

Рассчитаны мощности слоев J_N^k для $N \leq 20$. В приводимой ниже таблице указано количество классов сопряженных элементов, содержащихся в слое J_N^k для $k = 2, 3, 4, 5$.

N	2	3	4	5
2	1			
4	2			
6	3	4	6	5
8	5	8	12	
10	7	16	22	20
12	11	36	40	
14	15	62	69	66
16	22	113	118	
18	30	186	195	190
20	42	313	317	

ЛИТЕРАТУРА

1. *Brenner J. L.* Covering theorems for FINANSIGS VIII — Almost all conjugacy classes in A_n have exponent ≤ 4 // *J. Austral. Math. Soc.* 1978. V. 25. P. 210–214.
2. Products of conjugacy classes in groups / eds. Z. Arad, M. Herzog // *Lecture Notes in Math.* Berlin: Springer Verlag, 1985. V. 1112. P. 198–221.
3. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Т. II. М.: Гелиос АРВ, 2003.
4. *Тужилин М. Э.* О порождении знакопеременной группы полурегулярными инволюциями // *Обзорные прикладной и промышленной математики.* 2004. Т. 11. Вып. 4. С. 938–939.

УДК 519.1

СВОЙСТВА ВНЕШНИХ УПРАВЛЯЮЩИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В. М. Фомичев

Свойства выходной гаммы и преобразований состояний генератора с внешним управлением неравномерным движением существенным образом определяются свойствами управляющей гаммы. Например, в генераторах « δ - τ -шагов» и в генераторах с перемежающимся шагом, построенных на основе линейных регистров сдвига (ЛРС) с максимальными длинами периодов, порядок линейной подгруппы циклической группы преобразований состояний генератора определяется длиной периода t управляющей гаммы [1, разд. 18.4.2, 2]: линейные уравнения гаммообразования соответствуют всем тактам работы генератора, номера которых кратны t .

Показано, что в генераторах с внешним управлением доля линейных уравнений гаммообразования тем больше, чем меньше h -период управляющей последовательности, где h — функция, отображающая отрезки управляющей последовательности в подходящее множество. Свойства h -периодов последовательностей над $\mathbb{N}_0$ для конкретной функции h суммирования членов последовательности, полученные в [3], в работе обобщены.

Для аддитивных функций h доказано, что длина h -периода периодической последовательности делит длину периода, для некоторых h исследованы длины h -периодов последовательностей де Брёйна и линейных рекуррентных последовательностей над конечными полями.

Для широкого класса генераторов гаммы с внешним управлением неравномерным движением показано, что доля линейных уравнений относительно знаков промежуточного состояния среди уравнений гаммообразования, соответствующих знакам периода гаммы, равна $1/\tau$, где τ — длина h -периода управляющей гаммы и h — аддитивная функция маркировки слов.

Пусть $\mathbb{N}$ — множество натуральных чисел; $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; $X_{\rightarrow} = \{x_0, x_1, \dots\}$ — последовательность над множеством X ; $X^* = \bigcup_{s \geq 1} X^s$ — множество всех слов натуральной длины в алфавите X ; (t, τ) — наибольший общий делитель чисел $t, \tau \in \mathbb{N}$.

Множество X^* образует полугруппу относительно операции конкатенации. Результат конкатенации слова u длины ℓ и слова u' длины ℓ' есть слово uu' длины $\ell + \ell'$. Слово $x_\nu, x_{\nu+1}, \dots, x_{\nu+s-1}$ длины s в алфавите X (обозначим его $x_{(\nu,s)}$) называют s -граммой последовательности $X_{\rightarrow}$, где $t \in \mathbb{N}$, $\nu \in \mathbb{N}_0$.

Обозначим $t = t(X_{\rightarrow})$ и $\nu = \nu(X_{\rightarrow})$ — длины периода и предпериода последовательности $X_{\rightarrow}$. Период последовательности $X_{\rightarrow}$ есть слово $x_{\nu+i}, x_{\nu+i+1}, \dots, x_{\nu+i+t-1}$ при любом $i \geq 0$, а предпериод — слово $x_0, x_1, \dots, x_{\nu-1}$ при $\nu \geq 0$. Если $\nu(X_{\rightarrow}) = 0$, то $X_{\rightarrow}$ предпериода не имеет и называется чисто периодической последовательностью.

Рассмотрим функцию $h : X^* \rightarrow Y$, где Y — некоторое множество. Функцию h можно рассматривать как обобщение хеш-функции. Через h^s обозначим ограничение функции h на множество X^s , то есть $h^s : X^s \rightarrow Y$, $s \geq 1$.

При натуральном s и при $\mu \in \mathbb{N}_0$ последовательности $X_{\rightarrow}$ поставим в соответствие последовательность $X_{\rightarrow}^{\mu,s}$ её s -грамм: $X_{\rightarrow}^{\mu,s} = \{(x_{(\mu+ks,s)}), k = 0, 1, \dots\}$, которой также соответствует последовательность $h(X_{\rightarrow}^{\mu,s})$ над Y : $h(X_{\rightarrow}^{\mu,s}) = \{h^s(x_{(\mu+ks,s)}), k = 0, 1, \dots\}$.

Последовательность $X_{\rightarrow}$ назовем h -периодической, если при некоторых $s \in \mathbb{N}$ и $\mu \in \mathbb{N}_0$

$$h(x_{(\mu+ks,s)}) = h(x_{(\mu+(k+1)s,s)}), \quad k = 0, 1, \dots; \quad (1)$$

равенство (1) будем интерпретировать так: в $X_{\rightarrow}$ имеются h^s -совпадения с начальным номером μ . Наименьшее из таких s назовем длиной h -периода последовательности $X_{\rightarrow}$ (обозначается $t_h(X_{\rightarrow})$, кратко t_h), и если t_h — длина h -периода, то наименьший из начальных номеров совпадения μ назовем длиной h -предпериода последовательности $X_{\rightarrow}$ (обозначается $\nu_h(X_{\rightarrow})$, кратко ν_h). Если (1) выполняется при $\mu = 0$, то последовательность $X_{\rightarrow}$ назовем чисто h -периодической. Для последовательности $X_{\rightarrow}$ назовем h -периодом слово $x_{(\mu+ks,s)}$ и h -предпериодом — слово $x_0, x_1, \dots, x_{\mu-1}$, где $s = t_h$ и $\mu = \nu_h, k = 0, 1, \dots$.

Заметим, если в периодической последовательности имеются h^s -совпадения с начальным номером μ , то не обязательно t_h делит s и ν_h равно μ . Это подтверждается примером чисто периодической последовательности $X_{\rightarrow}$ над $\mathbb{N}_0$ при $h^s(x_i, x_{i+1}, \dots, x_{i+s-1}) = x_i + x_{i+1} + \dots + x_{i+s-1}$, где $s > 0$, $i \in \mathbb{N}_0$, $a \in \mathbb{N}$:

$$X_{\rightarrow} = \{a, 2a, 0, 0, 2a, a, a, 2a, 0, 0, 2a, a, a, 2a, 0, \dots\}. \quad (2)$$

Длина периода последовательности $X_{\rightarrow}$ равна 6, в $X_{\rightarrow}$ имеются h^3 -совпадения с начальным номером 0 и h^2 -совпадения с начальным номером 1, но нет h^1 -совпадений. Следовательно, $t_h(X_{\rightarrow}) = 2$, $\nu_h(X_{\rightarrow}) = 1$.

Отметим элементарные свойства h -периодических последовательностей.

- 1) Периодическая последовательность $X_{\rightarrow}$ с длиной предпериода ν и длиной периода t является h -периодической для любой функции $h : X^* \rightarrow Y$, при этом $t_h \leq t, \nu_h \leq \nu$ (в $X_{\rightarrow}$ имеются h^t -совпадения с начальным номером ν).

- 2) Подпоследовательность $\{x_i, x_{i+1}, \dots\}$ h -периодической последовательности $X_{\rightarrow}$ с длиной h -периода t_h и длиной h -предпериода ν_h является чисто h -периодической, если и только если $(i - \nu_h)$ кратно t_h .
- 3) Не всякая h -периодическая последовательность является периодической, что показывается примером последовательности хаотически чередующихся s -грамм u и w в алфавите X , где $h^s(u) = h^s(w)$:

$$X_{\rightarrow} = \{u, w, w, u, u, w, u, w, w, u, u, w, u, w, u, w, w, u, \dots\}.$$

В чисто h -периодической последовательности $X_{\rightarrow}$ имеются h^s -совпадения, значит, $X_{\rightarrow}$ имеет длину h -периода не более s , но не является периодической, так как построена как аperiodическая последовательность s -грамм u и w .

Пусть Y — аддитивная полугруппа. Функцию $h : X^* \rightarrow Y$ назовем аддитивной, если для любого слова w длины $s > 1$ из того, что $w = uu'$, где $u \in X^\ell$, $u' \in X^r$, $\ell + r = s$, следует, что

$$h^s(w) = h^\ell(u) + h^r(u').$$

Пример 1 (аддитивные функции).

- 1) Длина слова u , то есть функция $L : X^* \rightarrow \mathbb{N}$, определенная для $u = x_1x_2 \dots x_\ell \in X^\ell$ формулой $L(u) = \ell$.
- 2) Частота символа a в слове u , где $a \in X$; обозначим эту функцию $m_a(u)$.
- 3) Пусть $X = \{a_1, a_2, \dots, a_k\}$, $m_i(u)$ — частота символа a_i в слове u , $i = 1, \dots, k$. Функцией маркировки слов назовем функцию $m : X^* \rightarrow \mathbb{N}_0^k$, определенную формулой $m(u) = (m_1(u), \dots, m_k(u))$.
- 4) Пусть $X = \mathbb{N}_0$ или $X = \text{GF}(k)$, где k — простое, и $u = x_1x_2 \dots x_\ell \in X^\ell$. Функцией веса слов из X^* назовем функцию $\text{wt} : X^* \rightarrow \mathbb{N}_0$, определенную формулой $\text{wt}(u) = \text{wt}(x_1) + \dots + \text{wt}(x_\ell)$, где $\text{wt}(x_i) = x_i$ для любого $x_i \in X$.

Теорема 1. Пусть $X_{\rightarrow} = \{x_0, x_1, \dots\}$ — чисто периодическая последовательность с длиной периода t и длиной h -периода t_h , где h — аддитивная функция. Тогда t_h делит t .

Следствие 1. Пусть t — простое, тогда $t_h = 1$, если $h(x_0) = \dots = h(x_{t-1})$, и $t_h = t$ в остальных случаях.

Обозначим через ЛРПмах- n линейную рекуррентную последовательность порядка n над произвольным полем P порядка k с максимальной длиной периода, то есть $t = k^n - 1$.

Теорема 2. Для ЛРПмах- n в каждом из следующих случаев $t_h = k^n - 1$:

- а) $h = m_a(u)$, где a отлично от нуля поля P ;
- б) $h = m(u)$;
- в) $h = \text{wt}(u)$, где $P = \text{GF}(2)$ или $P = \text{GF}(3)$.

Если $P = \text{GF}(k)$, где $k > 3$ — простое, то $t_{\text{wt}} = (k^n - 1)/d$, где d делит $(k - 1)/2$.

Чисто периодическую рекуррентную последовательность порядка n над множеством X , где $|X| = k$, называют нормальной рекуррентной последовательностью, если длина ее периода равна k^n , и обозначают НРП(k, n). Генерируются НРП(k, n) полноцикловыми регистрами сдвига длины n над множеством X . НРП($2, n$) называют последовательностями де Брёйна. Обзор свойств НРП(k, n) дан в [4].

Теорема 3. В любой НРП(2, n) имеются h -совпадения на расстоянии 2^{n-1} при $n > 0$ и при всех функциях h из $\{m_0(u), m_1(u), m(u), \text{wt}(u)\}$.

Следствие 2. Длина h -периода последовательности де Брёйна порядка n равна 2^r , где $r < n$, при всех функциях $h \in \{m_0(u), m_1(u), m(u), \text{wt}(u)\}$.

При анализе линейности уравнений гаммообразования, связанных с генераторами гаммы с внешним управлением неравномерным движением, важным свойством является h -периодичность управляющей гаммы.

Рассмотрим класс генераторов, включающий генераторы « δ - τ -шагов» и генераторы с перемежающимся шагом. Пусть $X_{\rightarrow}$ — последовательность над простым полем $X = \text{GF}(k)$, управляющая движением информации в линейных регистрах сдвига ЛРС-0, ..., ЛРС- $(k-1)$ над полем P , которые реализуют линейные подстановки $g_0, \dots, g_{k-1}$ векторных пространств определенных размерностей. В i -м такте подстановка $g(i)$ пространства P^n состояний набора ЛРС-0, ..., ЛРС- $(k-1)$ определяется знаком x_i управляющей гаммы, схемой движения регистров, задаваемой матрицей $\Delta = (\delta(i, j))$ над $\mathbb{N}_0$ размера $k \times k$ (строки матрицы различны), и набором подстановок $g = (g_0, \dots, g_{k-1})$. Пусть в i -м такте состояние всех ЛРС генератора есть $y(i) = (y_0(i), \dots, y_{k-1}(i))$, где $y_j(i)$ — состояние ЛРС- j , $j = 0, \dots, k-1$, $i \geq 0$. Тогда

$$y_j(i+1) = g_j^{\delta(x_i, j)}(y_j(i)).$$

Знак γ_i выходной гаммы генератора есть сумма битов, записанных в i -м такте в крайних ячейках всех ЛРС (как в генераторе с перемежающимся шагом).

Пусть $m_j(i, \tau)$ — частота символа j в слове $x_{(i, \tau)}$ и $G(i, \tau) = g(i) \cdot g(i+1) \cdot \dots \cdot g(i+\tau-1)$. Тогда

$$G(i, \tau) = (g_0^{z_0(i, \tau)}, \dots, g_{k-1}^{z_{k-1}(i, \tau)}),$$

где $z_j(i, \tau) = m_0(i, \tau) \cdot \delta(0, j) + \dots + m_{k-1}(i, \tau) \cdot \delta(k-1, j)$ — суммарная продвижка ЛРС- j при управляющем слове $x_{(i, \tau)}$, $j = 0, \dots, k-1$. Заметим, что $G(i, \tau)$ и $G(\ell, \tau)$ суть одинаковые линейные подстановки пространства P^n , если одинаковы наборы величин $(z_0(i, \tau), \dots, z_{k-1}(i, \tau))$ и $(z_0(\ell, \tau), \dots, z_{k-1}(\ell, \tau))$. Отсюда если m — функция маркировки слов и $x_{(i, \tau)}$ есть m -период управляющей гаммы, то наборы величин $(z_0(i + r\tau, \tau), \dots, z_{k-1}(i + r\tau, \tau))$ одинаковы при любом $r = 0, 1, \dots$. Следовательно, если длина m -периода неизвестной чисто m -периодической управляющей последовательности равна τ , то линейные подстановки $G(i + r\tau, \tau)$ однозначно определены при некотором $i \in \{0, \dots, \tau-1\}$ и при $r = 0, 1, \dots$, поэтому знаки $\gamma_{i+r\tau}$ гаммы линейно выражаются через знаки состояния $y(i)$ генератора.

Выводы

- 1) Для криптографических приложений важным свойством является h -периодичность последовательностей при различных функциях h .
- 2) Наилучшие криптографические свойства ряда генераторов с неравномерным движением, связанные с нелинейностью уравнений гаммообразования, достигаются в схемах с управляющей гаммой, имеющей большие длины периода и m -периода, где m — функция маркировки слов.

ЛИТЕРАТУРА

1. Фомичев В. М. Методы дискретной математики в криптологии. М.: ДИАЛОГ-МИФИ, 2010. 424 с.

2. *Фомичев В. М., Фомичев Н. В.* Исследование линейных подсистем нелинейных систем уравнений гаммообразования // Системы высокой доступности. М.: Радиотехника, 2009. № 4. Т. 5. С. 28–33.
3. *Горьков И. Д.* Свойства σ -периодических последовательностей // Системы высокой доступности. М.: Радиотехника, 2009. № 4. Т. 5. С. 34–37.
4. *Агибалов Г. П.* Нормальные рекуррентные последовательности // Вестник Томского государственного университета. 2007. Приложение. № 23. С. 4–11.