G. S. Tseitin, The lower estimate of number of steps for reversing normal algorithms and other similar algorithms, *Zap. Nauchn. Sem. LOMI*, 1971, Volume 20, 243–262

Г.С.Цейтин

НИЖНЯЯ ОЦЕНКА ЧИСЛА ШАГОВ ДЛЯ ОБРАЩАЮЩЕГО НОРМАЛЬНОГО АЛГОРИФМА И ДРУГИХ АНАЛОГИЧНЫХ АЛГОРИФМОВ*)

В этой статье будет доказана общая теорема, из которой следует, в частности, что число шагов нормального алгорифма, переворачивающего любое слово в некотором (не менее, чем двухбуквенном) алфавите, для "почти всех" слов должно быть не меньше, чем Cn^2, где n - длина слова, а C - константа, определяемая по схеме алгорифма.

Аналогичные результаты для машин Тьюринга получаются сравнительно несложно при помощи техники следов (см., например, оценку для распознавания симметрии в [I]). Эту технику не удается применить для нормальных алгорифмов из-за того, что там в процессе работы возможно "растяжение" и "сжатие" слова. Метод доказательства, используемый в настоящей работе, основан на представлении о распространении по слову двух встречных потоков информации. Используя этот метод, автор в 1957 году получил для числа шагов обращающего алгорифма более слабую нижнюю оценку**) - $\frac{cn^2}{\ell n^2 n}$ (результат докладывался в 1957 г. на семинаре в Математическом институте АН СССР и в 1961 г. на 4-ом Всесоюзном математическом съезде; см.также [I]). Оценка, полученная в настоящей статье, - точная (она достигается, например, обращающим алгорифмом, построенным в [2:П. § 4. I3]).

Общая схема доказательства состоит в следующем. Разделим ис-

---

*) Результат настоящей статьи докладывался на Ленинградском семинаре по теории сложности алгорифмов в ноябре и декабре 1969 г.

**) Показатель степени мы будем писать при знаке логарифма.

ходное слово на две части и далее на всех промежуточных словах будем наблюдать распространение по слову информации о левой части исходного слова. Для этого на каждом из промежуточных слов определим информационную функцию - каждому концу слова поставим в соответствие некоторое число, выражающее степень его зависимости от левой части исходного слова. Эту функцию удобно представлять себе графически, откладывая над каждой буквой написанного слова (или над промежутком между буквами) по ординате значение этой функции для конца слова, начинающегося с этого места. На исходном слове эта функция равна нулю на правой части и какому-нибудь большому числу - на левой, а по мере работы алгорифма эта функция постепенно "перетекает" в правую часть. Аналогичная информационная функция определяется для зависимости начал промежуточных слов от правой части исходного слова. Эта функция по мере работы "перетекает" влево.

Степень взаимного "перемешивания" этих двух функций определяется следующим образом. Для каждой "точки" в слове строится на плоскости прямоугольник $(0, x) \times (0, y)$, где x и y - значения указанных информационных функций в этой точке, и рассматривается "подграфик" слова - объединение всех таких прямоугольников. Далее доказательство распадается на две части: с одной стороны, надо оценить сверху возрастание площади подграфика в зависимости от числа шагов, с другой стороны, - показать, что при малых значениях информационной функции разнообразие концов (соответственно, начал), обладающих такими значениями, будет невелико. Отсюда будет следовать, что "почти все" слова требуют больших значений информационных функций и тем самым большой площади подграфика.

Наиболее простой вариант определения информационной функции связан непосредственно с шагами рассматриваемого алгорифма (надлежащим образом преобразованного): считается, что каждый шаг передает не более одной единицы информации. Точнее, если на некотором шаге был заменен отрезок слова с минимальным значением информационной функции x_1 и максимальным значением x_2, то на вновь полавленном отрезке слова информационная функция полагается рав-

ной $x_1 + sign(x_2 - x_1)$. Именно этот способ привел к упомянутой выше оценке с квадратом логарифма в знаменателе. Ухудшение нижней оценки по этому способу связано с тем, что фактически в отдельных случаях короткий участок слова на определенном шаге и в определенной позиции может нести большую информацию (в сопоставлении с другими исходными словами); тогда большое количество информации будет передаваться за малое число шагов. Получение точной оценки для числа шагов потребовало совсем другого, вероятностного подхода к определению информационных функций и к оценке площади подграфика.

Рассмотрим некоторое конечное множество слов и введем на нем некоторую вероятностную меру - каждому элементу поставим в соответствие некоторое, для простоты рациональное, положительное число, так чтобы сумма всех этих чисел была равна I. Зафиксируем некоторую переменную, пробегающую это множество - "основную случайную переменную". Термы, содержащие свободно эту переменную, будем называть случайными словами или случайными величинами, а формулы, содержащие ее свободно, - случайными событиями. Вероятностью случайного события будем называть сумму чисел, поставленных в соответствие всем тем значениям основной случайной переменной, при которых данная формула выполняется; аналогично определяются и другие теоретико-вероятностные понятия. Основная случайная переменная не будет явно присутствовать в обозначениях; вместо этого для некоторых термов и формул, содержащих ее, (т.е. для некоторых случайных величин и случайных событий) будут введены самостоятельные обозначения в виде букв с тильдой наверху. Вероятность события $\tilde{A}$ будем обозначать $p(\tilde{A})$, вероятность $\tilde{A}$ при условии $\tilde{B}$ (т.е. $\frac{p(\tilde{A}\&\tilde{B})}{p(\tilde{B})}$) - через $p(\tilde{A}|\tilde{B})$; математическое ожидание случайной величины $\tilde{a}$ будем обозначать $E(\tilde{a})$. Знаки p и E, подобно кванторам, связывают основную случайную переменную, поэтому вероятности и математические ожидания уже не являются случайными величинами.

Пусть даны случайные слова $\tilde{X}$ и $\tilde{Y}$. Введем некоторую специальную меру зависимости $\tilde{Y}$ от $\tilde{X}$. Множеством возможных значений пары $\tilde{X}, \tilde{Y}$ будем называть множество пар слов (X, Y), таких что

$p(\tilde{X}=X \,\&\, \tilde{Y}=Y)>0$. Фиксируем некоторое натуральное число m и рассмотрим всевозможные подмножества $\mathcal{M}$ множества возможных значений $\tilde{X},\tilde{Y}$, содержащие для каждого X не более m различных пар с первой компонентой X (при $m=1$ это униформные множества). Через $\varphi(m)$ обозначим наибольшее значение $p((\tilde{X},\tilde{Y})\in\mathcal{M})$ достигаемое на таких $\mathcal{M}$ (множество $\mathcal{M}$, на котором достигается это наибольшее значение вероятности, легко построить, выбрав для каждого X те m значений $\tilde{Y}$, которые наиболее вероятны при условии $\tilde{X}=X$). Функцию φ, определенную таким образом, будем называть ф у н к ц и е й п о к р ы т и я [*] $\tilde{Y}$ относительно $\tilde{X}$ (Нетрудно заметить, что $\varphi(m)$ монотонно возрастает от 0 при $m=0$ до I при некотором натуральном m и что функция φ -выпуклая, т.е.

$$\varphi(n+1)-\varphi(n)\leqslant\varphi(n)-\varphi(n-1)$$

при n целом положительном). Определим также "обратную" функцию Φ: при рациональном a, таком что $0\leqslant a<1$, полагаем $\Phi(a)$ равным наименьшему m, при котором $\varphi(m)>a$. Функцию Φ будем называть ф у н к ц и е й р а з н о о б р а з и я $\tilde{Y}$ относительно $\tilde{X}$ (она показывает, сколько различных значений $\tilde{Y}$ на одно значение $\tilde{X}$ нужно взять для того, чтобы с вероятностью больше a случайная пара $(\tilde{X},\tilde{Y})$ попадала в отобранное множество).

Заимствуем обозначения, относящиеся к словам и алгорифмам, из

---

[*] Можно было бы (и с позиций конструктивной математики это было бы логически проще) вместо функции покрытия φ ввести предикат φ', такой что $\varphi'(m,a)$ в том и только том случае, если $a\geqslant p((\tilde{X},\tilde{Y})\in\mathcal{M})$ для любого множества $\mathcal{M}$, содержащего не более m различных пар (X,Y) при каждом X. В данной статье в этом и в ряде последующих случаев предпочтение отдано функциональному (операторному), а не предикатному способу изложения с целью сделать результаты более наглядными. В допустимости функционального способа изложения (т.е. в существовании требуемых алгорифмов) в каждом конкретном случае нетрудно убедиться, поскольку (именно с этой целью) для некоторых переменных предусмотрено, что они принимают только рациональные значения.

[2] и [3] . В дальнейшем, если не будет оговорено противное, латинские буквы без тильды будут служить переменными, прописные - для слов, а строчные - для натуральных чисел. Введем также следующие обозначения: $P \prec Q$ будет означать "P является началом Q", а $P \succ Q$ "Q является концом P" (заметим, что $P \succ Q$ и $Q \prec P$ - разные утверждения); $P \prec Q \prec R$ будет означать $P \prec Q \;\&\; Q \prec R$, а $P \succ Q \succ R$ будет означать $P \succ Q \;\&\; Q \succ R$. Будем писать также $\mathfrak{A} : X \vdash$ (где $\mathfrak{A}$ - нормальный алгорифм), если существует такое Y, что $\mathfrak{A} : X \vdash Y$ и $\mathfrak{A} : X \nvdash$ в противоположном случае.

Назовем степенью вложенности начал (концов) для пары случайных слов $\tilde{X}$, $\tilde{Y}$ наибольшее натуральное число k, при котором существуют такое слово X и такая цепочка слов $Y_1, \ldots, Y_k$, что при каждом i, таком что $1 \leqslant i \leqslant k$, будет $p(\tilde{X} = X \;\&\; \tilde{Y} = Y_i) > 0$ и при каждом i, таком что $1 \leqslant i < k$, будет $Y_i \neq Y_{i+1}$ и $Y_i \prec Y_{i+1}$ (соответственно, $Y_{i+1} \succ Y_i$). Степень вложенности начал (концов) по существу характеризует множество возможных значений пары $\tilde{X}$, $\tilde{Y}$.

Теперь можно дать формулировку основной теоремы.

Теорема. По всякому нормальному алгорифму $\mathfrak{A}$ можно указать такую положительную рациональную константу c, что для любой четверки случайных слов $\tilde{P}, \tilde{Q}, \tilde{K}, \tilde{L}$ в алфавите алгорифма $\mathfrak{A}$ имеет место следующее: если рациональное положительное и целое положительное t_0 таковы, что

$$p(\mathfrak{A}(\tilde{P}\tilde{Q}) = \tilde{K}\tilde{L} \;\&\; t_{\mathfrak{A}}(\tilde{P}\tilde{Q}) + |\tilde{P}\tilde{Q}| \leqslant t_0) \geqslant p_0, \qquad (1)$$

то*),

$$t_0 \geqslant c \max_{x+y=p_0(1-\varepsilon)} \varepsilon (\ln \Phi(x) \dot{-} \ln x)(\ln \Psi(x) \dot{-} \ln \lambda), \qquad (2)$$

*) Знак $\dot{-}$ обозначает арифметическую разность ($\alpha \dot{-} \beta = 0$, если $\alpha < \beta$).

где Φ - функция разнообразия $\tilde{K}$ относительно $\tilde{P}$, Ψ - функция разнообразия $\tilde{L}$ относительно $\tilde{Q}$, $\varkappa$ - степень вложенности начал для пары $\tilde{P}$, $\tilde{K}$, λ - степень вложенности концов для пары $\tilde{Q}$, $\tilde{L}$, а x, y и ε пробегают рациональные значения в промежутке (0,I).

Проиллюстрируем применение этой теоремы на обращающем алгорифме. Возьмем некоторый s -буквенный алфавит A и натуральное число n. Определим четверку случайных слов $\tilde{P}$, $\tilde{Q}$, $\tilde{K}$, $\tilde{L}$ таким образом, чтобы $\tilde{P}$ пробегало с равными вероятностями все слова в A длиной $[\frac{n}{2}]$, а $\tilde{Q}$ - независимо от $\tilde{P}$ с равными вероятностями все слова в A длиной $[\frac{n+1}{2}]$ и чтобы во всех случаях было $\tilde{K}=[\tilde{Q}^{\smile}$ и $\tilde{L}=[\tilde{P}^{\smile}$ (тогда $\tilde{K}\tilde{L}=[\tilde{P}\tilde{Q}^{\smile}$). Случайное слово $\tilde{K}$ независимо от P принимает с равными вероятностями $s^{[\frac{n+1}{2}]}$ различных значений, поэтому

$$\Phi(x)=]xs^{[\frac{n+1}{2}]}[;$$

аналогично,

$$\Psi(y)=]ys^{[\frac{n}{2}]}[,$$

$\varkappa=\lambda=1$, и из (2) следует

$$t_0 > c \max_{x+y=p_0(1-\varepsilon)} \varepsilon \ln(xs^{[\frac{n+1}{2}]}) \ln(ys^{[\frac{n}{2}]}).$$

Полагая $x=y=\frac{1}{3}p_0$ и $\varepsilon=\frac{1}{3}$, получим отсюда

$$t_0 > \frac{1}{12} c \ln^2 s \cdot (n-q)^2, \qquad (3)$$

где

$$q = 1 - \frac{\ln \frac{1}{3}p_0}{\ln s}.$$

Если $\mathfrak{A}$ - обращающий алгорифм в A, то событие $\mathfrak{A}(\tilde{P}\tilde{Q})=\tilde{K}\tilde{L}$ до-

стоверно. Полагаем $\tilde{P}\tilde{Q} = \tilde{R}$; случайное слово $\tilde{R}$ пробегает с равными вероятностями все n-буквенные слова в А. Пусть $t_0 = t_1 + n$. Тогда (I) принимает вид

$$p(t_{\mathfrak{A}}(\tilde{R}) \leqslant t_1) \geqslant p_0.$$

Из (3) получаем, что при выполнении этого условия будет

$$t_1 > \frac{1}{12} c \ln^2 s \cdot (n-q)^2 - n.$$

При помощи такого же рассуждения можно получить аналогичные оценки и для других алгорифмов, работа которых связана с перестановкой частей слова.

Доказательство теоремы. I°. Пусть дан алгорифм $\mathfrak{A}$ в алфавите А. Подвергнем его ряду последовательных преобразований. Вначале применим теорему I из [3] и построим алгорифм $\mathfrak{L}$ в алфавите Б с оперативным алфавитом В (причем $A \subseteq Б \setminus B$), вполне эквивалентный $\mathfrak{A}$ относительно А, и такие константы c_1, c_2, c_3, что для любого слова R, к которому применим $\mathfrak{A}$, будет

$$t_{\mathfrak{L}}(R) \leqslant c_1 \cdot t_{\mathfrak{A}}(R) + c_2 \cdot |R| + c_3. \qquad (4)$$

Введем новые буквы γ и δ и перестроим схему алгорифма $\mathfrak{L}$ следующим образом: заменим левую часть последней формулы буквой γ, выбросим из правых частей заключительных формул все вхождения букв алфавита В (если они там были), заменим все точки буквой δ и, наконец, добавим к схеме (все равно, в каком месте) формулы

$$\delta\xi \to \xi\delta \quad (\xi \in Б \setminus B).$$

Алгорифм с такой схемой в алфавите $Б \cup \{\gamma, \delta\}$ обозначим $\mathfrak{L}$. Для любых слов R, S в А, таких что $\mathfrak{L}(R) = S$, имеем $\mathfrak{L}(\gamma R) = S\delta$ и

$$t_{\mathfrak{L}}(\gamma R) \leqslant t_{\mathfrak{L}}(R) + |S|.$$

В схеме $\mathfrak{L}$ каждая формула имеет вид $X\chi Y \to X'\chi'Y'$, где $\chi, \chi' \in В \cup \{\gamma, \delta\}$. Если $|X'| - |X| > 1$, то, полагая $X' = X_1\xi$ и

вводя новую букву ψ , заменяем эту формулу на две формулы

$$X\chi Y \to X_1 \psi Y'$$

Аналогично поступаем, если $|Y'| - |Y| > 1$. Применяя эту операцию многократно, получим алгорифм ϑ в некотором алфавите Г, содержащем подалфавит Д, такой что $A \subseteq Г \setminus Д$ и $\gamma, \delta \in Д$, причем выполняются следующие условия: во-первых, каждая формула схемы ϑ имеет вид

$$X\chi Y \to X'\chi' Y', \qquad (5)$$

где X , Y , X' , Y' - слова в $Г \setminus Д$, χ , $\chi' \in Д$, $|X'| - |X| \leqslant 1$ и $|Y'| - |Y| \leqslant 1$, во-вторых, для любых слов R и S в A, таких что $\mathfrak{L}(\gamma R) = S\delta$, будет $\vartheta(\gamma R) = S\delta$ и

$$t_{\vartheta}(\gamma R) \leqslant c_{ц} \cdot t_{\mathfrak{L}}(\gamma R),$$

где $c_{ц}$ не зависит от R и S .

Возьмем такое натуральное число τ , что во всех формулах (5) $|X| \leqslant \tau$ и $|Y| \leqslant \tau$ (ср. доказательство теоремы 2 в [3]). Введем новую букву ω . Рассмотрим всевозможные слова вида $M\chi N$, где M и N - слова в $Г \setminus Д$, $\chi \in Д$, $|M| \leqslant \tau$ и $|N| \leqslant \tau$. Если алгорифм переводит (одним шагом) слово $M\chi N$ в слово P , то построим формулу

$$\omega^{\tau - |M|} M\chi N \omega^{\tau - |N|} \to \omega^{\tau - |M|} P \omega^{\tau - |N|}.$$

Алгорифм в алфавите $Г \cup \{\omega\}$, схема которого состоит из всех таких формул (порядок безразличен), обозначим $\mathfrak{E}$. Для любых слов R и S в A, таких что $\vartheta(\gamma R) = S\delta$, имеем

$$\mathfrak{E}(\omega^{\tau}\gamma R \omega^{\tau}) = \omega^{\tau} S \delta \omega^{\tau},$$

$$t_{\mathfrak{E}}(\omega^{\tau}\gamma R \omega^{\tau}) = t_{\vartheta}(\gamma R).$$

Кроме того, всякая формула в схеме $\mathfrak{E}$ имеет вид

$$X\chi Y \to X'\chi'Y',$$

где X, Y, X', Y' – слова в $\Gamma \cup \{\omega\} \setminus Д$, $\chi, \chi' \in Д$, $|X| = |Y| = \tau$, $|X'| \leq \tau+1$ и $|Y'| \leq \tau+1$.

Введем, наконец, новые буквы π и θ и построим алфавиты $E = \Gamma \cup \{\omega, \theta\} \setminus Д$ и $Ж = Д \cup \{\pi\}$. Буквы алфавита $Ж$ будем называть о п е р а т и в н ы м и буквами. Построим алгорифм $\mathfrak{f}$ в алфавите $E \cup Ж$ со схемой, получаемой из схемы $\mathfrak{C}$ добавлением (в произвольном порядке) следующих формул:

$$\theta^\tau \pi \theta^i \omega^{\tau-i} \to \theta^\tau \pi \theta^{i+1} \omega^{\tau-i} \qquad (0 \leq i < \tau)$$

$$\theta^\tau \pi \theta^\tau \to \theta^{\tau-1} \pi \theta^\tau$$

$$\xi \theta^{\tau-1} \pi \theta^\tau \to \theta^\tau \pi \theta^\tau \xi \qquad (\xi \in \Gamma \setminus Д)$$

$$\omega^{\tau-i} \theta^i \pi \theta^\tau \to \omega^{\tau-i} \theta^{i-1} \pi \theta^\tau \qquad (0 < i < \tau)$$

$$\omega^\tau \pi \theta^\tau \to \omega^\tau \gamma$$

$$X \theta^i \delta \omega^\tau \to X \theta^{i+1} \delta \omega^\tau \qquad (0 \leq i < \tau, |X| = \tau - i,$$
X – слово в $E \setminus \{\theta\}$)

$$\theta^\tau \delta \theta^i \omega^{\tau-i} \to \theta^\tau \delta \theta^{i+1} \omega^{\tau-i} \qquad (0 \leq i < \tau)$$

$$\theta^\tau \delta \theta^\tau \to \theta^{\tau-1} \delta \theta^\tau \qquad (*)$$

$$\xi \theta^{\tau-1} \delta \theta^\tau \to \theta^\tau \delta \theta^\tau \xi \qquad (\xi \in \Gamma \setminus Д).$$

В схеме алгорифма $\mathfrak{f}$ все формулы снова имеют вид

$$X\chi Y \to X'\chi'Y',$$

где χ, χ' – оперативные буквы, X , Y , X' , Y' – слова в E, $|X| = |Y| = \tau$, $|X'| \leq \tau+1$ и $|Y'| \leq \tau+1$. Объединяя соотношения, выписанные для алгорифмов $\mathfrak{L}$, $\mathfrak{L}, \mathfrak{V}$ и $\mathfrak{C}$, получаем, что для любых слов R , S , таких что $\mathfrak{A}(R) = S$, будет

$$\mathfrak{f}(\omega^\tau R \theta^\tau \pi \omega^\tau) = \omega^\tau \theta^{\tau-1} \delta \theta^\tau S \omega^\tau,$$

$$t_{\mathfrak{f}}(\omega^{r}R\theta^{r}\pi\omega^{r}) = t_{\mathfrak{G}}(\omega^{r}\alpha R\omega^{r}) + 2\cdot|R| + 2\cdot|S| + 4r + 2 \leq$$

$$\leq c_4(t_{\mathfrak{G}}(R) + |S|) + 2\cdot|R| + 2\cdot|S| + 4r + 2.$$

Используя (4), а также соотношение

$$|S| \leq |R| + c_5 t_{\alpha}(R),$$

где c_5 – максимальная длина правых частей формул в схеме $\mathfrak{A}$, найдем такую натуральную константу c', что для любого слова R, к которому применим алгорифм $\mathfrak{A}$, будем иметь

$$t_{\mathfrak{f}}(\omega^{r}R\theta^{r}\pi\omega^{r}) \leq c'(t_{\alpha}(R) + |R| + 1). \qquad (6)$$

Заметим, наконец, что последним шагом при работе алгорифма $\mathfrak{f}$ над словом $\omega^{r}R\theta^{r}\pi\omega^{r}$ является в этом случае применение формулы(*).

Занумеруем все формулы в схеме $\mathfrak{f}$ числами от I до некоторого $\bar{k}$; Левую часть k -й формулы обозначим V_k, а правую – W_k. Номер формулы (*) обозначим k^*.

2°. Рассмотрим случайные слова $\tilde{P}$, $\tilde{Q}$, $\tilde{K}$, $\tilde{L}$. Полагаем

$$\tilde{R}_0 = \omega^{r}\tilde{P}\tilde{Q}\theta^{r}\pi\omega^{r},$$

$$\tilde{t} = t_{\mathfrak{f}}(\tilde{R}_0).$$

Определим $\tilde{R}_n$, $\tilde{k}_n$, $\tilde{S}_n$ и $\tilde{T}_n$ индукцией по n таким образом, чтобы при $\mathfrak{f}: \tilde{R}_{n-1} \vdash$ было

$$\tilde{R}_{n-1} = \tilde{S}_n V_{\tilde{k}_n} \tilde{T}_n, \qquad (7)$$

$$\tilde{R}_n = \tilde{S}_n W_{\tilde{k}_n} \tilde{T}_n,$$

а при $\mathfrak{f}: \tilde{R}_{n-1} \urcorner$ термы $\tilde{S}_n$, $\tilde{k}_n$, $\tilde{T}_n$, $\tilde{R}_n$ оставались неопределенными ($\tilde{R}_n$ – это результат n шагов работы алгорифма $\mathfrak{f}$ над словом $\tilde{R}_0$, а $\tilde{k}_n$ – номер формулы, примененной на n-м шаге; из равенства (7) значения $\tilde{k}_n$, $\tilde{S}_n$ и $\tilde{T}_n$ определяются однозначно). Таким образом, $\tilde{k}_n$, $\tilde{S}_n$ и $\tilde{T}_n$ определены при $0 < n \leq \tilde{t}$.

Возьмем некоторое натуральное $\bar{t}$ и предположим временно, что события $\alpha(\tilde{P}\tilde{Q}) = \tilde{K}\tilde{L}$ и $\tilde{t} \leq \bar{t}$ достоверны. Далее буква P будет употребляться в качестве переменной, пробегающей множество всех возможных значений $\tilde{P}$, т.е. таких слов Z, что $p(\tilde{P} = Z) > 0$; аналогично, Q будет пробегать множество возможных значений $\tilde{Q}$. Введем следующие функции

$$\alpha(P, X) = \sum_{n=1}^{\bar{t}} p(X = \tilde{S}_n \mid \tilde{P} = P),$$

$$\alpha'(P, X) = \sum_{n=1}^{\bar{t}} p(\tilde{S}_n V_{\tilde{k}_n} \prec X \prec \tilde{R}_{n-1} \mid \tilde{P} = P),$$

$$\beta(Q, Y) = \sum_{n=1}^{\bar{t}} p(Y = \tilde{T}_n \mid \tilde{Q} = Q),$$

$$\beta'(Q, Y) = \sum_{n=1}^{\bar{t}} p(\tilde{R}_{n-1} \succ Y \succ V_{\tilde{k}_n} \tilde{T}_n \mid \tilde{Q} = Q);$$

в этих формулах высказывания, содержащие $\tilde{S}_n$, $\tilde{k}_n$ и т.п., в случае неопределенности этих термов рассматриваются как ложные.

Эти выражения соответствуют информационным функциям, упомянутым в начале этой статьи: если X - начало $\tilde{R}_n$, то в качестве значения информационной функции для него берется $-\ln \alpha'(\tilde{P}, X)$ или $-\ln \alpha(\tilde{P}, X)$ в зависимости от того, входит или нет в слово X оперативная буква; аналогично для концов $\tilde{R}_n$.

Лемма Iа. Если $X \prec \omega^r P$, то $\alpha(P, X) \geq 1$.

Действительно, из схемы $\mathcal{F}$ видно, что для любого X, такого что $X \prec \omega^r \tilde{P}\tilde{Q}$, найдется такое n, что $\tilde{S}_n = X$; поэтому, если $X \prec \omega^r P$, то

$$p(\exists n (X = \tilde{S}_n) \mid \tilde{P} = P) = 1,$$

следовательно,

$$\sum_{n=1}^{\bar{t}} p(X = \tilde{S}_n \mid \tilde{P} = P) \geq 1.$$

Лемма Iб. Если $0 \leq i \leq r$, то $\beta(Q, \omega^i) \geq 1$.

Лемма Iв. Если $Q\theta^r \pi \omega^r \succ Y \succ \theta^r \pi \omega^r$, то $\beta'(Q, Y) \geq 1$.

Лемма 2а. Если $\mathcal{F}: X \vdash$ и $X \prec X_1$, то $\alpha'(P, X_1) \leq \alpha'(P, X)$.

Действительно, из $\tilde{S}_n V_{\tilde{k}_n} \prec X_1 \prec \tilde{R}_{n-1}$ следует $\tilde{S}_n V_{\tilde{k}_n} \prec X \prec R_{n-1}$.

Лемма 2б. Если $\mathcal{F}: Y \vdash$ и $Y_1 \succ Y$, то $\beta'(Q, Y_1) \leq \beta'(Q, Y)$.

Лемма 3а. Если $\mathcal{F}: X \vdash X_1 \vdash$ то $\alpha'(P, X) \leq \alpha'(P, X_1)$.

Действительно, в этом случае из $\tilde{S}_n V_{\tilde{k}_n} \prec X \prec \tilde{R}_{n-1}$ следует, что $n < \tilde{t} \leq \bar{t}$, $X_1 \prec \tilde{R}_n$ и $\tilde{S}_{n+1} V_{\tilde{k}_{n+1}} \prec X_1$; поэтому

$$p(\tilde{S}_{\tilde{t}} V_{\tilde{k}_{\tilde{t}}} \prec X \prec \tilde{R}_{\tilde{t}-1} \mid \tilde{P} = P) = 0,$$

а при $n < \bar{t}$ будет

$$p(\tilde{S}_n V_{\tilde{k}_n} \prec X \prec \tilde{R}_{n-1} \mid \tilde{P} = P) \leq p(\tilde{S}_{n+1} V_{\tilde{k}_{n+1}} \prec X_1 \prec \tilde{R}_n \mid \tilde{P} = P).$$

Лемма 3б. Если $\mathcal{F}: Y \vdash Y_1 \vdash$, то $\beta'(Q, Y) \leq \beta'(Q, Y_1)$

Лемма 4а. Если $\mathcal{F}$ переводит слово X в слово $X_1 Z$ по формуле, отличной от (ж), и $(\tau+1)$-я от начала буква слова Z - оперативная, то $\alpha'(P, X) \leq \alpha(P, X_1)$.

Действительно, в этом случае из $\tilde{S}_n V_{\tilde{k}_n} \prec X \prec \tilde{R}_{n-1}$ следует, что $n < \tilde{t} \leq \bar{t}$ и $\tilde{S}_{n+1} = X_1$.

Лемма 4б. Если $\mathcal{F}$ переводит слово Y в слово $Z Y_1$ по формуле, отличной от (ж), и $(\tau+1)$-я от конца буква слова Z - оперативная, то $\beta'(Q, Y) \leq \beta(Q, Y_1)$.

Лемма 5а. $\alpha'(P, X V_k) = \sum_{n=1}^{\bar{t}} p(X = \tilde{S}_n \,\&\, k = \tilde{k}_n \mid \tilde{P} = P)$.

Следствие. $\alpha(P, X) = \sum_{k=1}^{\bar{k}} \alpha'(P, X V_k)$.

Лемма 5б. $\beta'(Q, V_k Y) = \sum_{n=1}^{\bar{t}} p(Y = \tilde{T}_n \,\&\, k = \tilde{k}_n \mid \tilde{P} = P)$.

Следствие. $\beta(Q, Y) = \sum_{k=1}^{\bar{k}} \beta'(Q, V_k Y)$.

Определим следующие интервалы на числовой прямой (здесь выражение $(0, -\ln a)$, где a - рациональное, означает при $a \geq 1$ пустое множество, а при $a = 0$ - интервал $(0, +\infty)$).

$$\tilde{A}(X) = (0, -\ln \alpha(\tilde{P}, X)).$$

$$\tilde{\mathcal{A}}'(X)=\begin{cases}\varnothing & ,\text{если } \mathcal{F}:X\urcorner,\\ (0,-\ln\alpha'(\tilde{P},X)) & ,\text{если } \mathcal{F}:X\vdash,\end{cases}$$

$$\tilde{\mathcal{B}}(Y)=(0,-\ln\beta(\tilde{Q},Y)),$$

$$\tilde{\mathcal{B}}'(Y)=\begin{cases}\varnothing & ,\text{если } \mathcal{F}:Y\urcorner\\ (0,-\ln\beta'(\tilde{Q},Y)) & ,\text{если } \mathcal{F}:Y\vdash\end{cases}$$

Определим следующие множества на плоскости:

$$\tilde{\mathcal{C}}_n=\bigcup_{XY=\tilde{R}_n}\tilde{\mathcal{A}}(X)\times\tilde{\mathcal{B}}'(Y),$$

$$\tilde{\mathcal{D}}_n=\bigcup_{XY=\tilde{R}_n}\tilde{\mathcal{A}}'(X)\times\tilde{\mathcal{B}}(Y),$$

$$\tilde{\mathcal{E}}_n=\bigcup_{i=1}^{\min(n,\tilde{t})}\mathcal{A}'(\tilde{S}_i V_{\tilde{k}_i})\times\tilde{\mathcal{B}}'(V_{\tilde{k}_i}\tilde{T}_i)$$

(множества $\tilde{\mathcal{C}}_n\cup\tilde{\mathcal{D}}_n$ и $\tilde{\mathcal{E}}_n$ будут играть роль подграфика).

Лемма 6. Если $n\le\tilde{t}$, то $(\tilde{\mathcal{C}}_n\cup\tilde{\mathcal{D}}_n)\subseteq\tilde{\mathcal{E}}_n$.

Доказательство леммы. Применим индукцию по n. Имеем $\tilde{\mathcal{C}}_0=\varnothing$ ввиду лемм Ia и Iв, $\tilde{\mathcal{D}}_0=\varnothing$ ввиду леммы Iб. Пусть $(\tilde{\mathcal{C}}_{n-1}\cup\tilde{\mathcal{D}}_{n-1})\subseteq\tilde{\mathcal{E}}_{n-1}$. Докажем, что $\tilde{\mathcal{C}}_n\subseteq\tilde{\mathcal{E}}_n$ (доказательство для $\tilde{\mathcal{D}}_n\subseteq\tilde{\mathcal{E}}_n$ аналогичное).

Нам нужно доказать, что из $XY=\tilde{R}_n$ следует

$$\tilde{\mathcal{A}}(X)\times\tilde{\mathcal{B}}'(Y)\subseteq\tilde{\mathcal{E}}_n. \qquad (8)$$

Имеем $\tilde{R}_n=\tilde{S}_n W_{\tilde{k}_n}\tilde{T}_n$. При $\tilde{\mathcal{B}}'(Y)=\varnothing$ соотношение (8) выполняется. Пусть $\tilde{\mathcal{B}}'(Y)\neq\varnothing$. Тогда $\mathcal{F}:Y\vdash$. Предположим, что $X\prec\tilde{S}_n$. Тогда $\tilde{S}_n=XZ$ при некотором Z, и $Y=ZW_{\tilde{k}_n}\tilde{T}_n$. Полагая $Y_1=ZV_{\tilde{k}_n}\tilde{T}_n$, имеем $\mathcal{F}:Y_1\vdash Y$ и $XY_1=\tilde{R}_{n-1}$.

По лемме 3б получим, что $\beta'(\tilde{Q},Y_1)\le\beta'(\tilde{Q},Y)$, значит,

$\tilde{\mathcal{B}}'(Y) \le \tilde{\mathcal{B}}'(Y_1)$, и

$$\tilde{\mathcal{A}}(X)\times\tilde{\mathcal{B}}'(Y)\le\tilde{\mathcal{A}}(X)\times\tilde{\mathcal{B}}'(Y_1)\le\tilde{\mathcal{C}}_{n-1}\le\tilde{\mathcal{E}}_{n-1}\le\tilde{\mathcal{E}}_n.$$

Пусть теперь X не является началом $\tilde{S}_n$. Тогда Y является собственным концом слова $W_{\tilde{k}_n}\tilde{T}_n$. Из того, что $\mathcal{F}: Y \vdash$, следует, что левое крыло вхождения оперативной буквы в Y имеет длину не менее τ ; с другой стороны, по построению схемы $\mathcal{F}$ в слове $W_{\tilde{k}_n}$ левое крыло вхождения оперативной буквы имеет длину не более $\tau+1$. Следовательно, левое крыло вхождения оперативной буквы в $W_{\tilde{k}_n}$ имеет длину ровно $\tau+1$ (значит, $\tilde{k}_n \neq k^*$), а левое крыло вхождения оперативной буквы в Y имеет длину ровно τ . Следовательно, $W_{\tilde{k}_n}$ представимо в виде ξZ , где Z имеет оперативную букву на $(\tau+1)$ -м месте от начала, $Y = Z\tilde{T}_n$ и $XZ = \tilde{S}_n W_{\tilde{k}_n}$. Имеем

$$\mathcal{F}: \tilde{S}_n V_{\tilde{k}_n} \vdash \tilde{S}_n W_{\tilde{k}_n} = XZ,$$

$\tilde{k}_n \neq k^*$, следовательно, по лемме 4а,

$$\alpha'(\tilde{P}, \tilde{S}_n V_{\tilde{k}_n}) \le \alpha(\tilde{P}, X)$$

значит,

$$\tilde{\mathcal{A}}(X) \le \tilde{\mathcal{A}}'(\tilde{S}_n V_{\tilde{k}_n}). \qquad (9)$$

С другой стороны,

$$\mathcal{F}: V_{\tilde{k}_n}\tilde{T}_n \vdash W_{\tilde{k}_n}\tilde{T}_n,$$

$W_{\tilde{k}_n}\tilde{T}_n \succ Y$ и $\mathcal{F}: Y \vdash$, откуда по леммам 3б и 2б имеем

$$\beta'(\tilde{Q}, V_{\tilde{k}_n}T_n) \le \beta'(\tilde{Q}, W_{\tilde{k}_n}\tilde{T}_n) \le \beta(\tilde{Q}, Y)$$

Значит,

$$\tilde{\mathcal{B}}'(Y) \le \tilde{\mathcal{B}}'(V_{\tilde{k}_n}\tilde{T}_n),$$

что вместе с (9) дает

$$\tilde{\mathcal{A}}(X)\times\tilde{\mathcal{B}}'(Y)\subseteq\tilde{\mathcal{A}}'(\tilde{S}_n V_{\tilde{k}_n})\times\tilde{\mathcal{B}}'(V_{\tilde{k}_n}\tilde{T}_n)\subseteq\tilde{\mathcal{E}}_n$$

т.е. снова выполняется (8). Лемма доказана.

3°. Будем использовать букву μ для обозначения длины интервала или площади плоского множества. Найдем верхнюю оценку для $E(\mu\tilde{\mathcal{E}}_{\tilde{t}})$.

Пусть $0<n\leq t$. Тогда

$$\tilde{\mathcal{A}}(\tilde{S}_n)\times\tilde{\mathcal{B}}'(V_{\tilde{k}_n}\tilde{T}_n)\subseteq\tilde{\mathcal{C}}_{n-1},$$

$$\tilde{\mathcal{A}}'(\tilde{S}_n V_{\tilde{k}_n})\times\tilde{\mathcal{B}}(\tilde{T}_n)\subseteq\tilde{\mathcal{D}}_{n-1}.$$

Применяя лемму 6, получим

$$\tilde{\mathcal{E}}_n\setminus\tilde{\mathcal{E}}_{n-1}\subseteq(\tilde{\mathcal{A}}'(\tilde{S}_n V_{\tilde{k}_n})\times\tilde{\mathcal{B}}'(V_{\tilde{k}_n}\tilde{T}_n))\setminus\tilde{\mathcal{E}}_{n-1}$$

$$\subseteq(\tilde{\mathcal{A}}'(\tilde{S}_n V_{\tilde{k}_n})\times\tilde{\mathcal{B}}'(V_{\tilde{k}_n}\tilde{T}_n))\setminus(\tilde{\mathcal{C}}_{n-1}\cup\tilde{\mathcal{D}}_{n-1})$$

$$\subseteq(\tilde{\mathcal{A}}'(\tilde{S}_n V_{\tilde{k}_n})\times\tilde{\mathcal{B}}'(V_{\tilde{k}_n}\tilde{T}_n))\setminus((\tilde{\mathcal{A}}(\tilde{S}_n)\times\tilde{\mathcal{B}}'(V_{\tilde{k}_n}\tilde{T}_n))\cup(\tilde{\mathcal{A}}'(\tilde{S}_n V_{\tilde{k}_n})\times$$

$$\times\tilde{\mathcal{B}}(\tilde{T}_n)))=(\tilde{\mathcal{A}}'(\tilde{S}_n V_{\tilde{k}_n})\setminus\tilde{\mathcal{A}}(\tilde{S}_n))\times(\tilde{\mathcal{B}}'(V_{\tilde{k}_n}\tilde{T}_n)\setminus\tilde{\mathcal{B}}(\tilde{T}_n)).$$

Далее,

$$\mu(\tilde{\mathcal{E}}_n\setminus\tilde{\mathcal{E}}_{n-1})\leq\mu(\tilde{\mathcal{A}}'(\tilde{S}_n V_{\tilde{k}_n})\setminus\tilde{\mathcal{A}}(\tilde{S}_n))\cdot\mu(\tilde{\mathcal{B}}'(V_{\tilde{k}_n}\tilde{T}_n)\setminus\tilde{\mathcal{B}}(\tilde{T}_n))=$$

$$=(\ln\alpha(\tilde{P},\tilde{S}_n)-\ln\alpha'(\tilde{P},\tilde{S}_n V_{\tilde{k}_n}))\cdot(\ln\beta(\tilde{Q},\tilde{T}_n)-\ln\beta'(\tilde{Q},V_{\tilde{k}_n}\tilde{T}_n))$$

(согласно следствиям лемм 5а и 5б оба сомножителя неотрицательны).

Полагаем

$$\tilde{a}_n=\begin{cases}\ln\dfrac{\alpha(\tilde{P},\tilde{S}_n)}{\alpha'(\tilde{P},\tilde{S}_n V_{\tilde{k}_n})} & \text{, если } n\leq\tilde{t}\\ 0 & \text{, если } n>\tilde{t}\end{cases}$$

$$\tilde{b}_n=\begin{cases}\ln\dfrac{\beta(\tilde{Q},\tilde{T}_n)}{\beta'(\tilde{Q},V_{\tilde{k}_n}\tilde{T}_n)} & \text{, если } n\leq\tilde{t}\\ 0 & \text{, если } n>\tilde{t}.\end{cases}$$

Имеем

$$\mu\tilde{\xi}_{\bar{t}} = \sum_{n=1}^{\bar{t}} \mu(\tilde{\xi}_n \setminus \tilde{\xi}_{n-1}) \le \sum_{n=1}^{\bar{t}} \tilde{a}_n \tilde{b}_n \le \frac{1}{2}\left(\sum_{n=1}^{\bar{t}} \tilde{a}_n^2 + \sum_{n=1}^{\bar{t}} \tilde{b}_n^2\right),$$

$$E(\mu\tilde{\xi}_{\bar{t}}) \le \frac{1}{2}\left(\sum_{n=1}^{\bar{t}} E(\tilde{a}_n^2) + \sum_{n=1}^{\bar{t}} E(\tilde{b}_n^2)\right).$$

Случайная величина $\tilde{a}_n^2$ выражается через $\tilde{P}$, $\tilde{S}_n$ и $\tilde{k}_n$, причем, если $\tilde{S}_n$ и $\tilde{k}_n$ не определены, то $\tilde{a}_n^2 = 0$. Пусть переменная S пробегает все возможные значения $\tilde{S}_n$ при всех n. Тогда

$$E(\tilde{a}_n^2) = \sum_{P,S} \sum_{k=1}^{\bar{k}} \ln^2 \frac{\alpha(P,S)}{\alpha'(P,SV_k)} p(\tilde{P}=P \,\&\, S=\tilde{S}_n \,\&\, k=\tilde{k}_n) =$$

$$= \sum_{P} p(\tilde{P}=P) \sum_{S} \sum_{k=1}^{\bar{k}} \ln^2 \frac{\alpha(P,S)}{\alpha'(P,SV_k)} p(S=\tilde{S}_n \,\&\, k=\tilde{k}_n \mid \tilde{P}=P)$$

(чтобы избежать бессмысленных выражений под знаком логарифма, считаем, что в суммировании по k участвуют лишь те слагаемые, в которых последний сомножитель отличен от 0). Используя лемму 5а, находим

$$\sum_{n=1}^{\bar{t}} E(\tilde{a}_n^2) = \sum_{P} p(\tilde{P}=P) \sum_{S} \sum_{k=1}^{\bar{k}} \ln^2 \frac{\alpha(P,S)}{\alpha'(P,SV_k)} \sum_{n=1}^{\bar{t}} p(S=\tilde{S}_n \,\&\, k=\tilde{k}_n \mid \tilde{P}=P) =$$

$$= \sum_{P} p(\tilde{P}=P) \sum_{S} \sum_{k=1}^{\bar{k}} \ln^2 \frac{\alpha(P,S)}{\alpha'(P,SV_k)} \cdot \alpha'(P,SV_k) =$$

$$= \sum_{P} p(\tilde{P}=P) \sum_{S} \alpha(P,S) \sum_{k=1}^{\bar{k}} \ln^2 \frac{\alpha(P,S)}{\alpha'(P,SV_k)} \cdot \frac{\alpha'(P,SV_k)}{\alpha(P,S)}.$$

По $\bar{k}$ можно найти такое c'', что для любых P, S

$$\sum_{k=1}^{\bar{k}} \ln^2 \frac{\alpha(P,S)}{\alpha'(P,SV_k)} \cdot \frac{\alpha'(P,SV_k)}{\alpha(P,S)} \le c''.$$

В самом деле, каждое слагаемое в этой сумме не превосходит $4e^{-2}$, значит, можно взять $c'' = 4\bar{k}e^{-2}$. (Используя следствие леммы 5а, мо-

жно получить для этой суммы верхнюю оценку $\ell n^2 \tilde{k}$). Имеем

$$\sum_{n=1}^{\tilde{t}} E(\tilde{a}_n^2) \le c'' \sum_{P} p(\tilde{P}=P) \sum_{S} \alpha(P,S) =$$

$$= c'' \sum_{P} p(\tilde{P}=P) \sum_{S} \sum_{n=1}^{\tilde{t}} p(S=\tilde{S}_n \mid \tilde{P}=P) =$$

$$= c'' \sum_{S} \sum_{n=1}^{\tilde{t}} p(S=\tilde{S}_n) = c'' \sum_{n=1}^{\tilde{t}} \sum_{S} p(S=\tilde{S}_n) =$$

$$= c'' \sum_{n=1}^{\tilde{t}} p(\exists S (S=\tilde{S}_n)) \le c'' \tilde{t}.$$

Такую же оценку получим и для $\sum_{n=1}^{\tilde{t}} E(\tilde{b}_n^2)$, следовательно,

$$E(\mu \tilde{\mathcal{E}}_t) \le c'' \tilde{t}.$$

4^0. Перейдем к оценке разнообразия результата при ограничениях на значение информационной функции. Из того, что $\alpha(\tilde{P}\tilde{Q}) = \tilde{K}\tilde{L}$, получим (согласно построению алгорифма $\mathcal{F}$), что при работе алгорифма $\mathcal{F}$ над словом $\tilde{R}_0$ встретится слово

$$\omega^z \tilde{K} \theta^z \delta \theta^z \tilde{L} \omega^z.$$

Таким образом, при некотором n будем иметь $\tilde{S}_n = \omega^z K$, $\tilde{k}_n = k^*$ и $\tilde{T}_n = \tilde{L}\omega^z$. Следовательно,

$$\tilde{\mathcal{A}}'(\omega^z \tilde{K} V_{k^*}) \times \tilde{\mathcal{B}}'(V_{k^*} \tilde{L} \omega^z) \le \tilde{\mathcal{E}}_{\tilde{t}},$$

$$E(\mu \tilde{\mathcal{A}}'(\omega^z \tilde{K} V_{k^*}) \cdot \mu \tilde{\mathcal{B}}'(V_{k^*} \tilde{L} \omega^z)) \le E(\mu \tilde{\mathcal{E}}_{\tilde{t}}) \le c'' \tilde{t}.$$

Зафиксируем некоторые рациональные a и b , бóльшие I. Имеем

$$c'' \tilde{t} \ge E(\mu \tilde{\mathcal{A}}'(\omega^z \tilde{K} V_{k^*}) \cdot \mu \tilde{\mathcal{B}}'(V_{k^*} \tilde{L} \omega^z)) \ge$$

$$p(\mu \tilde{\mathcal{A}}'(\omega^z \tilde{K} V_{k^*}) \ge \ln a \;\&\; \mu \tilde{\mathcal{B}}'(V_{k^*} \tilde{L} \omega^z) \ge \ln b) \cdot \ln a \ln b =$$

$$= p(\alpha'(\tilde{P}, \omega^z \tilde{K} V_{k^*}) \le \tfrac{1}{a} \;\&\; \beta'(\tilde{Q}, V_{k^*} \tilde{L} \omega^z) \le \tfrac{1}{b}) \cdot \ln a \ln b.$$

Построим множества

$$\mathcal{K}_a(P)=\{K\mid \alpha'(P,\omega^{\tau}KV_{k^*})>\tfrac{1}{a}\ \&\ p(\tilde{K}=K\ \&\ \tilde{P}=P)>0\},$$

$$\mathcal{L}_b(Q)=\{L\mid \beta'(Q,V_{k^*}L\omega^{\tau})>\tfrac{1}{b}\ \&\ p(\tilde{L}=L\ \&\ \tilde{Q}=Q)>0\}.$$

Тогда

$$p(\tilde{K}\notin\mathcal{K}_a(\tilde{P})\ \&\ \tilde{L}\notin\mathcal{L}_b(\tilde{Q}))\leqslant\frac{c''\bar{t}}{\ln a\ln b},$$

$$p(\tilde{K}\in\mathcal{K}_a(\tilde{P})\vee\tilde{L}\in\mathcal{L}_b(\tilde{Q}))\geqslant 1-\frac{c''t}{\ln a\ln b}. \qquad (10)$$

Пусть $K\in\mathcal{K}_a(P)$. Тогда

$$\alpha'(P,\omega^{\tau}KV_{k^*})>\tfrac{1}{a},$$

т.е., в силу леммы 5а,

$$\sum_{n=1}^{\bar{t}}p(\omega^{\tau}K=\tilde{S}_n\ \&\ k^*=\tilde{k}_n\mid\tilde{P}=P)>\tfrac{1}{a}.$$

Из построения алгорифма $\mathfrak{f}$ следует, что события

$$\omega^{\tau}K=\tilde{S}_n\ \&\ k^*=\tilde{k}_n$$

при различных n несовместны и, кроме того, что

$$\exists n\,(\omega^{\tau}K=\tilde{S}_n\ \&\ k^*=\tilde{k}_n)\equiv K\prec\tilde{K}\tilde{L}.$$

Таким образом, если $K\in\mathcal{K}_a(P)$, то

$$p(K\prec\tilde{K}\tilde{L}\mid\tilde{P}=P)>\tfrac{1}{a}.$$

Пусть множество $\mathcal{K}_a(P)$ содержит m различных элементов $(m>0)$. Тогда

$$\sum_{K\in\mathcal{K}_a(P)}p(K\prec\tilde{K}\tilde{L}\mid\tilde{P}=P)>\frac{m}{a}.$$

Если соотношение $K\prec\tilde{K}\tilde{L}$ имеет место при нескольких различных K, то эти K можно расположить в цепочку так, что каждое слово, кроме последнего, будет началом следующего слова. Поэтому при

фиксированном значении $\tilde{P}$ из событий $K \prec \tilde{K}\tilde{L}$ для различных K, таких что, $P(\tilde{K}=K \& \tilde{P}=P)>0$, могут иметь место одновременно не более, чем $\mathfrak{ж}$ событий ($\mathfrak{ж}$ - степень вложенности начал для пары $\tilde{P}$, $\tilde{K}$). Следовательно, сумма вероятностей этих событий при условии $\tilde{P}=P$ не превосходит $\mathfrak{ж}$, значит, $\mathfrak{ж} > \frac{m}{a}$ и $m < a\mathfrak{ж}$. Итак, число элементов в множестве $\mathcal{K}_a(P)$ меньше $a\mathfrak{ж}$. Аналогично докажем, что число элементов в множестве $\mathcal{L}_b(Q)$ меньше $b\lambda$.

5°. Итак, в предположении, что события $\mathcal{A}(\tilde{P}\tilde{Q})=\tilde{K}\tilde{L}$ и $\tilde{t} \leqslant \bar{t}$ достоверны, мы, взяв произвольные рациональные a и b, бо́льшие I, построили для любых P, Q такие множество слов $\mathcal{K}_a(P)$ и $\mathcal{L}_b(Q)$, что $\mathcal{K}_a(P)$ содержит меньше $a\mathfrak{ж}$ элементов, $\mathcal{L}_b(Q)$ содержит меньше $b\lambda$ элементов и выполняется условие (IO). Снова рассмотрим произвольную четверку случайных слов $\tilde{P}$, $\tilde{Q}$, $\tilde{K}$, $\tilde{L}$ и обозначим теперь событие

$$\mathcal{A}(\tilde{P}\tilde{Q})=\tilde{K}\tilde{L} \,\&\, \tilde{t} \leqslant \bar{t}$$

через $\tilde{F}$. Повторим предыдущее рассуждение (пункты 2° - 4°), используя всюду вместо безусловных вероятностей вероятности при условии $\tilde{F}$ (т.е. изменив вероятности значений основной случайной переменной). Формулировка результата этого рассуждения останется прежней с той разницей, что (IO) примет вид

$$p(\tilde{K} \in \mathcal{K}_a(\tilde{P}) \vee \tilde{L} \in \mathcal{L}_b(\tilde{Q}) \mid \tilde{F}) \geqslant 1 - \frac{c''\bar{t}}{\ln a \ln b}.$$

Пусть при некотором рациональном положительном p_0 и целом положительном t_0 выполняется (I). Тогда, полагая

$$\bar{t} = 2c't_0,$$

получим, в силу (6), что $p(\tilde{F}) \geqslant p_0$. Отсюда следует, что

$$p(\tilde{K} \in \mathcal{K}_a(\tilde{P}) \vee \tilde{L} \in \mathcal{L}_b(\tilde{Q})) \geqslant p_0\left(1 - \frac{c''\bar{t}}{\ln a \ln b}\right).$$

Пусть φ - функция покрытия $\tilde{K}$ относительно $\tilde{P}$, а ψ - функция покрытия $\tilde{L}$ относительно $\tilde{Q}$. Имеем

$$p(\tilde{K} \in \mathcal{K}_a(\tilde{P})) \leq \varphi(]a\varkappa[),$$

$$p(\tilde{L} \in \mathcal{L}_b(\tilde{Q})) \leq \psi(]b\lambda[),$$

следовательно,

$$\frac{\varphi(]a\varkappa[)+\psi(]b\lambda[)}{p_0} \geq 1-\frac{2c'c''t_0}{\ln a \ln b}.$$

Пусть x, y и ε – произвольные рациональные числа из $(0,1)$, удовлетворяющие условию

$$x+y=p_0(1-\varepsilon).$$

Положим $a=\frac{\Phi(x)}{\varkappa}$ и $b=\frac{\psi(y)}{\lambda}$, где Φ и ψ – соответствующие функции разнообразия. Тогда для $a>1$ и $b>1$ имеем $\varphi(]a\varkappa[) \leq x$, $\psi(]b\lambda[) \leq y$,

$$1-\varepsilon \geq 1-\frac{2c'c''t_0}{\ln a \ln b},$$

$$t_0 \geq \frac{1}{2c'c''} \varepsilon \ln \frac{\Phi(x)}{\varkappa} \ln \frac{\psi(y)}{\lambda}.$$

Остается положить $C=\frac{1}{2c'c''}$, и теорема доказана.

ЛИТЕРАТУРА

1. Барздинь Я.М. Сложность распознавания симметрии на машинах Тьюринга. "Проблемы кибернетики", 1965, вып.15,245-248.
2. Марков А.А. Теория алгорифмов, "Тр.Матем.ин-та АН СССР", 1954. 42.
3. Цейтин Г.С. Приведенная форма нормальных алгорифмов и теорема о линейном ускорении. Настоящий сборник, 234-242.