ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Ноябрь—декабрь 2012. Том 19, № 6. С. 49–55

УДК 519.714

ФУНКЦИЯ ШЕННОНА ВЫЧИСЛЕНИЯ СЛОЖНОСТИ ПО АРНОЛЬДУ ДВОИЧНЫХ СЛОВ ДЛИНЫ 2^n *)

Ю. В. Мерекин

Аннотация. Для предложенного автором ранее метода быстрого вычисления сложности по Арнольду произвольных двоичных слов длины 2^n получено точное значение функции Шеннона для почти всех 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 слова* w, которую обозначим через $A(w)$, воспользуемся, как это делает Арнольд [1], 2^n-ярусным двоичным деревом. В корневой вершине, соответствующей нулевому ярусу, находится слово $00\dots0$, которое имеет нулевую сложность. 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, $\oplus$ означает сложение по модулю два. Число операторов

$$F(w) = w_1,\ F(w_1) = w_2, \dots,\ F(w_s) = 00\dots0,$$

преобразующих слово w в $00\dots0$, определяет величину $A(w)$. Следовательно, сложность $A(w)$ равна номеру яруса двоичного дерева, на котором находится слово w.

В [3] 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):

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

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 11–01–00997).

© 2012 Мерекин Ю. В.

где $1 \leqslant j \leqslant 2^n$, (w) и (u) — круговые слова. В операторе (2) используется параметр h, который назовём *рангом* оператора $F(w,h)$.

В [4] все слова v длины 2^n, $n \geqslant 1$, сложность $A(v)$ которых равна одному из чисел

$$2^k - 2^1 + 1,\ 2^k - 2^2 + 1, \dots, 2^k - 2^{k-1} + 1,\ 2^k - 2^{k-1} + 0, \quad 1 \leqslant k \leqslant n, \tag{3}$$

названы *итоговыми* словами и объединены в класс V. Показано, что сложность $A(v)$ любого итогового слова v находится очень просто.

В [4] описан метод вычисления сложности $A(w)$, состоящий в преобразовании слова w длины 2^n с помощью операторов (2) в слова из V. Если при этом используются операторы рангов $h_1, h_2, \dots, h_t$, то

$$A(w) = h_1 + h_2 + \ldots + h_t + A(v). \tag{4}$$

Пример 1. Пусть $n = 5$ и $w = x_1x_2\ldots x_{32} = 00\ldots010001$. Тогда

$$F(w, h_1 = 1) = w_1 = y_1y_2\ldots y_{32} = 00\ldots0110011,$$

$$F(w_1, h_2 = 2) = v = z_1z_2\ldots z_{32} = 00\ldots011111111.$$

В слове v каждый из фрагментов $z_iz_{i+2^3}z_{i+2\cdot2^3}z_{i+3\cdot2^3}$, $1 \leqslant i \leqslant 2^3$, содержит ровно одну единицу. В этом случае согласно теореме 1 из [4] слово v итоговое и $A(v) = 2^5 - 2^3 + 1$. Тогда $A(w) = h_1 + h_2 + A(v) = 28$ в силу (4). Таким образом, для вычисления сложности $A(w)$ достаточно применить оператор два раза.

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 обозначим через $M(w \mapsto V)$ и назовём *сложностью преобразования слова w в итоговое слово*. Нашей целью является нахождение функции Шеннона $\mathrm{Sh}(n) = \max M(w \mapsto V)$, где максимум берётся по всем круговым словам w длины 2^n.

Множество всех слов w длины 2^n, $n \geqslant 5$, разобьём на два класса: классу $S_1(n)$ принадлежат слова w с нечётной сложностью $A(w)$, а классу $S_2(n)$ — с чётной сложностью $A(w)$.

Для $S_1(n)$ определим функцию Шеннона $\mathrm{Sh}_1(n) = \max M(w \mapsto V)$, где максимум берётся по всем круговым словам w класса $S_1(n)$. Для класса $S_2(n)$ аналогично имеем $\mathrm{Sh}_2(n) = \max M(w \mapsto V)$. Тогда

$$\mathrm{Sh}(n) = \max\{\mathrm{Sh}_1(n),\ \mathrm{Sh}_2(n)\}.$$

В [2] доказано, что $\mathrm{Sh}(n) = 1,\ n \leqslant 4$, а в [5] получены верхние оценки

$$\mathrm{Sh}_1(n) \leqslant \lfloor n - 2\sqrt{n} + 1 \rfloor, \quad \mathrm{Sh}_2(n) \leqslant \lfloor n - 2\sqrt{n} + 2 \rfloor.$$

Ниже покажем, что для почти всех n верхняя оценка совпадает с нижней. Для этого достаточно для почти всех n найти круговые слова длины 2^n, для которых сложность $M(w \mapsto V)$ совпадает с верхней оценкой.

Лемма 1. *Для любого $n \geqslant 4$ справедливо равенство*

$$\lfloor n - 2\sqrt{n} + 1 \rfloor = n + 1 - \lfloor \sqrt{n} \rfloor - \lceil n/\lfloor \sqrt{n} \rfloor \rceil.$$

Доказательство. Для удобства доказательства рассмотрим три случая:

$$\lfloor n - 2\sqrt{n} + 1 \rfloor = n + 1 - \lfloor \sqrt{n} \rfloor - \lceil n/\lfloor \sqrt{n} \rfloor \rceil \\ = \begin{cases} n - 2m + 1 & \text{при } n = m^2, \\ n - 2m & \text{при } n = m^2 + i, \\ n - 2m - 1 & \text{при } n = m^2 + m + i, \end{cases} \tag{5}$$

где $1 \leqslant i \leqslant m = \lfloor \sqrt{n} \rfloor$.

Для доказательства первого из трёх случаев (5) достаточно заменить $\sqrt{n}$ на m. Докажем справедливость двух других.

1) Пусть $n = m^2 + i$, $1 \leqslant i \leqslant m$. Тогда

$$n + 1 - \lfloor \sqrt{n} \rfloor - \lceil n/\lfloor \sqrt{n} \rfloor \rceil = n + 1 - m - (\lceil (m^2 + i)/m \rceil) \\ = n + 1 - m - (m + \lceil i/m \rceil) = n + 1 - m - (m + 1) = n - 2m. \tag{6}$$

2) Пусть $n = m^2 + m + i$, $1 \leqslant i \leqslant m$. Тогда

$$n + 1 - \lfloor \sqrt{n} \rfloor - \lceil n/\lfloor \sqrt{n} \rfloor \rceil \\ = n + 1 - m - (\lceil (m^2 + m + i)/m \rceil) = n + 1 - m - (m + 1 + \lceil i/m \rceil) \\ = n + 1 - m - (m + 2) = n - 2m - 1. \tag{7}$$

3) Пусть $n = m^2 + i$, $1 \leqslant i \leqslant 2m$, $n \geqslant 4$. Тогда

$$\lfloor n - 2\sqrt{n} + 1 \rfloor = (n + 1) + \lfloor -2\sqrt{n} \rfloor = (n + 1) - \lceil 2\sqrt{n} \rceil \\ = (n + 1) - \lceil 2(m + \{\sqrt{n}\}) \rceil = (n + 1) - 2m - \lceil 2\{\sqrt{n}\} \rceil, \tag{8}$$

где $\{\sqrt{n}\}$ — дробная часть числа $\sqrt{n}$. Для завершения преобразований (8) необходимо найти границу, где $\{\sqrt{n}\ \} < 0,5$.

Представим все числа натурального ряда в виде $n = (\sqrt{n})^2 = (\lfloor\sqrt{n}\rfloor + \{\sqrt{n}\})^2 = (m + \{\sqrt{n}\})^2$ и рассмотрим произвольную конечную последовательность чисел

$$(m + \{\sqrt{m^2+1}\})^2, \ldots, (m + \{\sqrt{m^2+m}\})^2, (m + \{\sqrt{m^2+m+0,25}\})^2,$$
$$(m + \{\sqrt{m^2+m+1}\})^2, \ldots, (m + \{\sqrt{m^2+2m}\})^2,$$

в которой при любом фиксированном $m \geqslant 1$ все числа натуральные, кроме $(m + \{\sqrt{m^2+m+0,25}\})^2 = (m+0,5)^2$. Для дробных частей этой последовательности имеем неравенства

$$0 < \{\sqrt{m^2+1}\} < \ldots < \{\sqrt{m^2+m}\} < 0,5 < \{\sqrt{m^2+m+1}\}$$
$$\ldots < \{\sqrt{m^2+2m}\} < 1,$$

которые задают искомую границу $\{\sqrt{n}\ \} < 0,5$. Продолжив преобразование (8), получаем

$$\lfloor n - 2\sqrt{n} + 1\rfloor = \begin{cases} n - 2m & \text{при } n = m^2 + i,\ 1 \leqslant i \leqslant m, \\ n - 2m - 1 & \text{при } n = m^2 + m + i,\ 1 \leqslant i \leqslant m. \end{cases} \tag{9}$$

Следовательно, для всех $n \geqslant 4$ справедливы равенства (5). Лемма 1 доказана.

Из равенств (6) и (7) следует

Лемма 2. *Для любого $n \geqslant 5$ справедливы равенства*

$$\lceil n/\lfloor\sqrt{n}\rfloor\rceil = \begin{cases} m+1 & \textit{при } n = m^2 + i, \\ m+2 & \textit{при } n = m^2 + m + i, \end{cases}$$

где $1 \leqslant i \leqslant m = \lfloor\sqrt{n}\rfloor$.

Лемма 3. *Пусть $n \neq m^2$, $n \neq m^2 + m$, $n \neq m^2 + 2m$, где $m = \lfloor\sqrt{n}\rfloor$. Тогда для любого $n \geqslant 5$ справедливо неравенство*

$$\lceil n/\lfloor\sqrt{n}\rfloor\rceil(\lfloor\sqrt{n}\rfloor - 1) - (\lfloor\sqrt{n}\rfloor - 2) > \lfloor n - 2\sqrt{n} + 2\rfloor.$$

Доказательство.

Случай 1. Пусть $n = m^2 + i$, $1 \leqslant i < m$. Используя лемму 2 для левой части неравенства, получаем

$$\lceil n/\lfloor\sqrt{n}\rfloor\rceil(\lfloor\sqrt{n}\rfloor - 1) - (\lfloor\sqrt{n}\rfloor - 2)$$
$$= (m+1)(m-1) - (m-2) = m^2 - m + 1, \tag{10}$$

Используя (9) для левой части неравенства, имеем

$$\lfloor n-2\sqrt{n}+2\rfloor = n-2m+1 = m^2+i-2m+1. \qquad (11)$$

Сравнивая (10) и (11), получаем утверждение леммы для $n = m^2+i$, $1 \leqslant i < m$.

Случай 2. Пусть $n = m^2+m+i$, $1 \leqslant i < m$. Аналогично предыдущему случаю получаем равенства

$$\lceil n/\lfloor\sqrt{n}\rfloor\rceil(\lfloor\sqrt{n}\rfloor-1)-(\lfloor\sqrt{n}\rfloor-2) = (m+2)(m-1)-(m-2) = m^2,$$

$$\lfloor n-2\sqrt{n}+2\rfloor = n-2m+2 = m^2+m+i-2m = m^2+i-m,$$

которые подтверждают справедливость утверждения леммы для $n = m^2+m+i$, $1 \leqslant i < m$. Лемма 3 доказана.

Теорема 1. *Для любого $n \geqslant 5$ справедливо равенство*

$$\mathrm{Sh}_1(n) = \lfloor n-2\sqrt{n}+1\rfloor.$$

Доказательство. Пусть сложность $A(w)$ задаётся нечётным двоичным числом

$$A(w) = \underbrace{11\ldots10}_{l_1}\underbrace{11\ldots10}_{l_2}\ldots\underbrace{11\ldots10}_{l_{\lfloor\sqrt{n}\rfloor-1}}\underbrace{11\ldots11}_{l_{\lfloor\sqrt{n}\rfloor}}, \qquad (12)$$

где длины начальных $\lfloor\sqrt{n}\rfloor-1$ интервалов одинаковы и равны $\lceil n/\lfloor\sqrt{n}\rfloor\rceil$, а длина последнего интервала равна $l_{\lfloor\sqrt{n}\rfloor}$, $2 \leqslant l_{\lfloor\sqrt{n}\rfloor} \leqslant \lceil n/\lfloor\sqrt{n}\rfloor\rceil$, $n \geqslant 5$.

В числе (12) все единицы интервалов $2, 3, \ldots, \lfloor\sqrt{n}\rfloor-1$ и начальные $l_{\lfloor\sqrt{n}\rfloor}-1$ единиц последнего интервала $\lfloor\sqrt{n}\rfloor$ заменим нулями с помощью операторов $F(\cdot,h)$, ранги которых отличны от единицы. В результате получим

$$A(v) = 11\ldots100\ldots01, \qquad (13)$$

т. е. число из (3), которое содержит $\lceil n/\lfloor\sqrt{n}\rfloor\rceil$ единичных разрядов.

Число операторов $F(\cdot,h)$, которые участвуют в процессе преобразования слова w в итоговое слово v, равно

$$n-(\lfloor\sqrt{n}\rfloor-1)-\lceil n/\lfloor\sqrt{n}\rfloor\rceil = n+1-\lfloor\sqrt{n}\rfloor-\lceil n/\lfloor\sqrt{n}\rfloor\rceil,$$

где $\lfloor\sqrt{n}\rfloor-1$ — число нулевых разрядов в (12), а $\lceil n/\lfloor\sqrt{n}\rfloor\rceil$ — число единичных разрядов в (13).

Согласно равенству леммы 1 имеем

$$n+1-\lfloor\sqrt{n}\rfloor-\lceil n/\lfloor\sqrt{n}\rfloor\rceil = \lfloor n-2\sqrt{n}+1\rfloor.$$

Теорема 1 доказана.

Теорема 2. *Пусть $n \neq m^2$, $n \neq m^2+m$, $n \neq m^2+2m$, где $m = \lfloor\sqrt{n}\rfloor$. Тогда для любого $n \geqslant 5$ справедливо равенство*

$$\mathrm{Sh}_2(n) = \lfloor n - 2\sqrt{n} + 2\rfloor.$$

Доказательство. Пусть $A(w_1)$ чётно и

$$A(w_1) = \underbrace{11\ldots10}_{l_1}\underbrace{11\ldots10}_{l_2}\ldots\underbrace{11\ldots10}_{l_{\lfloor\sqrt{n}\rfloor-2}}\underbrace{11\ldots11}_{l_{\lfloor\sqrt{n}\rfloor-1}}\ \underbrace{00\ldots00}_{l_{\lfloor\sqrt{n}\rfloor}}. \tag{14}$$

В этом представлении длины начальных $(\lfloor\sqrt{n}\rfloor-1)$ интервалов, содержащих единицы, одинаковы и равны $\lceil n/\lfloor\sqrt{n}\rfloor\rceil$, а длина последнего интервала, содержащего только нули, равна $l_{\lfloor\sqrt{n}\rfloor}$, $2 \leqslant l_{\lfloor\sqrt{n}\rfloor} \leqslant \lceil n/\lfloor\sqrt{n}\rfloor\rceil - 1$, $n \geqslant 5$. Число единичных разрядов, содержащихся в (14), равно

$$\lceil n/\lfloor\sqrt{n}\rfloor\rceil(\lfloor\sqrt{n}\rfloor - 1) - (\lfloor\sqrt{n}\rfloor - 2). \tag{15}$$

Согласно лемме 3 число (15) превосходит величину $\lfloor n - 2\sqrt{n} + 2\rfloor$.

Рассмотрим два случая преобразования $w_1 \mapsto v$.

Случай 1. Пусть для преобразования $w_1 \mapsto v$ не применяется оператор $F(\cdot, h=1)$. Тогда из (14) необходимо удалить все, кроме одного, единичные разряды и получить $A(v) = 100\ldots0$. Такой вариант можно использовать в единственном случае, когда

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

Случай 2. Пусть для преобразования $w_1 \mapsto v$ применяется оператор $F(\cdot, h=1)$. Тогда $F(w_1, h=1) : (w_1) \mapsto (w)$ преобразует чётное значение (14) в нечётное (12), для которого $M(w \mapsto V) = \lfloor n - 2\sqrt{n} + 1\rfloor$. Тогда $M(w_1 \mapsto V) = M(w \mapsto V) + 1 = \lfloor n - 2\sqrt{n} + 2\rfloor$. Теорема 2 доказана.

ЛИТЕРАТУРА

1. **Арнольд В. И.** Топология и статистика формул арифметики // Успехи мат. наук. — 2003. — Т. 58, № 4. — с. 1–26.
2. **Мерекин Ю. В.** О вычислении сложности по Арнольду двоичных слов // Мат. XVI Междунар. конф. «Проблемы теоретической кибернетики» (Нижний Новгород, 20–25 июня 2011 г.). — Нижний Новгород: Изд-во Нижегородск. гос. ун-та, 2011. — С. 315–319.
3. **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.
4. **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.

5. **Merekin Yu. V.** Fast computation of the Arnold complexity of length 2^n binary words // ArXive e-print arXiv:1209.4700[mathCO], 2012.

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

Статья поступила
27 марта 2012 г.

Переработанный вариант —
23 августа 2012 г.