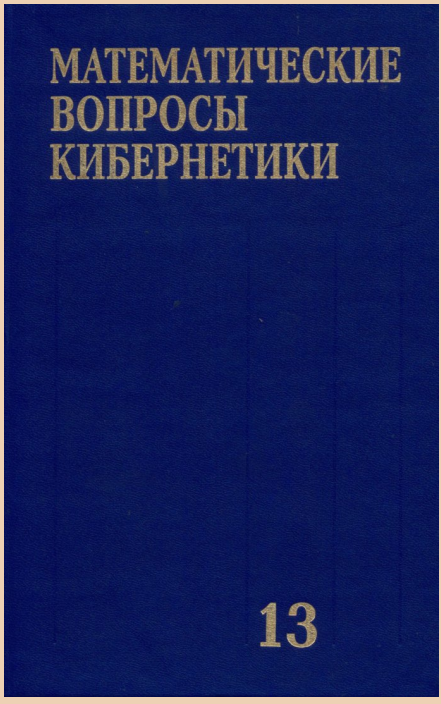
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 13




**В. М. Фомичев**

# О периодах усложненных последовательностей

**Рекомендуемая форма библиографической ссылки:** Фомичев В. М. О периодах усложненных последовательностей // Математические вопросы кибернетики. Вып. 13. — М.: ФИЗМАТЛИТ, 2004. — С. 37–40. URL: http://library.keldysh.ru/mvk.asp?id=2004-37

# О ПЕРИОДАХ УСЛОЖНЁННЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

***В. М. ФОМИЧЁВ***

(МОСКВА)

## Введение

Последовательность $\{x_1, x_2, \ldots, x_t, \ldots\}$ элементов множества $X$ назовём последовательностью над $X$ и обозначим $X_{\rightarrow}$.

Последовательность $X_{\rightarrow} = \{x_1, x_2, \ldots, x_t, \ldots\}$ над $X$ называется *чисто периодической с периодом* $T$, если $T$ — наименьшее из натуральных чисел, при котором $x_t = x_{t+T}$ для всех натуральных $t$.

Пусть $X_{i\rightarrow} = \{x_{t,i}\}$ — чисто периодическая последовательность над множеством $X_i$ с периодом $T_i$, $i = 1, \ldots, n$. Из последовательностей $X_{i\rightarrow}$ образуем последовательность $X_{\rightarrow} = \{x_t\}$ над $X$, $t = 1, 2, \ldots$, где $x_t = (x_{t,1}, \ldots, x_{t,n})$ и $X$ — декартово произведение множеств $X_1 \times \ldots \times X_n$. Последовательность $X_{\rightarrow}$ назовём *сопряжением* последовательностей $X_{1\rightarrow}, \ldots, X_{n\rightarrow}$, при этом используем обозначение $X_{\rightarrow} = X_{1\rightarrow}{}^* \ldots {}^* X_{n\rightarrow}$. Последовательность $Y_{\rightarrow} = \{\varphi(x_{t,1}, \ldots, x_{t,n})\}$, полученную из последовательности $X_{1\rightarrow}{}^* \ldots {}^* X_{n\rightarrow}$ с помощью отображения $\varphi(x_1, \ldots, x_n)$: $X_1 \times \ldots \times X_n \mapsto Y$, назовём *усложнённой* по отношению к исходным последовательностям $X_{1\rightarrow}, \ldots, X_{n\rightarrow}$.

Одной из важных задач дискретной математики является изучение зависимости периода усложнённых последовательностей от периодов исходных последовательностей. В данной работе оценивается период $T_Y$ последовательности $Y_{\rightarrow}$, полученной из последовательности $X_{1\rightarrow}{}^* \ldots {}^* X_{n\rightarrow}$ с помощью отображения $\varphi(x_1, \ldots, x_n)$, биективного по некоторым переменным.

Верхняя оценка известна уже давно [4] и имеет вид:

$$T_Y \mid НОК(T_1, \ldots, T_n).$$

Наиболее сложным является получение нижних оценок периода $T_Y$. К известным результатам подобного рода относятся оценки периода почленной суммы двух периодических последовательностей. С. Г. Гюнтер и Р. А. Рюппель [2, 3] независимо показали, что если $X_{1\rightarrow}$ и $X_{2\rightarrow}$ — последовательности над аддитивной группой X периодов $T_1$ и $T_2$ соответственно и $\varphi(x_{t,1}, x_{t,2}) = x_{t,1} + x_{t,2}$, $t = 1, 2, \ldots$, то

$$\frac{НОК(T_1, T_2)}{НОД(T_1, T_2)} \leqslant T_Y \leqslant НОК(T_1, T_2). \qquad (1)$$

## Оценка периодов усложнённых последовательностей

Оценим период $T_Y$ для произвольного $n$ и отображений $\varphi(x_1, \ldots, x_n)$, биективных по некоторым переменным. Введем обозначения:

$$N = HOK(T_1, \ldots, T_n),$$
$$N_i = HOK(T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_n), \quad i = 1, \ldots, n.$$

Теорема 1. *Если отображение $\varphi(x_1, \ldots, x_n)$ биективно по переменным с номерами $i_1, \ldots, i_b$, где $\{i_1, \ldots, i_b\} \subseteq \{1, \ldots, n\}$, $1 \leqslant b \leqslant n$, то*

$$T_Y \geqslant \prod_{h=1}^{b} \frac{N}{N_{i_h}}.$$

Доказательство. Пусть каноническое разложение числа $N$ имеет вид:

$$N = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}, \tag{2}$$

где $p_1, \ldots, p_s$ — попарно различные простые числа, $k_1, \ldots, k_s$ — натуральные числа. Так как $T_i \mid N$ и $N_i \mid N$ для каждого $i \in \{1, \ldots, n\}$, то числа $T_i$ и $N_i$ однозначно разлагаются в произведения неотрицательных степеней чисел $p_1, \ldots, p_s$:

$$T_i = p_1^{k_{i1}} \cdot \ldots \cdot p_s^{k_{is}}, \tag{3}$$

где в соответствии с определением числа $N$ и равенством (2) $k_{ij}$ — целые неотрицательные числа, $k_j = \max\{k_{1j}, \ldots, k_{nj}\}$, $i = 1, \ldots, n$, $j = 1, \ldots, s$;

$$N_i = p_1^{k_{1\setminus i}} \cdot \ldots \cdot p_s^{k_{s\setminus i}}, \tag{4}$$

где в соответствии с равенствами (2), (3) и определением чисел $N_i$ целые неотрицательные числа $k_{j\setminus i}$ задаются равенствами, $i = 1, \ldots, n$, $j = 1, \ldots, s$:

$$k_{j\setminus i} = \max_{r \in \{1, \ldots, n\} \setminus \{i\}} k_{rj}. \tag{5}$$

Обозначим $m_i = \frac{N}{N_i}$, $i = 1, \ldots, n$, и, используя равенства (2) и (4), запишем их разложения:

$$m_i = p_1^{k_1 - k_{1\setminus i}} \cdot \ldots \cdot p_s^{k_s - k_{s\setminus i}}, \tag{6}$$

где из (5) следует, что $k_j \geqslant k_{j\setminus i}$, $j = 1, \ldots, s$.

Пусть $p_j \mid m_i$, где $j \in \{1, \ldots, s\}$, $i \in \{1, \ldots, n\}$. В соответствии с равенством (6) это означает, что $k_j > k_{j\setminus i}$. Отсюда и из равенств (5) следует, что

$$k_j = \max\{k_{1j}, \ldots, k_{nj}\} = k_{ij},$$

и, следовательно, с учётом (5) для каждого $r \in \{1, \ldots, n\} \setminus \{i\}$ выполнено:

$$k_{j\setminus r} = k_{ij} = k_j.$$

Отсюда и из равенства (6) вытекает, что $p_j$ не делит число $m_r$ при любом $r \in \{1, \ldots, n\} \setminus \{i\}$. Таким образом, ненулевая степень каждого из чисел $p_1, \ldots, p_s$ записана в разложении не более чем одного из чисел $m_1, \ldots, m_n$.

В силу попарной взаимной простоты чисел $p_1, \ldots, p_s$ это равносильно тому, что $\{m_1, \ldots, m_n\}$ есть множество попарно взаимно простых чисел.

Пусть $B_i$ есть подмножество чисел $j$ множества $\{1, \ldots, s\}$, для которых ненулевая степень числа $p_j$ записана в разложении числа $m_i$:

$$m_i = \prod_{j \in B_i} p_j^{k_j - k_{j \setminus i}}, \tag{7}$$

и $B_{n+1}$ есть подмножество чисел $j$ множества $\{1, \ldots, s\}$, для которых ненулевая степень числа $p_j$ не записана в разложении ни одного из чисел $m_1, \ldots, m_n$. Так как ненулевая степень каждого из чисел $p_1, \ldots, p_s$ записана в разложении не более чем одного из чисел $m_1, \ldots, m_n$, то множества $B_1, \ldots, B_n, B_{n+1}$ образуют систему блоков разбиения множества $\{1, \ldots, s\}$. Некоторые блоки могут быть пустыми, при этом $B_i = \varnothing$ тогда и только тогда, когда $m_i = 1$, $i = 1, \ldots, n$.

Без ограничения общности рассуждений можно считать, что отображение $\varphi(x_1, \ldots, x_n)$ биективно по переменным $x_1, \ldots, x_b$, где $1 \leqslant b \leqslant n$. Докажем, что

$$T_Y \geqslant m_1 \cdot \ldots \cdot m_b. \tag{8}$$

Если $m_1 = \ldots = m_b = 1$, то неравенство (8) тривиально.

Если среди чисел $m_1, \ldots, m_b$ ровно $c$ чисел превышают 1, где $1 \leqslant c \leqslant b$, то без ущерба для общности рассуждений положим, что $m_1 > 1, \ldots, m_c > 1$ и, если $c < b$, то $m_{c+1} = \ldots = m_b = 1$.

Предположим что неравенство (8) неверно, т. е. $T_Y < m_1 \cdot \ldots \cdot m_c$. С учётом равенств (7) данное предположение принимает вид:

$$T_Y < \prod_{i=1}^{c} \prod_{j \in B_i} p_j^{k_j - k_{j \setminus i}}, \tag{9}$$

где для $i = 1, \ldots, c$ блок $B_i$ не пуст и, следовательно, $k_j > k_{j \setminus i}$ для всех $j \in B_i$.

Так как $T_Y \mid N$, то число $T_Y$ однозначно представляется в виде:

$$T_Y = p_1^{l_1} \cdot \ldots \cdot p_s^{l_s}, \tag{10}$$

где $0 \leqslant l_j \leqslant k_j$ для $j = 1, \ldots, s$ и для некоторой пары $(i, j)$, где $i \in \{1, \ldots, c\}$, $j \in B_i$, выполнено неравенство $l_j < k_j - k_{j \setminus i}$, иначе имеем противоречие с предполагаемым неравенством (9).

Пусть, например, для $r \in B_1$ выполнено неравенство $l_r < k_r - k_{r \setminus 1}$. Заметим, что блок $B_1$ не пуст и для $r \in B_1$ выполнено неравенство $k_r - k_{r \setminus 1} > 0$, из которого с учётом (5) следует, что

$$k_r = k_{1r}. \tag{11}$$

Рассмотрим число $\theta = p_1^{w_1} \cdot \ldots \cdot p_s^{w_s}$, где $w_r = l_r + k_{r \setminus 1}$ и $w_j = k_j$ для всех $j \in \{1, \ldots, s\} \setminus \{r\}$. Из определения чисел $w_j$ следует, что $w_j \geqslant k_{j \setminus 1}$ для всех $j = 1, \ldots, s$, поэтому из равенства (4) получаем, что $\theta$ кратно $N_1$, и, следовательно, $\theta$ кратно каждому из чисел $T_2, \ldots, T_n$. Поэтому для $i = 2, \ldots$ $\ldots, n$ и всех $t = 1, 2, \ldots$

$$x_{t,i} = x_{t+\theta,i}. \tag{12}$$

В то же время, из определения чисел $w_j$ и условий $l_j \leqslant k_j$, $j = 1, \ldots$ $\ldots, s$, следует, что $w_j \geqslant l_j$ для всех $j = 1, \ldots, s$. Отсюда и из равенства (10) вытекает, что $\theta$ кратно периоду $T_Y$, т. е. для всех $t = 1, 2, \ldots$

$$\varphi(x_{t,1}, x_{t,2}, \ldots, x_{t,n}) = \varphi(x_{t+\theta,1}, x_{t+\theta,2}, \ldots, x_{t+\theta,n}).$$

Из последнего равенства с учётом (12) имеем для всех $t = 1, 2, \ldots$

$$\varphi(x_{t,1}, x_{t,2}, \ldots, x_{t,n}) = \varphi(x_{t+\theta,1}, x_{t,2}, \ldots, x_{t,n}). \tag{13}$$

Вместе с тем, в условиях предполагаемого неравенства $l_r < k_r - k_{r\setminus 1}$ из равенства $w_r = l_r + k_{r\setminus 1}$ следует неравенство $w_r < k_r$, откуда с учётом равенства (11) вытекает: $w_r < k_{1r}$. Последнее неравенство с учётом (3) означает, что $\theta$ не кратно $T_1$. Следовательно, при некотором натуральном $t$

$$x_{t,1} \neq x_{t+\theta,1}.$$

Последнее неравенство несовместимо с (13) при отображении $\varphi(x_1, \ldots, x_n)$, биективном по первой переменной.

Следовательно, справедливо неравенство (8). Теорема доказана.

Следствие 1. *Если отображение $\varphi(x_1, \ldots, x_n)$ биективно по каждой переменной и числа $\frac{T_1}{d}, \ldots, \frac{T_n}{d}$ попарно взаимно просты, где $d = НОД(T_1, \ldots, T_n)$, то $T_Y \geqslant \frac{НОК(T_1, \ldots, T_n)}{НОД(T_1, \ldots, T_n)}$.*

Доказательство. Пусть $\tau_i = \frac{T_i}{d}$, $i = 1, \ldots, n$. Тогда в условиях следствия 1 $N = \tau_1 \cdot \ldots \cdot \tau_n \cdot d$, $N_i = \tau_1 \cdot \ldots \cdot \tau_{i-1} \cdot \tau_{i+1} \cdot \ldots \cdot \tau_n \cdot d$ и $\frac{N}{N_i} = \tau_i$, $i = 1, \ldots, n$. По теореме 1

$$T_Y \geqslant \tau_1 \cdot \ldots \cdot \tau_n = \frac{НОК(T_1, \ldots, T_n)}{НОД(T_1, \ldots, T_n)}.$$

Из следствия 1 получаем условия максимальности периода усложнённой последовательности.

Следствие 2. *Если отображение $\varphi(x_1, \ldots, x_n)$ биективно по каждой переменной и периоды $T_1, \ldots, T_n$ попарно взаимно просты, то $T_Y = T_1 \cdot \ldots \cdot T_n$.*

Замечание. Период усложнённой последовательности максимален и при других условиях. В частности [1, теорема 18.2], если $X_{1\rightarrow}, \ldots, X_{n\rightarrow}$ суть выходные последовательности двоичных линейных регистров сдвига с примитивными характеристическими многочленами и попарно взаимно простыми периодами $T_1, \ldots, T_n$ и отображение $\varphi(x_1, \ldots, x_n)$ не имеет фиктивных переменных, то $T_Y = T_1 \cdot \ldots \cdot T_n$.

## СПИСОК ЛИТЕРАТУРЫ

1. Фомичёв В. М. Дискретная математика и криптология. Курс лекций // Под общ. ред. д-ра физ.-мат. н. Н. Д. Подуфалова. — М.: ДИАЛОГ-МИФИ, 2003.
2. Günther C. G. On some properties of the sum of two pseudorandom sequences // Paper presented at Eurocrypt'86, Linkoping, Sweden, May 20–22, 1986.
3. Rueppel R. A. Analysis and Design of Stream Ciphers. — Berlin: Springer Verlag, 1986.
4. Selmer E. S. Linear recurrence relations over finite fields. — Lecture Notes, University of Bergen, Bergen, Norway, 1966.

Поступило в редакцию 1 VI 2004