Доклады Академии наук СССР
1971. Том 196, № 1

УДК 517.11

МАТЕМАТИКА

Ю. Я. БРЕЙТБАРТ

ОБ АВТОМАТНОЙ И «ЗОННОЙ» СЛОЖНОСТИ ПРЕДИКАТА «БЫТЬ k-й СТЕПЕНЬЮ ЧИСЛА»

(Представлено академиком П. С. Новиковым 27 V 1970)

1°. Пусть $\Sigma = \langle 0, 1, \ldots, (p-1)\rangle$, где p — простое число. Рассмотрим множество Σ^* слов в алфавите Σ, причем λ — пустое слово и $\lambda \in \Sigma^*$. Каждое такое слово (за исключением пустого) можно рассматривать как p-ичную запись некоторого натурального числа. Таким образом, если $x = a_1 \ldots a_t \in \Sigma^*$, то $|x|$ будет обозначать натуральное число, p-ичной записью которого является слово x. На множестве Σ^* для любого $k \geqslant 2$ определим предикат * $T_k(x)$ следующим образом:

если $x = \lambda$, то $T_k(x) = 0$;

если $x \neq \lambda$, то

$$T_k(x) = 1 \Leftrightarrow \exists y (y \in \Sigma^* \& |y|^k = |x|). \tag{1}$$

В настоящей заметке доказывается, что всякий конечный автомат, распознающий $T_k(x)$ на словах длины, не превосходящей n, требует по порядку не меньше чем $p^{n/k}$ состояний. Как следствие этого результата, будет получена оценка зоны on-line (off-line) машины Тьюринга, распознающей предикат $T_k(x)$, причем в первом случае оценка является по порядку окончательной.

2°. $P(x)$ — некоторый предикат на Σ^* и $n \geqslant 1$. Обозначим Σ_n^* множество слов в алфавите Σ, длина которых не превосходит n. На Σ_n^* введем отношение

$$x \equiv {}_n y \Leftrightarrow \forall z (z \in \Sigma^* \& l(xz) \leqslant n \& l(yz) \leqslant n \supset P(xz) = P(yz)) \text{ **}. \tag{2}$$

Назовем слова $x, y \in \Sigma_n^*$ n-эквивалентными, если $x \equiv {}_n y$. Пусть $\psi_P(n)$ — число слов из Σ_n^*, не являющихся попарно n-эквивалентными для данного предиката P.

Теорема 1. *Для предиката* $T_k(x)$ $\psi_{T_k}(n) \geqslant p^{n/k}$.

Доказательство. Обозначим $B_p(k, n)$ множество нечетных чисел, являющихся вычетами k-й степени по $\bmod p^n$, причем, если $a \in B_p(k, n)$, то

$$0 < a \leqslant p^n - 1 \tag{3}$$

и сравнение $x^k \equiv a \pmod{p^n}$ имеет, по крайней мере, одно решение $x \equiv b \pmod{p^n}$, где

$$]p^{n/(k-1)} / \sqrt[k-1]{k}[\leqslant b < p^n \text{ ***}. \tag{4}$$

Лемма 1.

1. *Если k четное, то* $\|B_2(k, n)\| \geqslant 2^n / 4k$.
2. *Если k нечетное, то* $\|B_2(k, n)\| \geqslant 2^{n-1} - 2^{n/(k-1)}$.

Доказательство. Вначале мы сформулируем необходимые для доказательства три результата теории чисел (²).

---

* Предикат на Σ^* — всюду определенная функция типа $\Sigma^* \to (0, 1)$.

** $l(x)$ — длина слова x.

*** $]a[$ — наименьшее целое число, не меньшее чем a.

а) Для любого нечетного числа $0 < b \leqslant 2^n - 1$ найдутся такие целые

$$0 \leqslant u \leqslant 1, \quad 1 \leqslant v \leqslant 2^{n-2}, \tag{5}$$

что $b \equiv (-1)^u \cdot 5^v \pmod{2^n}$, причем, если $b_1 \neq b_2$, то $\langle u_1, v_1\rangle \neq \langle u_2, v_2\rangle$. Пара $\langle u, v\rangle$ называется индексом числа b и обозначается $\operatorname{ind} b$.

Будем говорить, что

$$\langle u_1, v_1\rangle \equiv \langle u_2, v_2\rangle \pmod{\langle m, n\rangle} \Leftrightarrow u_1 \equiv u_2 \pmod m \,\&\, v_1 \equiv v_2 \pmod n. \tag{6}$$

б) $a \equiv b \pmod{2^n} \Leftrightarrow \operatorname{ind} a \equiv \operatorname{ind} b \pmod{\langle 2, 2^{n-2}\rangle}$.

в) $\operatorname{ind} a^m \equiv m \operatorname{ind} a \pmod{\langle 2, 2^{n-2}\rangle}$.

В силу а), б), в) имеет место система эквивалентностей:

$$x^k \equiv a \pmod{2^n} \Leftrightarrow \operatorname{ind} x^k \equiv \operatorname{ind} a \pmod{\langle 2, 2^{n-2}\rangle} \Leftrightarrow$$

$$\Leftrightarrow k \operatorname{ind} x \equiv \operatorname{ind} a \pmod{\langle 2, 2^{n-2}\rangle},$$

где x, a нечетные и $0 < a \leqslant 2^n - 1$.

Последнее сравнение по определению (6) эквивалентно системе

$$kx_1 \equiv u \pmod 2 \,\&\, kx_2 \equiv v \pmod{2^{n-2}}, \tag{7}$$

где $\langle u, v\rangle = \operatorname{ind} a$, $a\langle x_1, x_2\rangle = \operatorname{ind} x$.

В случае четного k (7) имеет решение тогда и только тогда, когда

$$u = 0, \quad d \mid v, \tag{8}$$

где $d = (k, 2^{n-2})$. Нетрудно видеть, что общее число таких пар $\langle u, v\rangle$, где u и v удовлетворяют условиям (8) и (5), не меньше чем $2^{n-2}/k$. Пусть $a_1, \ldots, a_t$ — все такие нечетные числа среди чисел от 1 до $2^n - 1$, индексы которых удовлетворяют условиям (8). Тогда для каждого такого a сравнение $x^k \equiv a \pmod{2^n}$ имеет, по крайней мере, два решения $x \equiv b \pmod{2^n}$ и $x \equiv 2^n - b \pmod{2^n}$, и тогда, по крайней мере, одно из этих решений не меньше 2^{n-1} и, следовательно, все $a_1, \ldots, a_t \in B_2(k, n)$, и в случае четного k лемма доказана.

В случае нечетного k система (7) имеет решение для любой пары $\langle u, v\rangle$, удовлетворяющей (5). Таким образом, любое нечетное число $0 < b \leqslant 2^n - 1$ является вычетом k-й степени по $\bmod 2^n$. Выберем из этих чисел такие, вычеты k-й степени которых удовлетворяют (4). Так как между всеми нечетными числами от 1 до $(2^n - 1)$ и вычетами k-й степени существует, в силу доказанного, взаимно однозначное соответствие, то тем самым лемма полностью доказана.

В [2] доказано: если $p > 2$ и p — простое, то число вычетов k-й степени по $\bmod p^n$ равно $(p^n - p^{n-1})/d$, где $d = (k, (p^n - p^{n-1}))$, откуда следует

Лемма 1′. *Если k четное и $p > 2$ простое, то $\|B_p(k, n)\| \geqslant (p^n - p^{n-1})/k$. Если k нечетное и $p > 2$ простое, то $\|B_p(k, n)\| \geqslant (p^n - p^{n-1})/k - p^{n/(k-1)}$.*

Лемма 2. $\psi_{T_k}(kn) \geqslant \|B_p(k, n)\|$, *где p простое.*

Доказательство. Пусть $a \in B_p(k, n)$; тогда существует такое b, удовлетворяющее (4), что $b^k \equiv a \pmod{p^n}$; тогда $b^k = a + p^n t$ и, в силу (4), получаем

$$p^{kn} > a + p^n t \geqslant p^{kn/(k-1)} / \sqrt[k-1]{k^k}, \tag{9}$$

откуда следует

$$p^{(k-1)n} > t \geqslant p^{n/(k-1)} / \sqrt[k-1]{k} - 1. \tag{10}$$

Таким образом, доказано, что для любого вычета a из $B_p(k, n)$ найдется такое t, удовлетворяющее (10), что $a + p^n t$ в точности k-я степень некото-

рого числа, лежащая в пределах (9). Покажем далее, что для данного t не найдется числа $c \in B_p(k, n)$ такого, что $c \neq a$ и $c + p^n t$ — также в точности k-я степень. В самом деле, предположим, что это не так. Пусть c_1 такое, что $c_1 + p^n t$ есть d^k. Пусть, для определенности $d > b$; тогда $d^k - b^k \geqslant kb^{k-1}$ и, в силу (7), $kb^{k-1} \geqslant p^n$, но $|a - c_1| < p^n$, так как a и c_1 — нечетные числа в пределах от 1 до $p^n - 1$. Получили противоречие.

Таким образом, для каждого $a \in B_p(k, n)$ найдется такое t, удовлетворяющее (10), что $a + p^n t = b^k$ для некоторого $1 \leqslant b < p^n$ и $c + p^n t \neq x^k$ ни при каком $c \neq a$, где $c \in B_p(k, n)$. Пусть теперь $\alpha_1 \ldots \alpha_r$ — слова, являющиеся p-ичной записью чисел $a_1 \ldots a_r$ соответственно, где $r = \|B_p(k, n)\|$, а $\gamma_1 \ldots \gamma_r$ — слова, являющиеся p-ичной записью таких $t_1 \ldots t_r$, что $a_i + p^n t_i = b_i^k$, и каждое из которых удовлетворяет (10). Тогда $\gamma_1 \ldots \gamma_r$ являются попарно не kn-эквивалентными, так как для каждого γ_i найдется такое продолжение α_i, что $\gamma_i \alpha_i$ есть p-ичная запись числа, являющегося k-й степенью, но $\gamma_i \alpha_i$ не является таковой при любом $j \neq i$. Заметив, что $l(\gamma_i \alpha_i) = kn$, мы завершим доказательство леммы.

Из лемм 1, 1′, 2 следует утверждение теоремы 1 для $n = kn_1$. Пусть теперь $kn_1 < n \leqslant k(n_1 + 1)$. Тогда $n = kn_1 + c$, где $1 \leqslant c \leqslant k - 1$ и $n - c = kn_1$. Следовательно, $\psi_{T_k}(n) \geqslant \psi_{T_k}(n - c) \geqslant p^{n/k}$.

3°. Конечный автомат (к.а.) $\mathfrak{B}$ в алфавите Σ есть четверка $\mathfrak{B} = \langle Q, \delta, q_0, F \rangle$, где Q — конечное непустое множество (состояния $\mathfrak{B}$), $F \subseteq Q$, $q_0 \in Q$, δ — всюду определенная функция типа $Q \times \Sigma \to 0$ (функция переходов $\mathfrak{B}$). Функция переходов δ может быть индуктивно продолжена на $Q \times \Sigma^*$ функцией $\bar{\delta}$ следующим образом:

$$\bar{\delta}(q, \lambda) = q; \quad \bar{\delta}(q, xa) = \delta(\bar{\delta}(q, x), a), \quad \text{где } x \in \Sigma^*, \quad a \in \Sigma.$$

Будем говорить, что к.а. $\mathfrak{B}$ допускает предикат $P(x)$, если

$$\forall x (x \in \Sigma^* \supset (P(x) = 1 \Leftrightarrow \bar{\delta}(q_0, x) \in F)).$$

Будем говорить, что к.а. $\mathfrak{B}$ n-допускает предикат $P(x)$, если

$$\forall x (x \in \Sigma_n^* \supset (P(x) = 1 \Leftrightarrow \bar{\delta}(q_0, x) \in F)). \tag{11}$$

Пусть $\varphi_p(n)$ — наименьшее возможное число такое, что существует к.а. $\mathfrak{B}$ с $\varphi_p(n)$-состояниями, n-допускающий $P(x)$.

Лемма 3. $\varphi_p(n) \geqslant \psi_p(n)$.

Доказательство. Предположим, что $\mathfrak{B} = \langle Q, \delta, q_0 F \rangle$ к.а., n-допускающий $P(x)$ и имеющий $\varphi_p(n)$ состояний. Предположим, что $\varphi_p(n) < \psi_p(n)$. Тогда найдутся такие x и y из Σ^*, что $x \not\equiv_n y$, но $\bar{\delta}(q_0, x) = \bar{\delta}(q_0, y)$. Следовательно, для любого $z \in \Sigma^*$

$$\bar{\delta}(q_0, xz) = \bar{\delta}(q_0, yz). \tag{12}$$

Но, в силу (2), найдется такое $z \in \Sigma^*$, что $l(xz) \leqslant n$ и $l(yz) \leqslant n$, но $P(xz) \neq P(yz)$. Это противоречит (12) в силу (11). Следовательно, $\varphi_p(n) \geqslant \psi_p(n)$.

Следствие 1. *Для любого $k > 1$ предикат $T_k(x)$ не является допустимым к.а. и $\varphi_{T^k}(n) \geqslant p^{n/k}$.*

4°. м.Т. есть устройство, имеющее: входную ленту, на которой записывается входное слово, и головку на ней, которая может сдвигаться вправо, влево или оставаться на месте по входу, но не может менять символов на нем; рабочую ленту, двусторонне бесконечную, на которой также имеется головка, и она может по рабочей ленте сдвигаться в любом направлении или оставаться на месте и менять обозреваемый символ. Кроме того, машина имеет управляющее устройство с конечным числом состояний. Эта м.Т. полностью определяется следующими данными: Σ — конечным непустым входным алфавитом, $\sigma, \tau \notin \Sigma$ — конечными маркерами, Γ — алфавитом рабочей ленты, $B \in \Gamma$ — пустым символом на рабочей ленте, Q — конечным

непустым множеством состояний, $q_0 \in Q$ — начальным состоянием, δ: $Q \times (\Sigma \cup \{\sigma\} \cup \{\tau\}) \times \Gamma \to Q \times \Gamma \times \{-1, 0, 1\}^2$ — функцией движения и $F \subseteq Q$ — подмножеством выделенных состояний.

Если $\delta(q_i, a_k, X_j) = q_l, Y_m, d_1, d_2$, то м.Т., находясь в состоянии q_i, обозревая на входной ленте a_k и на рабочей X_j, переходит в состояние q_l, на рабочей ленте в обозреваемой клетке записывает Y_m и сдвигается на одну клетку вправо, влево, или остается на месте ($d_1 = 1, -1, 0$), а по входной ленте сдвигается вправо, влево или остается на месте $d_2 = (1, -1, 0)$. Пусть $\mathfrak{A}$ — off-line м.Т. и $x \in \Sigma^*$. Пусть $\mathfrak{A}$ в начальном состоянии, на входной ленте записано $\sigma x \tau$, и считывающая головка обозревает на ней σ. На рабочей ленте записано B, и головка обозревает B. Тогда, применяя функцию движений, м.Т. начинает перерабатывать слово x и останавливается в тот момент, когда по входной ленте она впервые попала на τ, и в следующий момент функция движений предписывает ей сдвинуться вправо.

В дальнейшем мы рассматриваем лишь такое м.Т., которые останавливаются на любом слове из Σ^*. Мы скажем, что $P(x)$ допускается м.Т. $\mathfrak{A}$, если: $\forall x (P(x) = 1 \Leftrightarrow \mathfrak{A}$ останавливается на x в состоянии из $F)$. Мы скажем, что off-line м.Т. работает с зоной, не превосходящей $L(n)$, если для каждого входа x, длины не превосходящей n, число различных квадратов рабочей ленты, посещаемой м.Т. при переработке x, не превосходит $L(n)$. Off-line м.Т. называется on-line м.Т., если $\delta(q_i, a_k, X_j) = q_l Y_m, d_1, d_2$ и $d_2 \neq -1$. Предикат называется $L(u)$-допустимым, если существует м.Т., работающая с зоной не превосходящей $L(n)$.

Лемма 4 ([1]). *Если $P(x)$ не допускается к.а., то для всякой $L(n)$ такой, что $P(x)$ является $L(n)$-допустимым на* on-line (off-line) *м.Т., выполняется следующее*: $L(n) \geqslant \log \varphi_p(n) (\log \log \varphi_p(n))$.

Следствие 2. *Если $T_k(x)$ является $L(n)$-допустимым на* on-line *м.Т., то $L(n) \geqslant n$.*

Следствие 3. *Если $T_k(x)$ является $L(n)$-допустимым на* off-line *м.Т., то $L(n) \geqslant \log n$.*

Теорема 2. *$T_k(x)$ является n-допустимым на* on-line *м.Т.*

Специальное конструкторское бюро
биофизической аппаратуры и электронных машин
Москва

Поступило
26 V 1970

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] R. Karp, J. Assoc. Comp. Machinery, 14, № 3, 478 (1967). [2] И. М. Виноградов, Основы теории чисел, «Наука», 1965.