G. S. Tseitin, A reduced form of normal algorithms and a linear speed-up theorem, *Zap. Nauchn. Sem. LOMI*, 1971, Volume 20, 234–242

Г.С.Цейтин

ПРИВЕДЕННАЯ ФОРМА НОРМАЛЬНЫХ АЛГОРИФМОВ И ТЕОРЕМА О ЛИНЕЙНОМ УСКОРЕНИИ

Пусть дан нормальный алгорифм в алфавите А. Подалфавит Б этого алфавита будем называть оперативным алфавитом данного нормального алгорифма, если его схема удовлетворяет следующим условиям:

I) левая часть любой формулы подстановки, кроме последней, содержит единственное вхождение буквы из Б,

2) правая часть любой незаключительной формулы подстановки содержит единственное вхождение буквы из Б,

3) левая часть последней формулы подстановки - пустое слово

4) для каждой буквы из Б в схеме найдется формула, левая часть которой есть однобуквенное слово из этой буквы.

Очевидно, что, если мы применим этот алгорифм к слову, не содержащему букв из Б, то в получающейся цепочке слов каждое слово, кроме первого и, возможно, последнего, будет содержать единственное вхождение буквы из Б и каждый шаг, кроме первого, будет состоять в изменении некоторой "окрестности" этого вхождения. Работа такого алгорифма аналогична работе машины Тьюринга с той разницей, что здесь некоторым шагам будет соответствовать вставка или выбрасывание клеток в середине ленты, а также, что здесь операция может производиться одновременно над несколькими соседними клетками. Можно также считать, что левое и правое крылья вхождения буквы из Б записаны на отдельных лентах, содержимое каждой из которых будет меняться в режиме магазина; таким способом нетрудно построить автомат с двумя магазинами, моделирующий работу данного нормального алгорифма таким образом, что каждому шагу нормального алгорифма соответствует ограниченное число шагов этого автомата.

Далее используются термины и обозначения из [I] .

Через $t_{\mathfrak{A}}(P)$ будем обозначать число шагов, за которое алгорифм $\mathfrak{A}$ заканчивает работу над словом P (это выражение определено в том и только том случае, если $\mathfrak{A}$ примени́м к P). Через $|P|$ будем обозначать длину слова P .

Теорема I. По любому нормальному алгорифму $\mathfrak{M}$ в алфавите М можно построить алгорифм $\mathfrak{N}$ в расширении этого алфавита, вполне эквивалентный алгорифму $\mathfrak{M}$ относительно М и такой, что

1) $\mathfrak{N}$ имеет оперативный алфавит, не содержащий букв из М,

2) существуют такие натуральные числа c_1, c_2 и c_3, что для любого слова P, к которому приме́ним алгорифм $\mathfrak{M}$, будет

$$t_{\mathfrak{N}}(P) \leq c_1 \cdot t_{\mathfrak{M}}(P) + c_2 \cdot |P| + c_3$$

Эта теорема, так же как теорема 2 ниже, была доказана автором в 1954 г. и докладывалась на 3-м Всесоюзном математическом съезде в 1956 г. (см. также [2] стр. 44); однако автору не удавалось найти удобной формы для письменного изложения употребленной здесь конструкции. Интересно отметить, что этот результат существенно опирается на некоторые частные особенности определения нормального алгорифма и утрачивает силу, если вместо понятия нормального алгорифма рассматривать его небольшую модификацию - понятие алгорифма типа σ [3] . Контрпримером может служить алгорифм типа σ , переворачивающий любое слово в некотором алфавите за число шагов, являющееся линейной функцией длины этого слова (такой алгорифм типа σ нетрудно построить, кодируя переносимую букву номером схемы); как следует из доказательства в [4] , любой эквивалентный ему алгорифм типа σ с оперативным алфавитом имел бы квадратичный порядок роста числа шагов.

Доказательство. Не умаляя общности, будем считать, что последняя формула в схеме алгорифма $\mathfrak{M}$ имеет пустую левую часть, а в остальных формулах левые части непустые [I: Ш. § 2]. Число формул в схеме обозначим буквой m. Далее в этом доказательстве буквы ξ и η будут служить переменными для букв алфавита М, а i и j – для натуральных чисел от I до m включительно.

Для каждой буквы ξ введем $(m-1)$ новых букв, которые будем обозначать $\xi^{(2)}, \ldots, \xi^{(m)}$; положим также $\xi^{(1)} = \xi$. Алфавит, состоящий из всех букв вида $\xi^{(i)}$, обозначим буквой Н. Буквы X и Y будут служить далее переменными для слов в этом алфавите. Введем также пятибуквенный алфавит $\Pi = \{\alpha, \beta^-, \beta^+, \gamma, \delta\}$, не имеющий общих букв с $\mathfrak{N}$. Искомый алгорифм $\mathfrak{N}$ мы будем строить в алфавите Н$\cup$П, причем П будет служить оперативным алфавитом. Если R – слово в Н$\cup$П, то через $\bar{R}$ будем обозначать слово, получаемое из R заменой всех вхождений букв $\xi^{(i)}$ $(i>1)$ на ξ и выбрасыванием всех вхождений букв из П. Обозначим левую часть i-й формулы в схеме $\mathfrak{M}$ через A_i, а правую часть – через B_i; полагаем $\varphi_i = \alpha$, если i-я формула – обычная, и $\varphi_i = \gamma$, если i-я формула – заключительная.

Определим некоторые системы формул подстановок следующими сокращенно записанными схемами. Через $\mathfrak{A}_i$ обозначим систему формул

$$\xi^{(i)}\alpha \to \xi^{(i)}\beta^- \tag{I}$$

$$X\alpha Y \to \varphi_i B_i \quad (\bar{X}\bar{Y} = A_i) \tag{2}$$

$$\alpha\xi^{(i)} \to \beta^+\xi^{(i)}, \tag{3}$$

где формулы, получаемые из строки (2), расположены по убыванию $|X|$ (в остальном порядок формул произволен). Через $\mathfrak{L}_i^-$ при $i<m$ обозначим систему

$$\xi^{(j)}\beta^- X \to \alpha\xi^{(i)}X \quad (\xi\bar{X} = A_i, \ j \le i) \tag{4}$$

$$\xi^{(j)}\beta^-\eta^{(i)} \to \alpha\xi^{(i)}\eta^{(i)} \quad (j \le i), \tag{5}$$

а при $i=m$ – систему

$$\xi^{(j)}\beta^{-} \rightarrow \alpha\,\xi^{(m)}. \tag{6}$$

Аналогично, $\mathcal{L}_i^{+}$ будет при $i<m$ обозначать систему

$$X\beta^{+}\xi^{(j)} \rightarrow X\,\xi^{(i)}\alpha \quad (\bar{X}\xi = A_i\,,\ j<i) \tag{7}$$

$$\eta^{(i)}\beta^{+}\xi^{(j)} \rightarrow \eta^{(i)}\xi^{(i)}\alpha \qquad (j<i), \tag{8}$$

а при $i=m$ – систему

$$\beta^{+}\xi^{(j)} \rightarrow \xi^{(m)}\alpha \qquad (j<m) \tag{9}$$

Схема алгорифма $\mathfrak{N}$ будет состоять из всех систем формул $\mathfrak{A}_i$, $\mathcal{L}_i^{-}$ и $\mathcal{L}_i^{+}$, расположенных в порядке возрастания i (в остальном их порядок безразличен), к которым в конце приписана следующая система формул:

$$\beta^{-} \rightarrow\cdot \tag{10}$$

$$\beta^{+} \rightarrow\cdot \tag{11}$$

$$\xi^{(i)}\gamma \rightarrow \gamma\,\xi \tag{12}$$

$$\gamma \rightarrow \delta \tag{13}$$

$$\delta\,\xi^{(i)} \rightarrow \xi\,\delta \tag{14}$$

$$\delta \rightarrow\cdot \tag{15}$$

$$\rightarrow \alpha \tag{16}$$

Легко видеть, что П действительно является оперативным алфавитом для $\mathfrak{N}$ (формула с левой частью α получается из (2) при $i=m$).

Будем называть слово R в алфавите $H\cup\{\alpha, \beta^{-}, \beta^{+}\}$ п р а в и л ь н ы м , если выполнены следующие условия:

1) R содержит единственное вхождение букв $\alpha, \beta^{-}, \beta^{+}$,

2) если R начинается словом вида $X\xi^{(i)}$, то при $j<i$ слово $\bar{X}\xi$ не содержит вхождений A_j .

3) если R кончается словом вида $\xi^{(i)}X$, то при $j<i$ слово $\xi\bar{X}$ не содержит вхождений A_j .

Пусть P – слово в М. Тогда, по (16), $\mathfrak{N}: P \vdash \alpha P$, и слово αP – правильное.

Лемма I. Если $\mathfrak{N}: \alpha P \models R$ и в R не входят буквы γ и δ, то слово R – правильное.

Лемма доказывается индукцией по числу шагов. Особо нужно рассмотреть случай применения формул (4) – (9). Предположим, например, что в результате применения формулы из $\mathcal{L}_i^+$ слово $S\beta^+\xi^{(j)}T$ $(j < i)$ перешло в $S\xi^{(i)}\alpha T$ и $\bar{S}\xi$ содержит вхождение A_k, причем $k < i$. При $j < k$ это невозможно, так как вместо данной формулы применилась бы формула из $\mathcal{L}_k^+$. В случае же $k \leq j$ заметим, что предыдущим шагом могло быть только применение формулы (3) из $\mathfrak{A}_j$ к слову $S\alpha\xi^{(j)}T$; однако при нашем предположении вместо нее к слову должна применяться одна из формул (I) и (2) из $\mathfrak{A}_k$. Аналогично рассматривается случай $\mathcal{L}_i^-$.

Припишем вхождениям букв в слово веса следующим образом: вхождению буквы $\xi^{(i)}$ припишем вес $4(m-i+1)+2$, если это вхождение предшествует вхождению буквы из П, и вес $4(m-i+1)$ в противном случае, вхождению буквы α – вес I, а остальным вхождениям букв – вес 0. Весом слова будем называть сумму весов всех вхождений букв в него; вес слова R будем обозначать $w(R)$. Обозначим через ℓ максимум $|B_i|$ по всем i.

Лемма 2. Если R – правильное слово и $\mathfrak{N}: R \vdash S$, то имеет место одна из трех возможностей:

1) $\bar{R} = \bar{S}$ и $w(S) \leq w(R) - 1$,

2) $\mathfrak{M}: \bar{R} \vdash S$ и $w(S) \leq w(R) + 4\ell m$,

3) $\mathfrak{M}: \bar{R} \vdash\cdot \bar{S}$, $w(S) \leq w(R) + 4\ell m$ и в S входит γ.

Лемма доказывается путем непосредственного просмотра схемы $\mathfrak{N}$. (Заметим для пояснения, что последовательным попыткам применить к R формулы (I), (2) и (3) из $\mathfrak{A}_i$ соответствует поиск вхождения A_i в $\bar{R}$ вначале слева от места, указанного в R

буквой α, потом "около" этого места и, наконец, справа от него.

Лемма 3. Пусть $\mathfrak{N}: P \models_n S$ и в S не входит γ. Тогда существует такое k, что $\mathfrak{M}: P \models_k \bar{S}$ и

$$w(S) \leqslant 4m \cdot |P| + (4\ell m + 1)k - n + 2. \qquad (17)$$

Лемма доказывается индукцией по n на основании лемм I и 2.

Лемма 4. Пусть n - наименьшее число шагов, за которое $\mathfrak{N}$ преобразует P в слово S, содержащее вхождение γ. Тогда существует такое k, что $\mathfrak{M}: P \models_k \cdot S$ и выполняется (17).

Пусть теперь алгорифм $\mathfrak{N}$ применим к P. Работа алгорифма не могла закончиться применением формул (10) и (11). Пусть, действительно, применилась формула (11). Тогда на предыдущем шаге могло быть только применение формулы (3) из $\mathfrak{A}_i$. При этом формула (3) из $\mathfrak{A}_m$ не может применяться, так как ей предшествует формула с левой частью α, следовательно, $i < m$. Таким образом, в получившееся слово входит $\beta^+ \xi^{(i)}$, где $i < m$, и, следовательно, должна применяться формула (9), а не (11). Аналогично рассуждаем для формулы (10). Следовательно, работа $\mathfrak{N}$ кончилась применением формулы (15), откуда следует, что на некотором шаге применения $\mathfrak{N}$ к P получилось слово, содержащее вхождение буквы γ (вхождение δ могло возникнуть только из γ). Рассмотрев шаг, где впервые получилось слово с буквой γ, получим по лемме 4, что алгорифм $\mathfrak{M}$ тоже применим к P.

Пусть теперь дано, что алгорифм $\mathfrak{M}$ применим к P. Тогда соотношение $\mathfrak{M}: P \models_k Q$ возможно лишь при $k < t_{\mathfrak{M}}(P)$. Полагаем

$$n_0 = 4m \cdot |P| + (4\ell m + 1) \cdot t_{\mathfrak{M}}(P) + 2$$

По лемме 3 соотношение $\mathfrak{N}: P \models_n S$, где S не содержит γ, возможно лишь при $n < n_0$. Следовательно, найдутся n и S, удовлетворяющие условию леммы 4, и тогда $\mathfrak{N}: P \models_n S$, $\mathfrak{M}(P) = \bar{S}$ и $w(S) \leqslant n_0 - n$. Слово S содержит единственное вхождение буквы из П, поэтому, согласно формулам (I2)-(I5), будет $\mathfrak{N}: S \models\cdot_k \bar{S}$, где $k \leqslant 2\cdot|\bar{S}|+2$. Но, с другой стороны, $w(S) \geqslant 4\cdot|\bar{S}|$, следовательно, $k \leqslant w(S)+2$. Окончательно имеем $\mathfrak{N}(P) = \bar{S} = \mathfrak{M}(P)$ и $t_{\mathfrak{N}}(P) = n+k \leqslant n_0+2$. Теорема доказана.

Теорема 2. По любому нормальному алгорифму $\mathfrak{M}$ в алфавите М и любому положительному рациональному числу ε можно построить алгорифм $\mathfrak{R}$ в расширении М, вполне эквивалентный $\mathfrak{M}$ относительно М, обладающий оперативным алфавитом, не пересекающимся с М, и такой, что для любого слова P в М, к которому применим алгорифм $\mathfrak{M}$,

$$t_{\mathfrak{R}}(P) \leqslant \varepsilon\,(t_{\mathfrak{M}}(P) + |P|) + 2.$$

Доказательство. Построим вначале алгорифм $\mathfrak{N}$ и числа C_1, C_2 и C_3 со свойствами, указанными в формулировке теоремы I. Обозначим алфавит алгорифма $\mathfrak{N}$ через А, а его оперативный алфавит - через Б. Определим для любого слова R в А и любого натурального k слово $\mathfrak{N}_k(R)$ в алфавите $A \cup \{\cdot\}$ следующим образом:

$$\mathfrak{N}_0(R) = R$$

$$\mathfrak{N}_{k+1}(R) = \begin{cases} S, & \text{если } \mathfrak{N}: \mathfrak{N}_k(R) \vdash S, \\ \cdot S, & \text{если } \mathfrak{N}: \mathfrak{N}_k(R) \vdash\cdot S, \\ \mathfrak{N}_k(R), & \text{если } \mathfrak{N}_k(R) \text{ начинается точкой.} \end{cases}$$

Левая часть каждой формулы в схеме алгорифма $\mathfrak{N}$, кроме последней, имеет вид $X\omega Y$, где $\omega \in$ Б. Обозначим через v максимум $|X|$ и $|Y|$ по всем формулам $\mathfrak{N}$.

Лемма 5. Пусть X, Y - слова в алфавите $A \setminus Б$, $\omega \in Б$, S - слово в A и при некотором k

$$\mathfrak{N}_k(X\omega Y) = \eta S,$$

где η - пустое слово или точка. Тогда для любых слов V и W в $A \setminus Б$, удовлетворяющих условиям

$$(|X| < k\tau \supset V = \Lambda) \text{ и } (|Y| < k\tau \supset W = \Lambda),$$

будет

$$\mathfrak{N}_k(VX\omega YW) = \eta VSW.$$

Лемма доказывается индукцией по k ($\mathfrak{N}_{k+1}(R)$ представляем в виде $\mathfrak{N}_k(\mathfrak{N}_1(R))$, если $\mathfrak{N}_1(R)$ не начинается точкой).

Зафиксируем теперь некоторое k и построим алгорифм $\mathfrak{R}$ в алфавите А, схема которого состоит из всевозможных формул вида

$$X\omega Y \to \mathfrak{N}_k(X\omega Y),$$

где X и Y - слова в $A \setminus Б$, $|X| \leq k\tau$, $|Y| \leq k\tau$ и $\omega \in Б$, расположенных по убыванию $|X| + |Y|$, за которыми следует копия последней формулы схемы $\mathfrak{N}$. Нетрудно видеть, что Б является оперативным алфавитом также для $\mathfrak{R}$.

Первый шаг алгорифма $\mathfrak{R}$ над словом P в алфавите М будет идентичен первому шагу $\mathfrak{N}$, каждый последующий незаключительный шаг $\mathfrak{R}$ заменяет ровно k шагов алгорифма $\mathfrak{N}$, а заключительный шаг $\mathfrak{R}$ заменяет не более, чем k последних шагов алгорифма $\mathfrak{N}$. Поэтому для всякого слова P в М имеем

$$\mathfrak{R}(P) \simeq \mathfrak{N}(P),$$

$$t_{\mathfrak{R}}(P) \simeq 1 + \left]\frac{t_{\mathfrak{N}}(P)-1}{k}\right[$$

(здесь $]a[$ означает $-[-a]$).

При $k\varepsilon \geqslant c_1 + c_2 + c_3$ алгорифм $\mathfrak{R}$ будет искомым.

ЛИТЕРАТУРА

1. Марков А.А. Теория алгорифмов. "Тр.Матем.ин-та АН СССР", 1954, 42.
2. Яновская С.А. Математическая логика и основания математики. Математика в СССР за сорок лет, Физматгиз, М., 1959, I, 13-120.
3. Нагорный Н.М. Некоторые обобщения понятия нормального алгорифма, "Тр.Матем.ин-та АН СССР", 52,7-65.
4. Цейтин Г.С. Нижняя оценка числа шагов для обращающего нормального алгорифма и других аналогичных алгорифмов. Настоящий сборник, 243-262.