновероятном выборе h из класса всех полноцикловых подстановок множества V_n пара векторов (α, β) , где $\alpha = g(e_n)$, $\beta = g(u_n)$, есть равновероятная неповторная выборка из множества $(V_n \setminus \{u_n, e_n\})$. Число таких выборок равно $(2^n - 2)(2^n - 3)$.

Пусть для векторов α, β решётки V_n выполнено: $\|\alpha\| = r$, $\|\beta\| = p$, $\|\inf(\alpha, \beta)\| = k$, тогда $\|\sup(\alpha, \beta)\| = r + p - k$. Число пар таких векторов из V_n , обозначаемое $N(r, p, k)$, равно

$$N(r, p, k) = C_n^r \cdot C_r^k \cdot C_{n-r}^{p-k}.$$

Для такой пары векторов α, β выполнено

$$|\overline{U}_n(x^\beta)| = 2^n - 2^{n-p},$$

$$|(U_n(x^\alpha) \setminus \{x^{e_n}\}) \setminus \overline{U}_n(x^\beta)| = |U_n(x^{\sup(\alpha, \beta)}) \setminus \{x^{e_n}\}| = 2^{n-r-p+k} - 1,$$

$$|M_n(\alpha/e, \beta/u)| = |\overline{U}_n(x^\beta)| + |(U_n(x^\alpha) \setminus \{x^{e_n}\}) \setminus \overline{U}_n(x^\beta)| = 2^n - 2^{n-p} + 2^{n-r-p+k} - 1.$$

Следовательно, при случайном равновероятном выборе h из класса всех полноцикловых подстановок множества V_n среднее значение $|M_n(\alpha/e, \beta/u)|$ определяется формулой (используем принцип включения-исключения с учетом, что α, β, e_n, u_n суть различные векторы из V_n)

$$E |M_n(\alpha/e, \beta/u)| = \frac{1}{(2^n - 2)(2^n - 3)} \left[\sum_{r=0}^n \sum_{k=0}^r \sum_{p=k=0}^{n-r} N(r, p, k) (2^n - 2^{n-p} + 2^{n-r-p+k} - 1) - \right.$$

$$\begin{aligned}
& - \sum_{p=0}^n N(0, p, 0)(2^n - 1) - \sum_{p=0}^n N(n, p, p)(2^n - 2^{n-p}) - \sum_{r=0}^n N(r, 0, 0)(2^{n-r} - 1) - \\
& - \sum_{r=0}^n N(r, n, r)(2^n - 1) + (N(0, 0, 0) + N(0, n, 0) + N(n, 0, 0) + N(n, n, n))(2^n - 1) \Big].
\end{aligned}$$

Подсчёт сумм с использованием формулы бинома Ньютона даёт следующий результат:

$$E |M_n(\alpha/e, \beta/u)| = \frac{8^n - 6^n + 5^n - 4^{n+1} + 6 \cdot 2^n - 3}{(2^n - 2)(2^n - 3)}.$$

Отсюда получаем требуемую оценку. ■

Пример. Пусть функция переходов h автомата A реализуется линейным конгруэнтным генератором: $h(x) = (x + 1) \bmod 2^n$. Для подстановки h множества V_n выполнено:

1) $\text{per } W_j(h) = \text{per } W_j(H) = 2^j$, $j = 1, \dots, n$;

2) пусть $\text{per } f(H) = 2^n$, тогда $\tau = 2^{n-1}$, $h(x) \oplus h^\tau(x) = (0, \dots, 0, 1)$ при любом $x \in V_n$.

Последовательность $f(H)$ имеет алгебраические характеристики:

1) $m_H(\lambda) = (\lambda \oplus 1)^{\tau+1}$ — по утверждению a теоремы 1;

2) $M(H)$ содержит множество всех мономов от $x_1, \dots, x_{n-1}$ — по утверждению a теоремы 2;

3) $\deg W_n(H) = n - 1$.

Выводы

1. Последовательность выходных функций генератора гаммы, построенного на основе полноциклового подстановки множества состояний V_n , имеет высокую линейную сложность Λ , а именно $2^{n-1} + 1 \leq \Lambda \leq 2^n$.

2. Для порядка множества мономов на периоде последовательности выходных функций генератора верны оценки: $2^{n-1} \leq |M(f(H))| \leq 2^n - 1$. При $n \rightarrow \infty$ и при случайном равновероятном выборе функции переходов h из класса всех полноцикловых подстановок множества V_n математическое ожидание величины $|M(f(H))| / (2^n - 1)$ стремится к 1.

3. Сложность T_n определения начального состояния генератора методом формального кодирования по известному периоду гаммы удовлетворяет оценкам

$$TL(2^{n-1}) < T_n < TL(2^n),$$

где $TL(m)$ — сложность решения над $\text{GF}(2)$ системы из m линейных уравнений от m неизвестных.

ЛИТЕРАТУРА

1. *Schaumuller-Bichl*. Cryptanalysis of the Data Encryption Standard by a method of formal coding // Cryptography, Proc. Burg Feuerstein 1982. LNCS. 1983. V. 149. P. 235–255.
2. *Courtois N., Klimov A., Patarin J., Shamir A.* Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations // LNCS. 2000. V. 1807. P. 392–407.
3. *Фомичёв В. М.* Дискретная математика и криптология. М.: ДИАЛОГ–МИФИ, 2003. 400 с.