УДК 519.1

СВОЙСТВА h-ПЕРИОДИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В. М. Фомичев

Институт проблем информатики РАН, г. Москва, Россия

E-mail: fomichev@nm.ru

Введено понятие h-периодичности последовательностей, связанное с отображением h мультиграмм последовательности в некоторое множество. Исследованы свойства h-периодических последовательностей, при аддитивных функциях h установлена связь длин периода и h-периода последовательности. При некоторых аддитивных функциях h исследована длина h-периода линейных рекуррентных последовательностей над конечным полем и последовательностей де Брёйна. Показано, что криптографические свойства ряда генераторов гаммы с неравномерным движением зависят от длины h-периода управляющей гаммы, где h — функция маркировки слов.

Ключевые слова: *период последовательности, аддитивная функция, линейная подстановка.*

Введение

Для генерации последовательностей (гаммы) в криптографических схемах часто используется последовательное соединение автономного автомата (управляющего блока), в котором информация продвигается равномерно в соответствии с заданной тактовой частотой, и неавтономного автомата (генерирующего блока), в котором продвижение информации зависит от знаков управляющей гаммы. Такие генераторы гаммы реализуют внешнее управление неравномерным движением информации.

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 управляющей гаммы [1, разд. 18.4.2, 2]: линейные уравнения гаммообразования соответствуют всем тактам работы генератора, номера которых кратны длине периода управляющей гаммы.

В некоторых генераторах линейные уравнения гаммообразования могут встречаться весьма часто (это ослабляет свойства гаммы); например, если управляющая гамма является σ-периодической последовательностью [3], то есть если существует разбиение последовательности на слова одинаковой длины, при котором сумма элементов в каждом слове одинакова. Любая периодическая последовательность разбивается на такие отрезки, например на периоды. Для обеспечения положительных криптографических свойств важно, чтобы не существовало более глубокого разбиения последовательности на указанные слова.

В настоящей работе определяются h-периодические последовательности, где h — некоторое обобщение хеш-функции, позволяющее обобщить и свойство σ-периодичности.

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

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.

1. Периодические и h-периодические последовательности

Пусть $\mathbb{N}$ — множество натуральных чисел; $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; $X_\to = \{x_0, x_1, \ldots\}$ — последовательность над множеством X; $X^* = \bigcup\limits_{s\geqslant 1} X^s$ — 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 $x_\nu, x_{\nu+1}, \ldots, x_{\nu+s-1}$ длины s в алфавите X (обозначим его $x_{(\nu,s)}$) называют s-граммой последовательности $X_\to$, где $s \in \mathbb{N}$, $\nu \in \mathbb{N}_0$.

Последовательность $X_\to$ называют периодической, если $x_i = x_{i+t}$ при всех $i \geqslant \nu$. При этом говорят, что в $X_\to$ имеются совпадения на расстоянии t с начальным номером ν. Наименьшее из расстояний совпадения t называют длиной периода последовательности $X_\to$ (обозначается $t(X_\to)$), и при $t = t(X_\to)$ наименьший из начальных номеров совпадения ν называют длиной ее предпериода (обозначается $\nu(X_\to)$).

Обозначим для краткости $t = t(X_\to)$, $\nu = \nu(X_\to)$. Тогда период последовательности $X_\to$ есть слово $x_{\nu+i}, x_{\nu+i+1}, \ldots, x_{\nu+i+t-1}$ при любом $i \geqslant 0$, а предпериод — слово $x_0, x_1, \ldots, x_{\nu-1}$ при $\nu > 0$. Если $\nu(X_\to) = 0$, то $X_\to$ предпериода не имеет и называется чисто периодической последовательностью. Напомним элементарные свойства периодических последовательностей [1, с.130].

Свойство 1. Если в $X_\to$ имеются совпадения на расстоянии τ с начальным номером μ, то t делит τ и $\nu = \mu$.

Свойство 2. Пусть $X_\to$ — периодическая последовательность, $Y_\to = f^*(X_\to) = \{f(x_i)\}$, где $f : X \to Y$. Тогда $Y_\to$ — также периодическая последовательность, при этом $\nu(Y_\to) \leqslant \nu(X_\to)$ и $t(Y_\to)$ делит $t(X_\to)$. В частности, если f — биекция, то $\nu(Y_\to) = \nu(X_\to)$ и $t(Y_\to) = t(X_\to)$.

Свойство 3. Множество периодических последовательностей над полем P, длины периодов которых делят натуральное t, образуют линейное пространство над P.

Рассмотрим функцию $h : X^* \to Y$, 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 $h^s : X^s \to Y$, $s \geqslant 1$.

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

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

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

Равенство (1) будем интерпретировать так: в $X_\to$ имеются h^s-совпадения с начальным номером μ. Наименьшее из таких s назовем длиной h-периода последовательности $X_\to$ (обозначается $t_h(X_\to)$, 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 $x_0, x_1, \ldots, x_{\mu-1}$, где $s = t_h$ и $\mu = \nu_h, k = 0, 1, \ldots$

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

$$X_\rightarrow = \{a, 2a, 0, 0, 2a, a, a, 2a, 0, 0, 2a, a, a, 2a, 0 \ldots\} \tag{2}$$

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.

Свойство 4. Периодическая последовательность $X_\rightarrow$ с длиной предпериода ν и длиной периода t является h-периодической для любой функции $h : X^* \to Y$; при этом $t_h \leqslant t$, $\nu_h \leqslant \nu$ (в $X_\rightarrow$ имеются h^t-совпадения с начальным номером ν).

Свойство 5. Подпоследовательность $\{x_i, x_{i+1}, \ldots\}$ 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.

Свойство 6. Не всякая h-периодическая последовательность является периодической.

Примером является последовательность хаотически чередующихся s-грамм u и w в алфавите X, где $h^s(u) = h^s(w)$:

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

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 апериодическая последовательность s-грамм u и w.

2. Связь длин периодов и h-периодов последовательностей при аддитивной функции

Пусть Y — аддитивная полугруппа. Функцию $h : X^* \to Y$ 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 $L : X^* \to \mathbb{N}$, определенная для $u = x_1 x_2 \ldots x_\ell \in \in X^\ell$ формулой
$$L(u) = \ell.$$
2) Частота символа a в слове u, где $a \in X$; обозначим эту функцию $m_a(u)$.
3) Пусть $X = \{a_1, a_2, \ldots, a_k\}$, $m_i(u)$ — частота символа a_i в слове u, $i = 1, \ldots, k$. Функцией маркировки слов назовем функцию $m : X^* \to \mathbb{N}_0^k$, определенную формулой
$$m(u) = (m_1(u), \ldots, m_k(u)).$$

4) Пусть $X = \mathbb{N}_0$ или $X = \mathrm{GF}(k)$, где k — простое, и $u = x_1 x_2 \dots x_\ell \in X^\ell$. Функцией веса слов из X^* назовем функцию $\mathrm{wt} : X^* \to \mathbb{N}_0$, определенную формулой

$$\mathrm{wt}(u) = \mathrm{wt}(x_1) + \dots + \mathrm{wt}(x_\ell),$$

где $\mathrm{wt}(x_i) = x_i$ для любого $x_i \in X$.

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

Доказательство. По свойству 4 $t_h \leqslant t$. Пусть t_h не делит t, тогда разделим t на t_h с остатком:

$$t = kt_h + r, \quad 0 < r < t_h. \tag{3}$$

Покажем, что в последовательности $X_\to$ имеются h^θ-совпадения, где $\theta = (t_h, r)$. Так как $\theta < t_h$, то это приводило бы к противоречию, состоящему в том, что длина h-периода меньше t_h.

В соответствии с определением числа θ имеем: $t_h = p\theta$, $r = \delta\theta$, где $(p, \delta) = 1$. Тогда из (3) следует: $t = q\theta$, где $q = (kp + \delta)$.

Представим последовательность $X_\to$ как конкатенацию t_h-грамм: $X_\to = \{u_0 u_1 \dots\}$, где $u_i = x_{ip\theta} x_{ip\theta+1} \dots x_{ip\theta+p\theta-1}$, и как конкатенацию θ-грамм: $X_\to = \{w_0 w_1 \dots\}$, где $w_i = x_{i\theta} x_{i\theta+1} \dots x_{i\theta+\theta-1}$, $i \in \mathbb{N}_0$. Так как $\mathrm{HOK}(t, t_h) = qp\theta$, то слово $x_0 x_1 \dots x_{qp\theta-1}$ в последовательности $X_\to$ есть, с одной стороны, конкатенация t_h-грамм: $u_0 u_1 \dots u_{q-1}$, и, с другой стороны, конкатенация θ-грамм: $w_0 w_1 \dots w_{qp-1}$. Длина h-периода последовательности $X_\to$ есть t_h, поэтому при $i = 0, 1, \dots, q-1$

$$h^{p\theta}(u_i) = h^{p\theta}(u_{i+1}). \tag{4}$$

Вместе с тем из равенства $(p, \delta) = 1$ следует, что $(p, q) = 1$, значит (в соответствии с леммой Шора), упорядоченный набор слов $(u_0, u_1, \dots, u_{q-1})$ есть перестановка упорядоченного набора слов $(z_0, z_1, \dots, z_{q-1})$, где $z_i = w_i w_{i+1} \dots w_{i+p-1}$, $i = 0, 1, \dots, q-1$. Тогда из (4) получаем при $i = 0, 1, \dots, q-1$

$$h^{p\theta}(z_i) = h^{p\theta}(z_{i+1}).$$

Отсюда в соответствии с аддитивностью функции h выполнена цепь равенств:

$$\begin{aligned} h^\theta(w_i) + h^\theta(w_{i+1}) + \dots + h^\theta(w_{i+p-1}) \;&=\; h^{p\theta}(z_i) = \\ &= h^{p\theta}(z_{i+1}) \;= h^\theta(w_{i+1}) + \dots + h^\theta(w_{i+p-1}) + h^\theta(w_{i+p}), \end{aligned}$$

из которой следует, что $h^\theta(w_i) = h^\theta(w_{i+p})$, $i = 0, 1, \dots, q-1$. Последняя система равенств равносильна при $(p, q) = 1$ системе равенств

$$h^\theta(w_i) = h^\theta(w_{i+1}),$$

которая выполнена не только для $i = 0, 1, \dots, q-1$, но в силу периодичности последовательности $X_\to$ и для всех $i \in \mathbb{N}_0$. Отсюда следует, что длина h-периода последовательности $X_\to$ не превышает θ; значит, она меньше t_h, т. е. имеем противоречие. ■

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.

3. h-периодичность рекуррентных последовательностей

Обозначим через ЛРПmax-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 ЛРПmax-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) $h = \mathrm{wt}(u)$, где $P = \mathrm{GF}(2)$ или $P = \mathrm{GF}(3)$.

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

Доказательство. На периоде ЛРПmax-n содержится $k^{n-1} - 1$ нулей и по k^{n-1} остальных элементов поля P [1, с. 166]. Длина h-периода ЛРПmax-n делит длину периода в силу аддитивности функции $m_a(u)$, то есть $k^n - 1 = dt_h$, где $d \geqslant 1$. Тогда период ЛРПmax-n разделяется на такие слова $u_1, \ldots, u_d$ одинаковой длины, что $m_a(u_1) = \ldots = m_a(u_d)$. Следовательно, d делит $m_a(u)$, где $m_a(u) = k^{n-1}$, что возможно только при $d = 1$, так как $(k^n - 1, k^{n-1}) = 1$. Тем самым доказано и «б». Также доказано и «в» при $P = \mathrm{GF}(2)$, так как в этом случае функции $m_1(u)$ и $\mathrm{wt}(u)$ совпадают.

По теореме 1 $t_{\mathrm{wt}} = (k^n - 1)/d$, где d делит $k^n - 1$. Вес периода u ЛРПmax-n над простым полем $\mathrm{GF}(k)$, где $k \geqslant 3$, равен

$$\mathrm{wt}(u) = \sum_{i=1}^{k-1} i \cdot k^{n-1} = \frac{k^n(k-1)}{2}.$$

Тогда в силу аддитивности функции wt вес wt-периода ЛРПmax-n равен $k^n(k-1)/(2d)$. Следовательно, d делит $(k-1)/2$, так как $(k^n - 1, k^{n-1}) = 1$.

Отсюда имеем, в частности, что $d = 1$ при $k = 3$, т. е. $t_{\mathrm{wt}} = 3^n - 1$ при $P = \mathrm{GF}(3)$. ■

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 $\{m_0(u), m_1(u), m(u), \mathrm{wt}(u)\}$.

Доказательство. Пусть $X_{\rightarrow} = \{x_0, x_1, \ldots\}$ — последовательность де Брёйна, имеющая длину периода 2^n. На ее периоде имеется 2^{n-1} единиц и столько же нулей. Следовательно, имеется хотя бы одно разделение периода последовательности де Брёйна на два слова u_1, u_2 длины 2^{n-1}, таких, что $m_0(u_1) = m_0(u_2)$ и $m_1(u_1) = m_1(u_2)$. Следовательно, при указанном разделении $m(u_1) = m(u_2)$ и $\mathrm{wt}(u_1) = \mathrm{wt}(u_2)$. ■

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

4. К анализу генераторов гаммы с неравномерным движением

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 по-

лем $X = \mathrm{GF}(k)$, управляющая движением информации в линейных регистрах сдвига ЛРС-0, ..., ЛРС-$(k-1)$ над полем P, которые реализуют линейные подстановки $g_0, \ldots, g_{k-1}$ 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 $g = (g_0, \ldots, g_{k-1})$. Пусть в i-м такте состояние всех ЛРС генератора есть $y(i) = (y_0(i), \ldots, y_{k-1}(i))$, где $y_j(i)$ — состояние ЛРС-j, $j = 0, \ldots, k-1, i \geqslant 0$. 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 $G(i,\tau) = g(i)\cdot g(i+1)\cdot\ldots\cdot g(i+\tau-1)$; тогда

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

где $z_j(i,\tau) = m_0(i,\tau)\cdot\delta(0,j) + \ldots + m_{k-1}(i,\tau)\cdot\delta(k-1,j)$ — суммарная продвижка ЛРС-j при управляющем слове $x_{(i,\tau)}, j = 0, \ldots, k-1$. Заметим, что $G(i,\tau)$ и $G(\ell,\tau)$ суть одинаковые линейные подстановки пространства P^n, если одинаковы наборы величин $(z_0(i,\tau), \ldots, z_{k-1}(i,\tau))$ и $(z_0(\ell,\tau), \ldots, z_{k-1}(\ell,\tau))$. Отсюда если m — функция маркировки слов и $x_{(i,\tau)}$ есть m-период управляющей гаммы, то наборы величин $(z_0(i+r\tau,\tau), \ldots, z_{k-1}(i+r\tau,\tau))$ одинаковы при любом $r = 0, 1, \ldots$ 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 $i \in \{0, \ldots, \tau-1\}$ и при $r = 0, 1, \ldots$, 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. *Горъков 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 госуниверситета. 2007. Приложение № 23. С. 4–11.