ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель—июнь 2002. Серия 1. Том 9, № 2, 36–47

УДК 519.714

ОЦЕНКИ МУЛЬТИПЛИКАТИВНОЙ СЛОЖНОСТИ ДВОИЧНЫХ СЛОВ, ОПРЕДЕЛЯЕМЫХ ПОЯСКОВЫМИ БУЛЕВЫМИ ФУНКЦИЯМИ*)

Ю. В. Мерекин

Для двоичных слов, определяемых поясковыми булевыми функциями, в классе схем конкатенации слов получена асимптотика для мультипликативной сложности, отличная от известной асимптотики для почти всех двоичных слов, определяемых симметрическими булевыми функциями. Получены также асимптотики для мультипликативной сложности слов, определяемых элементарными и монотонными симметрическими булевыми функциями.

В данной статье продолжаются исследования из [4–9] по оценке сложности процедуры построения слов в алфавите $\{0,1\}$, когда разрешается многократное использование уже построенных слов, подобно тому, как это делается в моделях синтеза схем из функциональных элементов при реализации булевых функций [3]. Предысторией рассматриваемой задачи можно считать задачу построения слов в однобуквенном алфавите [1, 12, 13].

В классе схем конкатенации слов (в англоязычной литературе эти схемы называют word chains [10, 11]) исследуется специальный класс слов, определяемых поясковыми булевыми функциями. Ранее получены результаты [6, 8], которые для почти всех слов, определяемых симметрическими булевыми функциями, дают асимптотическое совпадение нижних и верхних оценок сложности. Применение этих результатов к исследуемым в настоящей статье словам приводит либо к различию нижней и верхней оценок в константу раз (т. е. дает результат лишь с точностью до порядка величины), либо к более значительному расхождению оценок. Ниже для класса слов, определяемых поясковыми булевыми функциями, получена нижняя оценка сложности, которая асимптотически совпадает с верхней оценкой.

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 02–01–00939).

Длиной $|W|$ слова W называется число входящих в него символов. Операция *конкатенации* слов U и V определяется как запись слова V за словом U и обозначается через $U \bullet V$. В некоторых случаях знак $\bullet$ опускается. Слово V называется *подсловом* слова W и обозначается через $V \sqsubseteq W$, если для некоторых (возможно, пустых) слов X и Y справедливо равенство $W = X \bullet V \bullet Y$. При пустом X подслово V называется *префиксом*, а при пустом Y — *суффиксом* слова W.

Последовательность слов $0, 1, X, Y, \ldots, Z$ называется *схемой конкатенации* (см. также [2, 14]) слова Z и обозначается через S, если для любого слова W из этой последовательности, начиная со слова X, в S имеются такие слова U, V (возможно, $U = V$), предшествующие слову W, что $W = U \bullet V$. Под *сложностью* $L(S)$ схемы S конкатенации слова Z понимается число слов в последовательности $X, Y, \ldots, Z$. Пусть $L(Z) = \min L(S)$, где минимум берется по всевозможным схемам конкатенации слова Z. Величина $L(Z)$ называется *мультипликативной сложностью* слова Z.

При получении нижних оценок сложности используются специальные представления слов. Пусть слово W представлено в виде $W = UxV$, где $x \in \{0, 1\}$. Если V является либо символом, отсутствующим в слове Ux, либо $V \sqsubseteq Ux$ и $xV \not\sqsubseteq U$, $|V| \geqslant 2$, то слово V называется *максимальным суффиксом* слова W (однобуквенное слово по определению является своим максимальным суффиксом). Например, для слова 00001 максимальным суффиксом является 1; для слова 010110 суффикс 10 — максимальный. Представление слова Z в виде $Z = Y_1 \bullet Y_2 \bullet \ldots \bullet Y_r$ называется *суффиксным представлением* , если длина слова Y_1 равна единице, а каждое слово Y_i, $1 \leqslant i \leqslant r$, является максимальным суффиксом слова $Y_1 \bullet Y_2 \bullet \ldots \bullet Y_i$. Например, слово 00001 имеет суффиксное представление $0 \bullet 0 \bullet 00 \bullet 1$; слово 010110 имеет суффиксное представление $0 \bullet 1 \bullet 01 \bullet 10$. Очевидно, что суффиксное представление любого слова единственно. Число операций конкатенации в суффиксном представлении слова Z называется *суффиксной сложностью* слова Z и обозначается через $L^*(Z)$.

Пусть слово W представлено в виде $W = UV$, где $|V| > 1$. Если $V \not\sqsubseteq U$, то слово V называется *расширенным суффиксом* слова W (при пустом U слово V по определению является расширенным суффиксом). Например, для слова 00001 суффиксы 01, 001, 0001 и 00001 являются расширенными; для слова 010110 такими суффиксами являются 110, 0110, 10110 и 010110. Представление слова Z в виде $Z = Y_1 \bullet Y_2 \ldots \bullet Y_u$ называется *расширенным представлением*, если

(i) каждый суффикс $Y_1, Y_2, \ldots, Y_u$ является либо максимальным, либо расширенным;

(ii) среди $Y_1, Y_2, \ldots, Y_u$ содержится хотя бы один расширенный суффикс.

Например, для слова 00001 представления $00 \bullet 00 \bullet 1$ и $0 \bullet 000 \bullet 1$ являются расширенными; для слова 010110 такими представлениями являются $01 \bullet 01 \bullet 10$, $0 \bullet 1 \bullet 0 \bullet 110$ и $0 \bullet 10 \bullet 110$. Расширенное представление слова, вообще говоря, не единственно. Число операций конкатенации в i-м расширенном представлении (предполагается, что все такие представления как-то перенумерованы) назовем *сложностью i-го расширенного представления* и обозначим через $L_i^{**}(Z)$.

В [4, 7] доказано, что для произвольного слова Z при любом i выполняются неравенства

$$L(Z) \geqslant L^*(Z) \geqslant L_i^{**}(Z). \tag{1}$$

Булева функция называется *симметрической*, если она принимает одно и то же значение на всех наборах с одинаковым числом единиц. Каждая симметрическая булева функция $f(x_1, \ldots, x_n)$ может быть задана последовательностью $\widehat{\sigma} = \widehat{\sigma}(f) = (\sigma_0, \sigma_1, \ldots, \sigma_n)$, в которой σ_i есть значение функции $f(x_1, \ldots, x_n)$ на любом наборе значений переменных, содержащем i единиц и $n - i$ нулей. Последовательность $\widehat{\sigma} = (\sigma_0, \sigma_1, \ldots, \sigma_n)$ называется *характеристической* для $f(x_1, \ldots, x_n)$.

Ниже мы используем введенное в [6] отображение ξ последовательности $\widehat{\alpha}$ слов $(\alpha_0, \alpha_1, \ldots, \alpha_t)$, $t \geqslant 1$, в последовательность $\widehat{\beta}$ слов $(\beta_0, \beta_1, \ldots, \beta_{t-1})$, определяемое следующим образом: $\widehat{\beta} = \xi(\widehat{\alpha}) = (\alpha_0 \bullet \alpha_1,\ \alpha_1 \bullet \alpha_2, \ldots, \alpha_{t-1} \bullet \alpha_t)$. Если положить $\xi^0(\widehat{\alpha}) = \widehat{\alpha}$, $\xi^i(\widehat{\alpha}) = \xi(\xi^{i-1}(\widehat{\alpha}))$, $1 \leqslant i \leqslant t$, то последовательность $\xi^t(\widehat{\alpha})$ состоит из одного слова.

Если таблица истинности симметрической булевой функции $f(x_1, \ldots, x_n)$ с характеристической последовательностью $\widehat{\sigma} = (\sigma_0, \sigma_1, \ldots, \sigma_n)$ имеет лексикографический порядок наборов значений аргументов, то слово $\xi^n(\widehat{\sigma})$ совпадает со столбцом значений таблицы истинности (см. [6]).

Обозначим через $\widehat{\sigma}(k, l, m)$ последовательность $\widehat{\sigma}$, в которой первые k символов $\sigma_1, \ldots, \sigma_k$ равны нулю, последующие l символов $\sigma_{k+1}, \ldots, \sigma_{k+l}$ равны единице и остальные m символов $\sigma_{k+l+1}, \ldots, \sigma_{k+l+m}$ равны нулю. Всякая последовательность $\widehat{\sigma}(k, l, m)$ является по определению характеристической для некоторой *поясковой* симметрической булевой функции. Обозначим через $W_{k,l,m}$ слово-столбец значений таблицы истинности поясковой булевой функции с характеристической последовательностью $\widehat{\sigma}(k, l, m)$. Тогда $\xi^n(\widehat{\sigma}(k, l, m)) = W_{k,l,m}$.

Из построения слова $W_{k,l,m}$ следуют

Предложение 1. *При любых натуральных k и l слово $W_{k,l,0}$ представимо в виде*

$$W_{k,l,0} = W_{k,l-1,0} \bullet W_{k-1,l,0}.$$

Предложение 2. *При любых натуральных l и m слово $W_{0,l,m}$ представимо в виде*

$$W_{0,l,m} = W_{0,l,m-1} \bullet W_{0,l-1,m}.$$

Предложение 3. *При любых натуральных k, l и m слово $W_{k,l,m}$ представимо в виде*

$$W_{k,l,m} = W_{k,l,m-1} \bullet W_{k-1,l,m}.$$

Предложение 4. *При любых натуральных k, l и m в слове $W_{k,l,m}$ содержатся слова $W_{i,l,t}$, $W_{i,j,0}$, $W_{0,j,t}$, $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant l$, $1 \leqslant t \leqslant m$,*

$$W_{k,l,m} \sqsupseteq W_{i,l,t},\ W_{i,j,0},\ W_{0,j,t}.$$

Слова

$$W_{i,1,0} = \underbrace{0\ldots0}_{2^i-1}1, \quad i \geqslant 2,$$
$$W_{1,j,0} = 0\underbrace{1\ldots1}_{2^j-1}, \quad j \geqslant 2,$$
$$W_{0,j,1} = \underbrace{1\ldots1}_{2^j-1}0, \quad j \geqslant 2,$$
$$W_{0,1,t} = 1\underbrace{0\ldots0}_{2^t-1}, \quad t \geqslant 2,$$

назовем *элементарными словами*. Представление двоичного слова W в виде конкатенации элементарных слов назовем *элементарным представлением* слова W.

Лемма 1. *При любых натуральных k, l и m слова $W_{0,l,m}$, $W_{k,l,0}$ и $W_{k,l,m}$ имеют элементарные представления.*

Доказательство. Применим предложение 3 сначала к слову $W_{k,l,m}$, затем ко всем словам $W_{i,l,t}$ $(i,t \neq 0)$, полученным на очередном шаге разложения. В результате получаем представление слова $W_{k,l,m}$ в виде конкатенации слов

$$W_{i,l,0}, \quad W_{0,l,t}, \quad 1 \leqslant i \leqslant k, \quad 1 \leqslant t \leqslant m. \tag{2}$$

Продолжим разложение слов (2), применяя на каждом шаге разложения ко всем словам $W_{i,j,0}$, $i,j \geqslant 2$, предложение 1, а ко всем словам $W_{0,j,t}$, $j,t \geqslant 2$, — предложение 2. В результате получаем элементарное представление слова $W_{k,l,m}$. В процессе разложения слова $W_{k,l,m}$ объектами

разложения были слова (2), что доказывает существование элементарных представлений слов $W_{0,l,m}$ и $W_{k,l,0}$. Лемма 1 доказана.

Слова

$$W_{1,j,0} \bullet W_{i,1,0} = 0\underbrace{1\ldots1}_{2^j-1}\bullet\underbrace{0\ldots0}_{2^i-1}1, \quad i,j \geqslant 2,$$

$$W_{0,1,t} \bullet W_{0,j,1} = 1\underbrace{0\ldots0}_{2^t-1}\bullet\underbrace{1\ldots1}_{2^j-1}0, \quad j,t \geqslant 2,$$

$$W_{0,1,t} \bullet W_{i,1,0} \bullet W_{i-1,1,0} = 1\underbrace{0\ldots0}_{2^t-1}\bullet\underbrace{0\ldots0}_{2^i-1}1\bullet\underbrace{0\ldots0}_{2^{i-1}-1}1, \quad i \geqslant 3, \quad t \geqslant 2,$$

назовем *ядрами*. Ядра $W_{1,j,0}W_{i,1,0}$ и $W_{0,1,t}W_{0,j,1}$ имеют единственное элементарное представление. Для всякого ядра $W_{0,1,t}W_{i,1,0}W_{i-1,1,0}$ существует второе элементарное представление $W_{0,1,i}W_{t,1,0}W_{i-1,1,0}$.

Попарно сравнивая ядра, легко убедиться, что справедливо

Предложение 5. *Все ядра различны, не существует попарного перекрытия ядер по элементарному слову и вхождения ядер друг в друга.*

Покажем, что в любом элементарном представлении слова W ядро $W_{0,1,t}W_{i,1,0}W_{i-1,1,0}$ может иметь непустое пересечение только с тремя, а ядра $W_{1,j,0}W_{i,1,0}$ и $W_{0,1,t}W_{0,j,1}$ — только с двумя элементарными словами.

Лемма 2. *Пусть $W_1W_2\ldots W_u$, $u \geqslant 2$, — элементарное представление слова W, которое содержит ядро $W_{0,1,t}W_{i,1,0}W_{i-1,1,0}$, $i \geqslant 3$, $t \geqslant 2$. Если ядро имеет непустое пересечение со всеми элементарными словами $W_1, W_2, \ldots, W_u$, то*

$$W = W_{0,1,t}W_{i,1,0}W_{i-1,1,0}.$$

Доказательство. Рассмотрим три случая вхождения ядра

$$W_{0,1,t} \bullet W_{i,1,0} \bullet W_{i-1,1,0} = 1\underbrace{0\ldots0}_{2^t-1}\bullet\underbrace{0\ldots0}_{2^i-1}1\bullet\underbrace{0\ldots0}_{2^{i-1}-1}1 \tag{3}$$

в слово W из условий леммы.

Случай 1. Пусть $W = W_1W_2$. Предположим, что ядро (3) имеет непустое пересечение с двумя элементарными словами W_1, W_2. В этом случае внутри двоичного слова (3) необходимо разместить единственный символ $\bullet$, разделяющий элементарные слова W_1 и W_2. При любой позиции символа образуется либо подслово $10^{2^t-1}0^{2^i-1}1$, либо подслово $10^{2^i-1}1$, которое должно входить в элементарные слова W_1 и W_2 соответственно, что противоречит определению элементарного слова. Поэтому $W \not\supseteq W_{0,1,t}W_{i,1,0}W_{i-1,1,0}$.

Случай 2. Пусть $W = W_1W_2W_3$ и ядро (3) имеет непустое пересечение с тремя элементарными словами W_1, W_2, W_3. В этом случае внутри

двоичного слова (3) необходимо разместить два символа •, разделяющих элементарные слова W_1 W_2 и W_3. Возможны два варианта размещения символов:

$$1\ \underbrace{0\ldots0}_{2^t+2^i-2^r-1}\bullet\underbrace{0\ldots0}_{2^r-1}1\bullet\underbrace{0\ldots0}_{2^{i-1}-1}1, \quad \text{где } W_2=0^{2^r-1}1,\ r\geqslant 2;$$

$$1\ \underbrace{0\ldots0}_{2^t+2^i-2}\bullet1\underbrace{0\ldots0}_{2^s-1}\bullet\underbrace{0\ldots0}_{2^{i-1}-2^s}1, \quad \text{где } W_2=10^{2^s-1},\ s\geqslant 2.$$

Рассмотрим первый вариант. Если $t=r$ (или $r=i$), то возникает равенство

$$W=W_{0,1,t}W_{i,1,0}W_{i-1,1,0}$$

из леммы. Если $t\neq r\neq i$, то слово $10^{2^t+2^i-2^r-1}$ не является элементарным и не может быть суффиксом элементарного слова W_1. Поэтому при $t\neq r\neq i$ имеем $W\not\equiv W_{0,1,t}W_{i,1,0}W_{i-1,1,0}$.

Рассмотрим второй вариант. При любых $i,t\geqslant 2$ слово $10^{2^t+2^i-2}$ не является элементарным и не может быть суффиксом элементарного слова W_1. Поэтому $W\not\equiv W_{0,1,t}W_{i,1,0}W_{i-1,1,0}$.

Случай 3. Пусть $W=W_1W_2\ldots W_u, u\geqslant 4$. Предположим, что ядро (3) имеет непустое пересечение с u элементарными словами $W_1, W_2, \ldots, W_u$. В этом случае внутри двоичного слова (3) необходимо разместить не менее трех символов •, разделяющих элементарные слова $W_1, W_2, \ldots, W_u$. Очевидно, что не менее двух символов должны разместиться либо внутри слова $10^{2^t-1}0^{2^i-1}1$, либо внутри слова $10^{2^{i-1}-1}1$. В обоих вариантах эти символы выделяют серию нулей, которая не является элементарным словом. Поэтому $W\not\equiv W_{0,1,t}W_{i,1,0}W_{i-1,1,0}$. Лемма 2 доказана.

Аналогично доказываются

Лемма 3. *Пусть $W_1W_2\ldots W_u, u\geqslant 2$, — элементарное представление слова W, которое содержит ядро $W_{1,j,0}W_{i,1,0}$, $i,j\geqslant 2$. Если ядро имеет непустое пересечение со всеми элементарными словами $W_1, W_2, \ldots, W_u$, то*

$$W=W_{1,j,0}W_{i,1,0}.$$

Лемма 4. *Пусть $W_1W_2\ldots W_u, u\geqslant 2$, — элементарное представление слова W, которое содержит ядро $W_{0,1,t}W_{0,j,1}$, $j,t\geqslant 2$. Если ядро имеет непустое пересечение со всеми элементарными словами $W_1, W_2, \ldots, W_u$, то*

$$W=W_{0,1,t}W_{0,j,1}.$$

Рассмотрим некоторые специальные представления слов $W_{k,l,m}$.

Лемма 5. *При любых $k \geqslant 2$, $l \geqslant 1$ и $m \geqslant 2$ слово $W_{k,l,m}$ представимо в виде*

$$W_{k,l,m} = W_{k,1,0}W_{k-1,1,0} \bullet X_{k,l,m} \bullet W_{0,1,m}.$$

Доказательство. Применим предложение 3 сначала к слову $W_{k,l,m}$, затем к каждому префиксу $W_{k,l,m-1}, W_{k,l,m-2}, \ldots, W_{k,l,1}$ из очередного полученного разложения

$$\begin{aligned} W_{k,l,m} = W_{k,l,m-1}W_{k-1,l,m} = \ldots &= W_{k,l,1}(W_{k-1,l,2}\ldots W_{k-1,l,m}) \\ &= W_{k,l,0}W_{k-1,l,1}(W_{k-1,l,2}\ldots W_{k-1,l,m}). \end{aligned}$$

Если $l = 1$, то разложим слово $W_{k-1,1,1}$ и, прекратив разложение префиксов, приступим к разложению суффиксов. Если $l \geqslant 2$, то продолжим разложение, применяя предложение 1 к каждому префиксу $W_{k,l,0}, W_{k,l-1,0}$, $\ldots, W_{k,2,0}$, а затем к слову $W_{k-1,2,0}$. В результате получаем

$$\begin{aligned} W_{k,l,0} = W_{k,l-1,0}W_{k-1,l,0} = \ldots &= W_{k,1,0}W_{k-1,2,0}(W_{k-1,3,0}\ldots W_{k-1,l,0}) \\ &= W_{k,1,0}W_{k-1,1,0}W_{k-2,2,0}(W_{k-1,3,0}\ldots W_{k-1,l,0}), \end{aligned}$$

где префикс $W_{k,1,0}W_{k-1,1,0}$ соответствует утверждению леммы.

Продолжим разложение, применяя предложение 3 сначала к суффиксу $W_{k-1,l,m}$, затем к каждому суффиксу $W_{k-2,l,m}, W_{k-3,l,m}, \ldots, W_{1,l,m}$ из очередного полученного разложения

$$\begin{aligned} W_{k-1,l,m} = W_{k-1,l,m-1}W_{k-2,l,m} = \ldots &= (W_{k-1,l,m-1}\ldots W_{2,l,m-1})W_{1,l,m} \\ &= (W_{k-1,l,m-1}\ldots W_{2,l,m-1})W_{1,l,m-1}W_{0,l,m}. \end{aligned}$$

Если $l = 1$, то разложение прекращается. Если $l \geqslant 2$, то, продолжая разложение, применим предложение 2 к каждому суффиксу $W_{0,l,m}, W_{0,l-1,m}$, $\ldots, W_{0,2,m}$. В результате получим

$$W_{0,l,m} = W_{0,l,m-1}W_{0,l-1,m} = \ldots = (W_{0,l,m-1}\ldots W_{0,2,m-1})W_{0,1,m},$$

где суффикс $W_{0,1,m}$ удовлетворяет утверждению леммы.

Из проведенного разложения следует, что при любых $k \geqslant 2$, $l \geqslant 1$ и $m \geqslant 2$ префикс $W_{k,1,0}W_{k-1,1,0}$ и суффикс $W_{0,1,m}$ слова $W_{k,l,m}$ не перекрываются. Лемма 5 доказана.

При доказательстве леммы 5 в процессе разложения слова $W_{k,l,m}$ на разных этапах объектами разложения были подслова $W_{k,l,0}$, $W_{k,l,1}$, $W_{0,l,m}$ и $W_{1,l,m}$. Рассматривая их в качестве начального объекта разложения, приведем без доказательства два следствия из леммы 5.

Следствие 1. *При любых $k \geqslant 2$ и $l \geqslant 2$ слова $W_{k,l,0}$ и $W_{k,l,1}$ представимы в виде*

$$W_{k,l,0} = W_{k,1,0} \bullet X_{k,l,0} \bullet W_{1,l,0}, \quad W_{k,l,1} = W_{k,1,0} \bullet Y_{k,l,1}.$$

Следствие 2. *При любых $l \geqslant 2$ и $m \geqslant 2$ слова $W_{0,l,m}$ и $W_{1,l,m}$ представимы в виде*

$$W_{0,l,m} = W_{0,l,1} \bullet X_{0,l,m} \bullet W_{0,1,m}, \quad W_{1,l,m} = Y_{1,l,m} \bullet W_{0,1,m}.$$

Рассмотрим вхождение ядер в слово $W_{k,l,m}$.

Лемма 6. *При любых $k \geqslant 4$, $l \geqslant 2$ и $m \geqslant 3$ в слово $W_{k,l,m}$ входят $(k-3)(m-2)+(k-2)(l-1)+(l-1)(m-2)$ различных ядер*

$$W_{0,1,t-1}W_{i-1,1,0}W_{i-2,1,0},\ W_{1,j,0}W_{i-1,1,0} \text{ и } W_{0,1,t-1}W_{0,j,1},$$
$$4 \leqslant i \leqslant k,\ 2 \leqslant j \leqslant l,\ 3 \leqslant t \leqslant m.$$

Доказательство. В некоторых словах, входящих в слово $W_{k,l,m}$, выделим по одному ядру и найдем число различных выделенных ядер. Используя предложение 4, образуем пять типов слов, входящих в $W_{k,l,m}$:

$$W_{k,l,m} \sqsupseteq W_{i,l,t},\ W_{i,j,0},\ W_{i,l,1},\ W_{0,j,t},\ W_{1,l,t},$$
$$2 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant l,\ 2 \leqslant t \leqslant m.$$

I. Разложив слово $W_{i,l,t}$ сначала по предложению 3, а затем продолжив разложение слов $W_{i,l,t-1}$ и $W_{i-1,l,t}$ по лемме 5, получаем представление

$$\begin{aligned} W_{i,l,t} &= W_{i,l,t-1} \bullet W_{i-1,l,t} \\ &= W_{i,1,0}W_{i-1,1,0}X_{i,l,t-1}W_{0,1,t-1} \bullet W_{i-1,1,0}W_{i-2,1,0}X_{i-1,l,t}W_{0,1,t}, \end{aligned}$$

в которое при любом заданном натуральном l и любых $i \geqslant 4$, $t \geqslant 3$ входит ядро $W_{0,1,t-1}W_{i-1,1,0}W_{i-2,1,0}$. Поэтому

$$W_{k,l,m} \sqsupseteq W_{i,l,t} \sqsupseteq W_{0,1,t-1}W_{i-1,1,0}W_{i-2,1,0}, \quad 4 \leqslant i \leqslant k, \quad 3 \leqslant t \leqslant m. \qquad (4)$$

Согласно предложению 5 все ядра из (4) различны. Следовательно, в слове $W_{k,l,m}$ содержится $(k-3)(m-2)$ различных ядер $W_{0,1,t-1}W_{i-1,1,0}$ $W_{i-2,1,0}$, $4 \leqslant i \leqslant k$, $3 \leqslant t \leqslant m$.

II. Разложив слово $W_{i,j,0}$ сначала по предложению 1, а затем продолжив разложение слов $W_{i,j-1,0}$ и $W_{i-1,j,0}$ по следствию 1, получаем представление

$$W_{i,j,0} = W_{i,j-1,0} \bullet W_{i-1,j,0} = W_{i,1,0}X_{i,j-1,0}W_{1,j-1,0} \bullet W_{i-1,1,0}X_{i-1,j,0}W_{1,j,0},$$

в которое при любых $i \geqslant 3$, $j \geqslant 3$ входит ядро $W_{1,j-1,0}W_{i-1,1,0}$. Поэтому

$$W_{k,l,m} \sqsupseteq W_{i,j,0} \sqsupseteq W_{1,j-1,0}W_{i-1,1,0}, \quad 3 \leqslant i \leqslant k, \quad 3 \leqslant j \leqslant l. \qquad (5)$$

Согласно предложению 5 все ядра из (5) различны. Следовательно, в слове $W_{k,l,m}$ имеется $(k-2)(l-2)$ различных ядер $W_{1,j-1,0}W_{i-1,1,0}$, $3 \leqslant i \leqslant k$, $3 \leqslant j \leqslant l$.

III. Разложив слово $W_{i,l,1}$ сначала по предложению 3, а затем продолжив разложение слов $W_{i,l,0}$ и $W_{i-1,l,1}$ по следствию 1, получаем представление

$$W_{i,l,1} = W_{i,l,0} \bullet W_{i-1,l,1} = W_{i,1,0}X_{i,l,0}W_{1,l,0} \bullet W_{i-1,1,0}Y_{i-1,l,1},$$

в которое при любом заданном $l \geqslant 2$ и при любом $i \geqslant 3$ содержится ядро $W_{1,l,0}W_{i-1,1,0}$. Поэтому

$$W_{k,l,m} \sqsupseteq W_{i,l,1} \sqsupseteq W_{1,l,0}W_{i-1,1,0}, \quad 3 \leqslant i \leqslant k. \tag{6}$$

Согласно предложению 5 все ядра из (6) различны. Следовательно, в слове $W_{k,l,m}$ имеется $k-2$ различных ядер $W_{1,l,0}W_{i-1,1,0}$, $3 \leqslant i \leqslant k$.

Объединяя (5) и (6), получаем

$$W_{k,l,m} \sqsupseteq W_{1,j,0}W_{i-1,1,0}, \quad 3 \leqslant i \leqslant k, \ 2 \leqslant j \leqslant l. \tag{7}$$

Следовательно, в слове $W_{k,l,m}$ имеется $(k-2)(l-1)$ различных ядер $W_{1,j,0}W_{i-1,1,0}$, $3 \leqslant i \leqslant k$, $2 \leqslant j \leqslant l$.

IV. Аналогично для слов $W_{0,j,t}$ и $W_{1,j,t}$ получаем

$$W_{k,l,m} \sqsupseteq W_{0,1,t-1}W_{0,j,1}, \quad 2 \leqslant j \leqslant l, \quad 3 \leqslant t \leqslant m. \tag{8}$$

Следовательно, в слове $W_{k,l,m}$ имеется $(l-1)(m-2)$ различных ядер $W_{0,1,t-1}W_{0,j,1}$, $2 \leqslant j \leqslant l$, $3 \leqslant t \leqslant m$.

Объединяя (4), (7) и (8), получаем

$$W_{k,l,m} \sqsupseteq W_{0,1,t-1}W_{i-1,1,0}W_{i-2,1,0}, \quad W_{1,j,0}W_{i-1,1,0}, \quad W_{0,1,t-1}W_{0,j,1},$$
$$4 \leqslant i \leqslant k, \quad 2 \leqslant j \leqslant l, \quad 3 \leqslant t \leqslant m,$$

где число различных ядер равно $(k-3)(m-2)+(k-2)(l-1)+(l-1)(m-2)$. Лемма 6 доказана.

Наличие различных ядер в слове $W_{k,l,m}$ позволяет построить его расширенное суффиксное представление и, используя неравенство (1), получить нижнюю оценку сложности $L(W_{k,l,m})$.

Теорема 1. *При любых $k \geqslant 4$, $l \geqslant 2$ и $m \geqslant 3$ справедливо неравенство*

$$L(W_{k,l,m}) \geqslant kl + lm + km + 10 - (3k + 4l + 4m). \tag{9}$$

Доказательство. По лемме 6 в слове $W_{k,l,m}$ имеется $(k-3)(m-2)+(k-2)(l-1)+(l-1)(m-2)$ различных ядер. Покажем, что любые два ядра, входящие в слово $W_{k,l,m}$, не перекрываются.

Зададим слово $W_{k,l,m}$ в виде элементарного представления (см. лемму 1). Каждое ядро $W_{0,1,t-1}W_{i-1,1,0}W_{i-2,1,0}$, содержащееся в слове $W_{k,l,m}$, совпадает с тремя (см. лемму 2), а каждое ядро $W_{1,j,0}W_{i-1,1,0}$, $W_{0,1,t-1}W_{0,j,1}$ — с двумя (см. леммы 3 и 4) элементарными словами. По

предложению 5 не существует попарного перекрытия ядер по элементарному слову и вхождения ядер друг в друга. Следовательно, все имеющиеся в $W_{k,l,m}$ ядра не перекрываются.

Просматривая слово $W_{k,l,m}$ слева направо, находим первое встретившееся ядро и ставим перед ним символ $\bullet$. Продолжая просмотр, находим очередное ядро, отличное от всех найденных ранее, и ставим перед ним символ $\bullet$. Процесс продолжается до выявления всех $(k-3)(l-2)+(k-2)(l-1)+(l-1)(m-2)$ различных ядер, входящих в слово $W_{k,l,m}$. Проставленные символы выделяют расширенные суффиксы. Поэтому $L^{**}(W_{k,l,m}) = kl+lm+km+10-(3k+4l+4m)$. Отсюда и из (1) следует, что $L(W_{k,l,m}) \geqslant kl+lm+km+10-(3k+4l+4m)$. Теорема 1 доказана.

Замечание 1. В [9] при получении оценки

$$L(W_{k,l,m}) \geqslant kl+lm+km+5-(2k+4l+2m)$$

в качестве ядер использовались слова $W_{0,1,t}W_{2,1,0}W_{1,1,0}$, которые при любом t не имеют элементарного представления. В настоящей статье, лишив слова $W_{0,1,t}W_{2,1,0}W_{1,1,0}$ статуса ядер, мы несколько ослабили нижнюю оценку, но упростили доказательства.

В [6] получена верхняя оценка сложности

$$L(W_{k,l,m}) \leqslant \begin{cases} kl+lm+km+(k+l)-2 & \text{при } k \geqslant m, \\ kl+lm+km+(l+m)-2 & \text{при } m > k. \end{cases} \tag{10}$$

Из оценок (9) и (10) получаем

Следствие 3. *При k, l, $m \to \infty$*

$$L(W_{k,l,m}) = (kl+lm+km)(1+o(1)).$$

В качестве дополнительного результата получаем асимптотики для мультипликативной сложности слов $W_{k,1,m}$ и $W_{k,l,0}$, которые определяются соответственно элементарными и монотонными булевыми функциями.

Следствие 4. *При k, $m \to \infty$*

$$L(W_{k,1,m}) = km(1+o(1)).$$

Доказательство. Нижняя оценка. При $k \geqslant 4$, $l=1$ и $m \geqslant 3$ согласно (4) в слове $W_{k,1,m}$ имеется $(k-3)(m-2)$ различных ядер. Выделяя различные ядра, как это делалось в доказательстве теоремы 1, построим расширенное суффиксное представление слова $W_{k,1,m}$. В результате получаем $L^{**}(W_{k,1,m}) = km+6-(2k+3m)$. Отсюда и из (1) следует, что при любых $k \geqslant 4$ и $m \geqslant 3$ справедливо неравенство

$$L(W_{k,1,m}) \geqslant km+6-(2k+3m). \tag{11}$$

Верхняя оценка

$$L(W_{k,1,m}) \leqslant \begin{cases} km + 2k + m - 1 & \text{при } k \geqslant m, \\ km + k + 2m - 1 & \text{при } m > k \end{cases} \tag{12}$$

получена в [6].

Из оценок (11) и (12) следует утверждение следствия 4.

Следствие 5. *При* $k, l \to \infty$

$$L(W_{k,l,0}) = kl(1 + o(1)).$$

Доказательство. Нижняя оценка. При $k \geqslant 3$ и $l \geqslant 3$ согласно (5) в слове $W_{k,l,0}$ имеется $(k-2)(l-2)$ различных ядер. Выделяя различные ядра, как это делалось в доказательстве теоремы 1, построим расширенное суффиксное представление слова $W_{k,l,0}$. В результате получаем $L^{**}(W_{k,l,0}) = kl + 4 - (2k + 2l)$. Отсюда и из (1) следует, что при любых $k \geqslant 3$ и $l \geqslant 3$ справедливо неравенство

$$L(W_{k,l,0}) \geqslant kl + 4 - (2k + 2l). \tag{13}$$

Верхняя оценка

$$L(W_{k,l,0}) \leqslant kl + k + l - 2 \tag{14}$$

получена в [6].

Из оценок (13) и (14) следует утверждение следствия 5.

Замечание 2. В [7] при специальном рассмотрении слов $W_{k,1,m}$ и $W_{k,l,0}$ получены нижние оценки

$$L(W_{k,1,m}) \geqslant km + k \quad \text{и} \quad L(W_{k,l,0}) \geqslant kl + 2,$$

которые несколько превосходят оценки (11) и (13).

ЛИТЕРАТУРА

1. **Гашков С. Б., Кочергин В. В.** Об аддитивных цепочках векторов, вентильных схемах и сложности вычислений степеней // Методы дискретного анализа в теории графов и сложности: Сб. науч. тр. Вып. 52. Новосибирск: Ин-т математики СО РАН, 1992. С. 22–40.
2. **Кочергин В. В.** О мультипликативной сложности двоичных слов с заданным числом единиц // Математические вопросы кибернетики. Вып. 8. М.: Наука; Физматлит, 1999. С. 63–76.
3. **Лупанов О. Б.** Асимптотические оценки сложности управляющих систем. М.: Изд-во Моск. ун-та, 1984.
4. **Мерекин Ю. В.** Нижняя оценка сложности для схем конкатенации слов // Дискрет. анализ и исслед. операций. 1996. Т. 3, № 1. С. 52–56.

5. **Мерекин Ю. В.** О сложности символьных последовательностей, определяемых линейными булевыми функциями // Сиб. журн. индустриальной математики. 1998. Т. 1, № 1. С. 145–147.
6. **Мерекин Ю. В.** Верхние оценки сложности символьных последовательностей, порождаемых симметрическими булевыми функциями // Дискрет. анализ и исслед. операций. Сер. 1. 1998. Т. 5, № 3. С. 38–43. Англ. пер.: *Merekin Yu. V.* Upper bounds for the complexity of sequences generated by symmetric Boolean functions // Discrete Applied Math. 2001. V. 114, N 1–3. P. 227–231.
7. **Мерекин Ю. В.** Нижние оценки мультипликативной сложности символьных последовательностей, определяемых монотонными симметрическими булевыми функциями // Дискрет. анализ и исслед. операций. Сер. 1. 1999. Т. 6, № 3. С. 3–9.
8. **Мерекин Ю. В.** Нижние оценки сложности символьных последовательностей, определяемых симметрическими булевыми функциями // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7, № 2. С. 54–64.
9. **Мерекин Ю. В.** Нижние оценки сложности символьных последовательностей, определяемых поясковыми булевыми функциями // Материалы XII Междунар. школы-семинара «Синтез и сложность управляющих систем». (Пенза, 15–21 октября 2001 г.). М.: Изд-во центра прикл. исслед. при мех.-мат. фак. МГУ, 2001. С. 151–154.
10. **Arnold A., Brlek S.** Optimal word chains for the Thue — Morse word // Inform. and Comput. 1989. V. 83, N 2. P. 140–151.
11. **Bousquet-Mélou M.** The number of minimal word chains computing the Thue — Morse word // Inform. Process. Lett. 1992. V. 44, N 2. P. 57–64.
12. **Brauer A.** On addition chains // Bull. Amer. Math. Soc. 1939. V. 45, N 10. P. 736–739.
13. **Erdős P.** Remarks on number theory. III. On addition chains // Acta Arithmetica. 1960. V. 6, N 1. P. 77–81.
14. **Red'kin N. P.** Complexity of concatenation schemes for words from some classes // Proc. of two joint French-Russian seminars on combinatorial and algorithmical properties of discrete structures. M.: MSU, 2001. P. 107–114.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск, Россия.
E-mail: merekin@math.nsc.ru

Статья поступила
11 февраля 2002 г.