ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Март—апрель 2014. Том 21, № 2. С. 59–75

УДК 519.714

ФУНКЦИЯ ШЕННОНА БЫСТРОГО ВЫЧИСЛЕНИЯ СЛОЖНОСТИ ПО АРНОЛЬДУ ДВОИЧНЫХ СЛОВ ДЛИНЫ 2^n ДЛЯ ПРОИЗВОЛЬНЫХ ЗНАЧЕНИЙ n *)

Ю. В. Мерекин

Аннотация. Установлено точное значение функции Шеннона быстрого вычисления сложности по Арнольду двоичных слов длины 2^n в случаях, когда n имеет вид $n = m^2$, $n = m^2 + m$ и $n = m^2 + 2m$, $m \geqslant 2$. Тем самым устанавливается точное значение функции Шеннона при любом n.

Ключевые слова: двоичное слово, сложность слова, сложность по Арнольду, функция Шеннона.

Пусть $w = x_1x_2 \dots x_{2^n}$ — произвольное двоичное слово длины 2^n, $n \geqslant 1$. Для иллюстрации определения сложности по Арнольду $A(w)$ слова w воспользуемся 2^n-ярусным двоичным деревом [1] таким, что слова, расположенные на одном ярусе, имеют одинаковую сложность. В корневой вершине, соответствующей нулевому ярусу, находится слово $00\dots0$ нулевой сложности. Любым двум вершинам, соединённым ребром дерева, соответствуют слова $w = x_1x_2 \dots x_{2^n}$ и $u = y_1y_2 \dots y_{2^n}$ (w на i-м ярусе, u на $(i-1)$-м ярусе, $1 < i \leqslant 2^n$), для которых справедливо преобразование слова w в слово u с помощью оператора

$$F(w) : (w) \mapsto (u) : \ y_j = x_j \oplus x_{j+1}, \tag{1}$$

где $1 \leqslant j \leqslant 2^n$, (w) и (u) — круговые (циклические) слова, $\oplus$ является сложением по модулю два, т. е. $F(w) = u$. Заметим, что общий случай динамики с произвольной линейной рекуррентной функцией исследован в [2]. Число операторов $F(w) = w_1, F(w_1) = w_2, \dots, F(w_s) = 00\dots0$, преобразующих слово w в слово $00\dots0$, определяет величину сложности $A(w)$. Следовательно, номер яруса двоичного дерева, на котором

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 14–01–00507).

находится слово w, является значением сложности $A(w)$. Далее значение $A(w)$, являющееся натуральным числом, будем рассматривать в его двоичном представлении.

В [4] для преобразования слова $w = x_1x_2\dots x_{2^n}$ в $u = y_1y_2\dots y_{2^n}$, когда $A(w) - A(u) = h$, $1 \leqslant h = 2^r$, $0 \leqslant r \leqslant n$, введено обобщение оператора (1):

$$F(w,h) : (w) \mapsto (u) : \ y_j = x_j \oplus x_{j+h}, \tag{2}$$

где $1 \leqslant j \leqslant 2^n$, (w) и (u) — круговые слова. В операторе (2) используется параметр h, который называется *рангом* оператора $F(w,h)$. Далее в результате действия оператора $F(w,h) = u$, преобразующего произвольное слово w, сложность которого равна $A(w)$, в слово u, сложность которого равна $A(u)$, нас интересует не первичность преобразования w в u, а преобразование числа $A(w)$ в число $A(u)$.

В [5] все слова v, сложность $A(v)$ которых равна одному из чисел

$$\begin{array}{rcl} 2^k - 2^1 + 1 & = & 11\dots111, \\ 2^k - 2^2 + 1 & = & 11\dots101, \dots, \\ 2^k - 2^{k-1} + 1 & = & 10\dots001, \\ 2^k - 2^{k-1} + 0 & = & 10\dots000, \quad 1 \leqslant k \leqslant n, \end{array}$$

где справа записаны их двоичные представления, названы *итоговыми* словами и объединены в класс V итоговых слов. Показано, что сложность любого итогового слова находится очень просто.

В [5] описан метод вычисления сложности $A(w)$, состоящий в преобразовании произвольного слова w длины 2^n с помощью операторов (2) в слова из V. Если при этом используются операторы рангов $h_{i_1}, h_{i_2}, \dots$, h_{i_t}, то

$$A(w) = h_{i_1} + h_{i_2} + \dots\ + h_{i_t} + A(v).$$

Для любого слова w, отличного от итогового, существует хотя бы одно итоговое слово v, для которого в процессе преобразования $w \mapsto v$ участвует минимальное число операторов (2). Это число обозначается через $M(w \mapsto V)$ и называется *сложностью преобразования слова w в итоговое слово* [3]. Следовательно, сложность $M(w \mapsto V)$ определяется минимальным числом операторов (2), преобразующих число $A(w)$ в одно из итоговых чисел.

В [6] исследована верхняя оценка функции Шеннона

$$\mathrm{Sh}(n) = \max M(w \mapsto V),$$

где максимум берётся по всем словам w длины 2^n. В [3] доказано равенство $\mathrm{Sh}(n) = \lfloor n-2\sqrt{n}+2 \rfloor$, $n \geqslant 5$, где $n \neq m^2$, $n \neq m^2+m$ и $n \neq m^2+2m$, $m \geqslant 2$.

Ниже получены точные значения величин $\mathrm{Sh}(n)$ при $n = m^2$, $n = m^2 + m$ и $n = m^2 + 2m$. Тем самым устанавливается точное значение функции Шеннона при любом n.

Нечётное n-разрядное, $n \in \{m^2, m^2+m, m^2+2m\}, m \geqslant 2$, число $A(w)$, содержащее ровно k, $1 \leqslant k \leqslant n-2$, нулевых разрядов, обозначим через $A_k^n(w)$. Число

$$A_k^n(w) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_k}0\underbrace{11\ldots1}_{l_{k+1}}1, \qquad (3)$$

в котором каждая из длин $l_1, l_2, \ldots, l_{k+1}$ равна либо $\lfloor (n-(k+1))/(k+1) \rfloor$, либо $\lceil (n-(k+1))/(k+1) \rceil$, назовём *базовым* и обозначим через $A_{k,1}^n(w)$, если

$$\lfloor (n-(k+1))/(k+1) \rfloor = \lceil (n-(k+1))/(k+1) \rceil = (n-(k+1))/(k+1),$$

и через $A_{k,2}^n(w)$ — в противном случае.

Для любых фиксированных n и k существует либо единственное нечётное базовое число $A_{k,1}^n(w)$, либо несколько базовых нечётных чисел $A_{k,2}^n(w)$.

Пример 1. Для $m = 2$ имеем табл. 1 n-разрядных базовых чисел, где жирным шрифтом выделены базовые числа типа $A_{k,1}^n(w)$.

Если $F(w,h) = u$, а двоичное число $A(w)$ содержит единичный разряд $h = 2^r$, $0 \leqslant r \leqslant n$, то двоичное число $A(u)$ можно получить из $A(w)$ путём удаления единичного разряда h. Следовательно, сложность $M(w \mapsto V)$ определяется минимальным числом единичных разрядов, которые необходимо удалить для преобразования $A(w)$ в итоговое число $A(v)$.

Таблица 1

k	$A_{k,t}^{n=2^2}(w)$	$A_{k,t}^{n=2^2+2}(w)$	$A_{k,t}^{n=2^2+2\times2}(w)$
1	**1011**	**110111**	**11101111**
2	1001	**101011**	11011011 11010111 10110111
3		101001 100101 100011	**10101011**
4		100001	10101001 10100101 10100011 10010101 10010011 10001011
5			10100001 10010001 10001001 10000101 10000011
6			10000001

Например, в базовом числе $A^n_{k,1}(w)$ для вычисления сложности $M(w \mapsto V)$ необходимо удалить отмеченные в (3) любые k серии единиц и получить итоговое число вида

$$A(v) = \underbrace{11\ldots1}_{l}0\ldots01 \quad \text{или} \quad A(v) = \underbrace{11\ldots1}_{l+1}.$$

Любое нечётное число $A^n_k(w_s)$ может быть получено из базового числа $A^n_{k,t}(w)$ в результате перенумерации позиций.

Пусть число $A^n_k(w_s)$ получено перестановкой номеров позиций нулей в базовом числе

$$A^n_{k,1}(w) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_k}0\underbrace{11\ldots1}_{l_{k+1}}1,$$

где $l_1 = l_2 = \ldots = l_k = l_{k+1} = l$. Любая перестановка номеров позиций нулей в числе $A^n_{k,1}(w)$ приводит к увеличению длины хотя бы одной серии единичных разрядов. Следовательно, нечётное число $A^n_k(w_s)$ содержит хотя бы один из фрагментов $\ldots0\underbrace{11\ldots1}_{l+t}0\ldots1$ или $\ldots0\underbrace{11\ldots1}_{l+1+t}$, $t \geqslant 1$, которые позволяют получить итоговое число вида

$$A(v) = \underbrace{11\ldots1}_{l+t}0\ldots01 \quad \text{или} \quad A(v) = \underbrace{11\ldots1}_{l+1+t}, \quad t \geqslant 1.$$

Следовательно, справедливо

Предложение 1. *Для любого нечётного числа $A^n_k(w_s)$, полученного из базового нечётного числа $A^n_{k,1}(w)$ в результате произвольной перестановки номеров позиций, на которых стоят нули, справедливо неравенство $M(w_s \mapsto V) < M(w \mapsto V)$.*

Пусть число $A^n_k(w_s)$ получено перестановкой номеров позиций нулей в базовом числе

$$A^n_{k,2}(w) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_k}0\underbrace{11\ldots1}_{l_{k+1}}1,$$

где каждая из длин $l_1, l_2, \ldots, l_{k+1}$ равна или l, или $l+1$. Любая перестановка номеров позиций нулей в числе $A^n_{k,2}(w)$ или увеличивает максимальную длину $l+1$, или не изменяет её. Стало быть, справедливо

Предложение 2. *Для любого нечётного числа $A^n_k(w_s)$, полученного из базового нечётного числа $A^n_{k,2}(w)$ в результате произвольной перестановки номеров позиций, на которых стоят нули, справедливо неравенство $M(w_s \mapsto V) \leqslant M(w \mapsto V)$.*

Лемма 1. *Пусть $F(u,1) = w$, нечётное число $A_k^n(w)$ содержит единственную серию единичных разрядов максимальной длины и в эту серию входит младший разряд. Тогда $M(u \mapsto V) = M(w \mapsto V)$.*

Доказательство. Число $A_k^n(w)$ содержит $n-k$ единичных разрядов. Для вычисления $M(w \mapsto V)$ из числа $A_k^n(w)$ с помощью операторов $F(\cdot, h \neq 1)$ удалим все единичные разряды кроме r младших. Тогда

$$M(w \mapsto V) = n - k - r.$$

В числе $A(u) = \underbrace{1\ldots1}_{l_1}\underbrace{00\ldots0}_{r}$ интервал l_1 содержит $k-1$ нулевых разрядов. Тогда число $A(u)$ содержит $(k-1)+r$ нулевых и $n-(k-1)-r$ единичных разрядов. Для вычисления сложности $M(u \mapsto V)$, применяя $n-(k-1)-r-1 = n-k-r$ раз операторы $F(\cdot, h \neq 1)$, из числа $A(u)$ удалим $n-k+r$ единичных разрядов. В результате получим чётное итоговое число, содержащее один единичный разряд, и

$$M(u \mapsto V) = n - k - r.$$

Лемма 1 доказана.

1. Функция Шеннона $\mathrm{Sh}(n)$ при $n = m^2$

Лемма 2. *Для любых $n = m^2$ и k, $1 \leqslant k \leqslant m^2 - 2$, $m \geqslant 2$, среди всех нечётных n-разрядных базовых чисел существует единственное число*

$$A_{(m-1),1}^{m^2}(w) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_{m-1}}0\underbrace{11\ldots1}_{l_m}1, \qquad (4)$$

где $l_1 = l_2 = \ldots = l_m = m-1$, для которого сложность $M(w \mapsto V)$ достигает максимального значения, равного $(m-1)^2$.

Доказательство. Для преобразования числа (4) в нечётное итоговое число $A(v)$, применяя $(m-1)^2$ раз операторы $F(\cdot, h \neq 1)$, из (4) удалим $m-1$ серий единичных разрядов, каждая из которых имеет длину, равную $m-1$. В результате получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{m-1}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{m}$ и сложность $M(w \mapsto V) = (m-1)^2$.

Меняя число и расположение нулевых разрядов, которые содержатся в двоичном числе (4), докажем, что для всех нечётных базовых чисел $A_{k,t}^{m^2}(w_\Delta)$, $1 \leqslant k \leqslant m^2-2$, отличных от (4), имеем

$$M(w_\Delta \mapsto V) < (m-1)^2.$$

Рассмотрим два случая: $A_k^{m^2}(w_\Delta)$, $1 \leqslant k \leqslant m-2$, и $A_k^{m^2}(w_\Delta)$, $m \leqslant k \leqslant m^2-2$.

Случай 1. В любом базовом n-разрядном нечётном числе

$$A_{(m-1-\Delta),t}^{m^2}(w_\Delta) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_{m-1-\Delta}}0\underbrace{11\ldots1}_{l_{m-\Delta}}1, \tag{5}$$

где $1 \leqslant \Delta \leqslant m-2$, среди отмеченных серий единичных разрядов существует серия максимальной длины $l_{(-\Delta)} = \lceil (m^2-(m-\Delta))/(m-\Delta)\rceil$.

Чтобы получить сложность $M(w_\Delta \mapsto V)$ из числа (5), содержащего $m^2-(m-1-\Delta)$ единичных разрядов, удалим все отмеченные в (5) серии единичных разрядов кроме одной, длина которой максимальна и равна $l_{(-\Delta)}$. Получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{l_{(-\Delta)}}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{l_{(-\Delta)}+1}$ и сложность

$$M(w_\Delta \mapsto V) = m^2-(m-\Delta)-\lceil (m^2-(m-\Delta))/(m-\Delta)\rceil.$$

Для всех базовых чисел (5) докажем справедливость неравенства

$$M(w_\Delta \mapsto V) < M(w \mapsto V) = (m-1)^2, \quad 1 \leqslant \Delta \leqslant m-2. \tag{6}$$

Имеем

$$M(w_\Delta \mapsto V) < M(w \mapsto V),$$

$$m^2-(m-\Delta)-\lceil (m^2-(m-\Delta))/(m-\Delta)\rceil < (m-1)^2,$$

$$m^2-m+\Delta-\lceil m^2/(m-\Delta)\rceil + 1 < m^2-2m+1,$$

$$m < \lceil m^2/(m-\Delta)-\Delta\rceil,$$

$$m < \lceil m(m/(m-\Delta)-\Delta/m)\rceil,$$

$$m < \lceil m((m^2-(m-\Delta)\Delta)/m(m-\Delta)\rceil,$$

$$m < \lceil m(m^2-m\Delta+\Delta^2)/(m^2-m\Delta)\rceil,$$

$$m < \lceil m(1+\Delta^2/(m^2-m\Delta))\rceil,$$

$$m < \lceil m+\varepsilon\rceil, \quad \varepsilon > 0.$$

Следовательно, неравенство (6) справедливо для всех нечётных базовых чисел (5).

Случай 2. В любом базовом n-разрядном нечётном числе

$$A^{m^2}_{((m-1)+\Delta),t}(w_\Delta) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_{(m-1)+\Delta}}0\underbrace{11\ldots1}_{l_{m+\Delta}}1, \qquad (7)$$

где $1 \leqslant \Delta \leqslant m^2 - m - 1$, среди отмеченных серий единичных разрядов существует серия максимальной длины $l_{(+\Delta)} = \lceil (m^2-(m+\Delta))/(m+\Delta)\rceil$.

Чтобы получить сложность $M(w_\Delta \mapsto V)$, из числа (7), содержащего $m^2-(m-1-\Delta)$ единичных разрядов, удалим все отмеченные в (7) серии единичных разрядов кроме одной, длина которой максимальна и равна $l_{(+\Delta)}$. В результате получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{l_{(+\Delta)}}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{l_{(+\Delta)}+1}$ и сложность

$$M(w_\Delta \mapsto V) = m^2 - (m+\Delta) - \lceil (m^2 - (m+\Delta))/(m+\Delta)\rceil.$$

Для всех базовых чисел (7) докажем справедливость неравенства

$$M(w_\Delta \mapsto V) < M(w \mapsto V) = (m-1)^2, \quad 1 \leqslant \Delta \leqslant m^2 - m - 1. \qquad (8)$$

Имеем

$$M(w_\Delta \mapsto V) < M(w \mapsto V),$$
$$m^2 - (m+\Delta) - \lceil (m^2 - (m+\Delta))/(m+\Delta)\rceil < (m-1)^2,$$
$$m^2 - m - \Delta - \lceil m^2/(m+\Delta)\rceil + 1 < m^2 - 2m + 1,$$
$$m < \lceil m^2/(m+\Delta) + \Delta\rceil,$$
$$m < \lceil m(m/(m+\Delta) + \Delta/m)\rceil,$$
$$m < \lceil m((m^2 + (m+\Delta)\Delta)/m(m+\Delta)\rceil,$$
$$m < \lceil m(m^2 + m\Delta + \Delta^2)/(m^2 + m\Delta)\rceil,$$
$$m < \lceil m(1 + \Delta^2/(m^2 + m\Delta))\rceil,$$
$$m < \lceil m + \varepsilon\rceil, \quad \varepsilon > 0.$$

Следовательно, неравенство (8) верно для всех базовых чисел (7). Лемма 2 доказана.

Теорема 1. *Для любого $n = m^2$, $m \geqslant 2$, справедливо равенство*

$$\mathrm{Sh}(n) = \lfloor n - 2\sqrt{n} + 1\rfloor.$$

Доказательство. Согласно лемме 2 для любого $n = m^2$, $m \geqslant 2$, существует единственное нечётное базовое число $A^{m^2}_{(m-1),1}(w)$ такое, что $M(w \mapsto V) = (m-1)^2$. Число $A^{m^2}_{(m-1),1}(w)$ содержит единственную серию единичных разрядов максимальной длины, в которую входит младший разряд. Пусть $F(u,1) = w$, т. е. $A(u) = A^{m^2}_{(m-1),1}(w) + 1$. Тогда согласно лемме 1

$$M(u \mapsto V) = M(w \mapsto V) = (m-1)^2.$$

Для всех нечётных базовых чисел $A^{m^2}_{k,t}(w_\Delta)$, отличных от $A^{m^2}_{(m-1),1}(w)$, в силу леммы 2 имеем

$$M(w_\Delta \mapsto V) < (m-1)^2.$$

Поэтому для всех чётных чисел $A(u_\Delta)$, равных $A^{m^2}_{(m-1-\Delta),t}(w_\Delta) + 1$ или $A(u_\Delta) = A^{m^2}_{(m-1+\Delta),t}(w_\Delta) + 1$, имеем

$$M(u_\Delta \mapsto V) \leqslant (m-1)^2.$$

Пусть нечётное число $A^{m^2}_k(w_s)$, $1 \leqslant k \leqslant m^2 - 2$, $m \geqslant 2$, получено из нечётного базового числа $A^{m^2}_{k,2}(w_\Delta)$ в результате произвольной перестановки номеров позиций, на которых стоят нули. В этом случае согласно предложению 2 имеем

$$M(w_s \mapsto V) \leqslant M(w_\Delta \mapsto V) < (m-1)^2, \quad 1 \leqslant \Delta \leqslant m-2.$$

Поэтому для всех чётных чисел $A(u_s) = A^{m^2}_k(w_s) + 1$ верно неравенство

$$M(u_s \mapsto V) \leqslant (m-1)^2.$$

Для любого $n = m^2$, $m \geqslant 2$, справедливо равенство $\lfloor n - 2\sqrt{n} + 1 \rfloor = (m-1)^2$. Следовательно, $\mathrm{Sh}(n) = \lfloor n - 2\sqrt{n} + 1 \rfloor$ при $n = m^2$. Теорема 1 доказана.

2. Функция Шеннона $\mathrm{Sh}(n)$ при $m^2 + m$

Лемма 3. *Для любых $n = m^2 + m$ и k, $1 \leqslant k \leqslant m-1$, $m \geqslant 2$, среди всех нечётных n-разрядных чисел существует единственное число*

$$A^{m^2+m}_{(m-1),1}(w) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_{m-1}}0\underbrace{11\ldots1}_{l_m}1, \tag{9}$$

где $l_1 = l_2 = \ldots = l_m = m$, для которого сложность $M(w \mapsto V)$ достигает максимального значения, равного $m(m-1)$.

Доказательство. Для преобразования числа (9) в нечётное итоговое число $A(v)$, применяя $m(m-1)$ раз операторы $F(\cdot, h \neq 1)$, из (9) удалим $m-1$ отмеченных в (9) серий единичных разрядов, каждая из которых имеет длину m. В результате получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{m}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{m+1}$ и сложность

$$M(w \mapsto V) = m(m-1).$$

В любом базовом n-разрядном нечётном числе

$$A^{m^2+m}_{(m-1-\Delta),t}(w_\Delta) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_{(m-1-\Delta)}}0\underbrace{11\ldots1}_{l_{m-\Delta}}1, \qquad (10)$$

где $1 \leqslant \Delta \leqslant m-2$, максимальная длина серии единичных разрядов, в которую не входит младший разряд, равна

$$l = \lceil (m^2 + m - (m-\Delta))/(m-\Delta) \rceil.$$

Чтобы получить сложность $M(w_\Delta \mapsto V)$, из числа (10), содержащего $m^2 + m - (m-1-\Delta)$ единичных разрядов, удалим все отмеченные в (10) серии единичных разрядов кроме одной, длина которой максимальна и равна l. В результате получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{l}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{l+1}$ и сложность

$$M(w_\Delta \mapsto V) = (m^2+m) - (m-\Delta) - \lceil (m^2 + m - (m-\Delta))/(m-\Delta) \rceil.$$

Для всех базовых чисел (10) докажем справедливость неравенства

$$M(w_\Delta \mapsto V) < M(w \mapsto V) = m(m-1), \quad 1 \leqslant \Delta \leqslant m-2. \qquad (11)$$

Имеем

$$M(w \mapsto V) > M(w_\Delta \mapsto V),$$
$$m(m-1) > (m^2+m) - (m-\Delta) - \lceil ((m^2+m) - (m-\Delta))/(m-\Delta) \rceil,$$
$$m^2 - m > m^2 + m - m + \Delta - \lceil (m^2+m)/(m-\Delta) \rceil + 1,$$
$$m < \lceil m(m+1)/(m-\Delta) \rceil - \Delta - 1,$$
$$m < \lceil m((m+1)/(m-\Delta) - (\Delta+1)/m) \rceil,$$
$$m < \lceil m(m(m+1) - (m-\Delta)(\Delta+1))/m(m-\Delta) \rceil,$$
$$m < \lceil m(m^2 + m - m\Delta + \Delta^2 - m + \Delta)/(m^2 - m\Delta) \rceil,$$

$$m < \lceil m(1 + (\Delta^2 + \Delta)/(m^2 - m\Delta))\rceil,$$

$$m < \lceil m + \varepsilon\rceil, \quad \varepsilon > 0.$$

Следовательно, неравенство (11) верно для всех базовых чисел (10). Лемма 3 доказана.

Лемма 4. *Для любых $n = m^2 + m$ и k, $m \leqslant k \leqslant m^2 + m - 2$, $m \geqslant 2$, среди всех нечётных n-разрядных чисел существует единственное число*

$$A^{m^2+m}_{m,1}(w) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_m}0\underbrace{11\ldots1}_{l_{m+1}}1, \qquad (12)$$

где $l_1 = l_2 = \ldots = l_{m+1} = m - 1$, для которого сложность $M(w \mapsto V)$ достигает максимального значения, равного $m(m-1)$.

Доказательство. Для преобразования числа (12) в нечётное итоговое число $A(v)$, применяя $m(m-1)$ раз операторы $F(\cdot, h \neq 1)$, из (12) удалим m отмеченных в (12) серий единичных разрядов, каждая из которых имеет длину, равную $m-1$. В результате получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{m-1}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{m}$ и сложность

$$M(w \mapsto V) = m(m-1).$$

В любом базовом n-разрядном нечётном числе

$$A^{m^2+m}_{(m+\Delta),t}(w_\Delta) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_{m+\Delta}}0\underbrace{11\ldots1}_{l_{m+1+\Delta}}1, \qquad (13)$$

где $1 \leqslant \Delta \leqslant m^2 - 2$, среди отмеченных серий единичных разрядов существует серия максимальной длины

$$l = \lceil((m^2 + m) - (m + 1 + \Delta))/(m + 1 + \Delta)\rceil.$$

Чтобы получить сложность $M(w_\Delta \mapsto V)$, из числа (13), содержащего $m^2 + m - (m - 1 - \Delta)$ единичных разрядов, удалим все отмеченные в (13) серии единичных разрядов кроме одной, длина которой максимальна и равна l. В результате получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{l}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{l+1}$ и сложность

$$M(w_\Delta \mapsto V) = (m^2{+}m){-}(m{+}1{+}\Delta){-}\lceil((m^2{+}m){-}(m{+}1{+}\Delta))/(m{+}1{+}\Delta)\rceil.$$

Для всех базовых чисел (13) докажем справедливость неравенства

$$M(w_\Delta \mapsto V) < M(w \mapsto V) = m(m-1), \quad 1 \leqslant \Delta \leqslant m^2 - 2. \tag{14}$$

Имеем

$$M(w \mapsto V) > M(w_\Delta \mapsto V),$$

$$m(m-1) > (m^2+m)-(m+1+\Delta)-\lceil((m^2+m)-(m+1+\Delta))/(m+1+\Delta)\rceil,$$

$$m^2 - m > m^2 + m - m - 1 - \Delta - \lceil(m^2+m)/(m+1+\Delta)\rceil + 1,$$

$$m < \lceil m(m+1)/(m+1+\Delta)\rceil + \Delta,$$

$$m < \lceil m((m+1)/(m+1+\Delta) + \Delta/m)\rceil,$$

$$m < \lceil m(m^2+m+(m+1+\Delta)\Delta)/m(m+1+\Delta)\rceil,$$

$$m < \lceil m(m^2+m+m\Delta+\Delta^2+\Delta)/(m^2+m+m\Delta)\rceil,$$

$$m < \lceil m(1+(\Delta^2+\Delta)/(m^2+m+m\Delta))\rceil,$$

$$m < \lceil m+\varepsilon\rceil, \quad \varepsilon > 0.$$

Следовательно, неравенство (14) верно для всех базовых чисел (13). Лемма 3 доказана.

Теорема 2. *Для любого* $n = m^2+m,\ m \geqslant 2$ *, справедливо равенство* $\mathrm{Sh}(n) = \lfloor n - 2\sqrt{n} + 1\rfloor$.

Доказательство. Согласно лемме 3 для любых $n = m^2 + m$ и k, $1 \leqslant k \leqslant m-1$, $m \geqslant 2$, среди всех нечётных n-разрядных чисел существует единственное число $A^{m^2+m}_{(m-1),1}(w)$, для которого $M(w \mapsto V) = m(m-1)$. Число $A^{m^2+m}_{(m-1),1}(w)$ содержит единственную серию единичных разрядов максимальной длины, в которую входит младший разряд. Пусть $A(u) = A^{m^2+m}_{(m-1),1}(w) + 1$. Тогда согласно лемме 1 получаем

$$M(u \mapsto V) = M(w \mapsto V) = m(m-1).$$

Для всех нечётных чисел $A^{m^2+m}_{(m-1-\Delta),t}(w_\Delta)$, $1 \leqslant \Delta \leqslant m-2$, $m \geqslant 2$, отличных от $A^{m^2+m}_{(m-1),1}(w)$, в силу леммы 3 имеем

$$M(w_\Delta \mapsto V) < m(m-1).$$

Поэтому для всех чётных чисел $A(u_\Delta) = A^{m^2+m}_{m-1-\Delta}(w_\Delta) + 1$ верно неравенство $M(u_\Delta \mapsto V) \leqslant m(m-1)$.

Пусть нечётное число $A^{m^2+m}_{m-1-\Delta}(w_s)$, $1 \leqslant \Delta \leqslant m-2$, $m \geqslant 2$, получено из нечётного базового числа $A^{m^2+m}_{(m-1-\Delta),2}(w_\Delta)$ в результате произвольной перестановки номеров позиций, на которых стоят нули. В этом случае согласно предложению 2

$$M(w_s \mapsto V) \leqslant M(w_\Delta \mapsto V) < m(m-1).$$

Поэтому для всех чётных чисел $A(u_s) = A^{m^2}_k(w_s) + 1$ имеем

$$M(u_s \mapsto V) \leqslant m(m-1).$$

С помощью лемм 4 и 1 аналогичный результат получается для всех $n = m^2 + m$ и k, $m \leqslant k \leqslant m^2 + m - 2$, $m \geqslant 2$.

Для любого $n = m^2 + m$, $m \geqslant 2$, справедливо равенство

$$\lfloor n - 2\sqrt{n} + 1 \rfloor = m(m-1).$$

Следовательно, $\mathrm{Sh}(n) = \lfloor n - 2\sqrt{n} + 1 \rfloor$ при $n = m^2 + m$. Теорема 2 доказана.

3. Функция Шеннона $\mathrm{Sh}(n)$ при $n = m^2 + 2m$

Лемма 5. *Для любых $n = m^2 + 2m$ и k, $1 \leqslant k \leqslant m-1$, $m \geqslant 2$, среди всех нечётных n-разрядных базовых чисел существует единственное число*

$$A^{m^2+2m}_{(m-1),1}(w) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_{m-1}}0\underbrace{11\ldots1}_{l_m}1, \tag{15}$$

где $l_1 = l_2 = \ldots = l_m = m+1$, для которого сложность $M(w \mapsto V)$ достигает максимального значения, равного $m^2 - 1$.

Доказательство. Для преобразования числа (15) в нечётное итоговое число $A(v)$, применяя $m^2 - 1$ раз операторы $F(\cdot, h \neq 1)$, из (15) удалим $m-1$ отмеченных в (15) серий единичных разрядов, каждая из которых имеет длину, равную $m+1$. В результате получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{m+1}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{m+2}$ и сложность

$$M(w \mapsto V) = m^2 - 1.$$

В любом базовом n-разрядном нечётном числе

$$A^{m^2+2m}_{(m-1-\Delta),t}(w_\Delta) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_{m-1-\Delta}}0\underbrace{11\ldots1}_{l_{m-\Delta}}1, \tag{16}$$

где $1 \leqslant \Delta \leqslant m-1$, среди отмеченных серий единичных разрядов существует серия максимальной длины $l = \lceil (m^2+2m-(m-\Delta))/(m-\Delta)\rceil$.

Чтобы получить сложность $M(w_\Delta \mapsto V)$, из числа (16), содержащего $m^2+2m-(m-1-\Delta)$ единичных разрядов, удалим все отмеченные в (16) серии единичных разрядов кроме одной, длина которой максимальна и равна l. В результате получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{l}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{l+1}$ и сложность

$$M(w_\Delta \mapsto V) = (m^2+2m)-(m-\Delta)-\lceil (m^2+2m-(m-\Delta))/(m-\Delta)\rceil.$$

Для всех базовых чисел (16) докажем справедливость неравенства

$$M(w_\Delta \mapsto V) < M(w \mapsto V) = m^2-1, \quad 1 \leqslant \Delta \leqslant m-1. \tag{17}$$

Имеем

$$M(w \mapsto V) > M(w_\Delta \mapsto V),$$

$$m^2-1 > (m^2+2m)-(m-\Delta)-\lceil (m^2+2m-(m-\Delta))/(m-\Delta)\rceil,$$

$$m^2-1 > m^2+2m-m+\Delta-\lceil (m^2+2m)/(m-\Delta)\rceil+1,$$

$$m < \lceil m(m+2)/(m-\Delta)\rceil-\Delta-2,$$

$$m < \lceil m((m+2)/(m-\Delta)-(\Delta+2)/m)\rceil,$$

$$m < \lceil m(m(m+2)-(m-\Delta)(\Delta+2))/m(m-\Delta)\rceil,$$

$$m < \lceil m(m^2+2m-m\Delta+\Delta^2-2m+2\Delta)/(m^2-m\Delta)\rceil,$$

$$m < \lceil m(1+(\Delta^2+2\Delta)/(m^2-m\Delta))\rceil,$$

$$m < \lceil m+\varepsilon\rceil, \quad \varepsilon > 0.$$

Следовательно, неравенство (17) верно для всех базовых чисел (16). Лемма 5 доказана.

Лемма 6. *Для любых $n = m^2+2m$ и $k = m$, $m \geqslant 2$, существуют $m+1$ нечётных базовых n-разрядных чисел*

$$A_{m,2}^{m^2+2m}(w_i) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_m}0\underbrace{11\ldots1}_{l_{m+1}}1, \tag{18}$$

где $l_1 = l_2 = \ldots = l_{i-1} = l_{i+1} = \ldots = l_{m+1} = m$, $l_i = m-1$, $1 \leqslant i \leqslant m+1$, которые имеют сложность $M(w_i \mapsto V) = m^2-1$.

Доказательство. Каждое из чисел (18) содержит m^2+m единичных разрядов. Для преобразования числа (18) в нечётное итоговое число $A(v)$, применяя $(m-1)m+(m-1)=m^2-1$ раз операторы $F(\cdot, h\neq 1)$, из (18) удалим $m-1$ отмеченных в (18) серий единичных разрядов, каждая из которых имеет длину, равную m, и одну серию длины $m-1$. В результате получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{m}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{m+1}$ и сложность $M(w_i \mapsto V) = m^2-1$, $1 \leqslant i \leqslant m+1$. Любое отличное от (18) нечётное число $A_m^{m^2+2m}(u)$ содержит хотя бы один из фрагментов $\ldots\underbrace{11\ldots1}_{m+1}0\ldots$ или $\ldots\underbrace{11\ldots1}_{m+2}$, который не подлежит удалению при вычислении сложности $M(u\mapsto V)$. Поэтому

$$M(u\mapsto V) < M(w_i\mapsto V) = m^2-1.$$

Лемма 6 доказана.

Лемма 7. *Для любых $n=m^2+2m$ и k, $m+1\leqslant k\leqslant m^2+2m-2$, $m\geqslant 2$, среди всех нечётных n-разрядных чисел существует единственное число*

$$A_{(m+1),1}^{m^2+2m}(w) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_{m+1}}0\underbrace{11\ldots1}_{l_{m+2}}1, \qquad (19)$$

где $l_1=l_2=\ldots=l_{m+2}=m-1$, для которого сложность $M(w\mapsto V)$ достигает максимального значения, равного m^2-1.

Доказательство. Для преобразования числа (19) в нечётное итоговое число $A(v)$, применяя $(m+1)(m-1)=m^2-1$ раз операторы $F(\cdot, h\neq 1)$, из (19) удалим $m+1$ отмеченных в (19) серий единичных разрядов, каждая из которых имеет длину, равную $m-1$. В результате получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{m-1}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{m}$ и сложность $M(w\mapsto V)=m^2-1$. В любом базовом n-разрядном нечётном числе

$$A_{(m+1+\Delta),t}^{m^2+2m}(w_\Delta) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_{m+1+\Delta}}0\underbrace{11\ldots1}_{l_{m+2+\Delta}}1, \qquad (20)$$

где $1\leqslant\Delta\leqslant m^2+m-3$, максимальная длина серии единичных разрядов, в которую не входит младший разряд, равна

$$l = \lceil (m^2+2m-(m+2+\Delta))/(m+2+\Delta)\rceil.$$

Чтобы получить сложность $M(w_\Delta \mapsto V)$, из числа (20), содержащего $(m^2+m)-(m+1+\Delta)$ единичных разрядов, удалим все отмеченные в (20) серии единичных разрядов кроме одной, длина которой максимальна и равна l. В результате получим итоговое число вида $A(v) = \underbrace{11\ldots1}_{l}0\ldots01$ или $A(v) = \underbrace{11\ldots1}_{l+1}$ и сложность

$$M(w_\Delta \mapsto V) = (m^2+2m)-(m+2+\Delta) \\ - \lceil (m^2+2m-(m+2+\Delta))\big/(m+2+\Delta)\rceil.$$

Для всех базовых чисел (20) докажем справедливость неравенства

$$M(w_\Delta \mapsto V) < M(w \mapsto V) = m^2-1, \quad 1 \leqslant \Delta \leqslant m^2+m-3. \qquad (21)$$

Имеем

$$M(w \mapsto V) > M(w_\Delta \mapsto V),$$
$$m^2-1 > (m^2+2m)-(m+2+\Delta)-\lceil (m^2+2m-(m+2+\Delta))\big/(m+2+\Delta)\rceil,$$
$$m^2-1 > m^2+2m-m-2-\Delta-\lceil (m^2+2m)\big/(m+2+\Delta)\rceil+1,$$
$$m < \lceil m(m+2)\big/(m+2+\Delta)\rceil+\Delta,$$
$$m < \lceil m((m+2)\big/(m+2+\Delta)+\Delta\big/m)\rceil,$$
$$m < \lceil m(m^2+2m+(m+2+\Delta)\Delta)\big/m(m+2+\Delta)\rceil,$$
$$m < \lceil m(m^2+2m+m\Delta+2\Delta+\Delta^2)\big/(m^2+2m+m\Delta)\rceil,$$
$$m < \lceil m(1+(\Delta^2+2\Delta)\big/(m^2+2m+m\Delta))\rceil,$$
$$m < \lceil m+\varepsilon\rceil, \quad \varepsilon > 0.$$

Следовательно, неравенство (21) верно для всех базовых чисел (20). Лемма 7 доказана.

Замечание 1. Лемма 5 аналогична лемме 3, а лемма 7 — лемме 4.

Теорема 3. *Для любого* $n = m^2+2m,\ m \geqslant 2$ *, справедливо равенство* $\mathrm{Sh}_2(n) = \lfloor n-2\sqrt{n}+2\rfloor$.

Доказательство. С учётом замечания 1, как в теореме 2, для любых

(i) базовых нечётных чисел из лемм 5 и 7,

(ii) нечётных чисел, полученных из базовых в результате перестановки позиций нулей и изменения числа нулей,

(iii) чётных чисел, сложность которых превосходит сложность нечётных чисел на одну единицу,

сложность преобразования произвольного слова w в итоговое слово v не превосходит величины m^2-1.

Остаётся рассмотреть числа из леммы 6. Для любых $n = m^2+2m$ и $k = m$, $m \geqslant 2$, существуют $m+1$ нечётных базовых n-разрядных чисел $A^{m^2+2m}_{m,2}(w_i)$, для которых достигается максимальное значение сложности, равное m^2-1. Каждое из этих $m+1$ чисел, за исключением числа

$$A^{m^2+2m}_{m,2}(w_i) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_m}0\underbrace{11\ldots1}_{l_{m+1}}, \tag{22}$$

где $l_1 = l_2 = \ldots = l_{m+1} = m$, содержит единственную серию единичных разрядов максимальной длины, в которую входит младший разряд. Следовательно, согласно лемме 1 для всех этих чисел кроме числа (22) имеем

$$M(u_i \mapsto V) = M(w_i \mapsto V) = m^2-1,$$

где $A(u_i) = A^{m^2+2m}_{k,2}(w_i)+1$.

Покажем, что среди чётных чисел $A(u_i) = A^{m^2+2m}_{m,2}(w_i)+1$ существует число, для которого $M(u_i \mapsto V) = m^2$. Число (22) увеличим на одну единицу и получим

$$A(u_i) = \underbrace{11\ldots1}_{l_1}0\underbrace{11\ldots1}_{l_2}0\ldots\underbrace{11\ldots1}_{l_{m-1}}0\underbrace{11\ldots1}_{l_m}1\underbrace{00\ldots0}_{l_{m+1}}, \tag{23}$$

где $l_1 = l_2 = \ldots = l_{m+1} = m$. Для вычисления сложности $M(u_i \mapsto V)$ числа (23), которое содержит m^2+1 единичных разрядов, существуют два варианта:

$A(u_i)$ преобразуется в чётное итоговое число вида $A(v) = 10\ldots0$,

$A(u_i)$ — в нечётное итоговое число вида $A(v) = 11\ldots10\ldots01$.

В первом варианте, применяя m^2 раз операторы $F(\cdot, h \neq 1)$, удалим m^2 единичных разрядов. Во втором, применив $F(u_i, 1) = w_i$, получим число $A^{m^2+2m}_{m,2}(w_i)$, которое согласно лемме 6 имеет сложность $M(w_i \mapsto V) = m^2-1$. Следовательно,

$$A(u_i) = A^{m^2+2m}_{k,2}(w_i)+1, \quad M(u_i \mapsto V) = m^2.$$

Для любого $n = m^2+2m,\ m \geqslant 2$, верно равенство $\lfloor n-2\sqrt{n}+2\rfloor = m^2$. Следовательно, $\mathrm{Sh}(n) = \lfloor n-2\sqrt{n}+2\rfloor$ при $n = m^2+2m$. Теорема 3 доказана.

Из теорем 1–3 непосредственно следует, что для всех натуральных $n \geqslant 4$ имеем

$$\mathrm{Sh}(n) = \begin{cases} \lfloor n - 2\sqrt{n} + 1 \rfloor & \text{при } n = m^2 \text{ или } n = m^2 + m,\ m \geqslant 2; \\ \lfloor n - 2\sqrt{n} + 2 \rfloor & \text{в противном случае.} \end{cases}$$

ЛИТЕРАТУРА

1. **Арнольд В. И.** Топология и статистика формул арифметики // Успехи мат. наук. — 2003. — Т. 58, № 4. — С. 1–26.
2. **Евдокимов А. А., Пережогин А. Л.** Структура функционирования дискретных динамических систем циркулянтного типа с линейными функциями в вершинах сети // Дискрет. анализ и исслед. операций. — 2011. — Т. 18, № 3. — С. 39–48.
   Evdokimov A. A. Perezhogin A. L. Discrete dynamical systems of a circulant type with linear functions at the vertices of a network // J. Appl. Industr. Math. — 2012. — Vol. 6, N 2. — P. 160–166.
3. **Мерекин Ю. В.** Функция Шеннона вычисления сложности по Арнольду двоичных слов длины 2^n // Дискрет. анализ и исслед. операций. — 2012. — Т. 19, № 6. — С. 49–55.
   Merekin Yu. V. The Shannon function for calculating the Arnold complexity of length 2^n binary words // J. Appl. Industr. Math. — 2013. — Vol. 7, N 2. — P. 229–233.
4. **Merekin Yu. V.** On the computational complexity of the Arnold complexity of binary words // Asian-Eur. J. Math. — 2009. — Vol. 2, N 4. — P. 641–648.
5. **Merekin Yu. V.** On the computation of Arnold complexity of length 2^n binary words // Asian-Eur. J. Math. — 2011. — Vol. 4, N 2. — P. 295–300.
6. **Merekin Yu. V.** Fast computation of the Arnold complexity of length 2^n binary words // Southeast Asian Bull. Math. — 2012. — Vol. 36, N 6. — P. 855–862.

Мерекин Юрий Владимирович,
e-mail: merekin@math.nsc.ru

Статья поступила
11 февраля 2013 г.

Переработанный вариант —
25 декабря 2013 г.