ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ՏԵՂԵԿԱԳԻՐ
ИЗВЕСТИЯ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР
Մաթեմատիկա XIII, № 2, 1978 Математика

Г. З. САРКИСЯН

ЭФФЕКТВНАЯ ВЫЧИСЛИМОСТЬ АРИФМЕТИЧЕСКИХ ПРЕДИКАТОВ И ФУНКЦИЙ НА ОСНОВЕ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

В работе Р. Карпа [1] вводится определенное математическое уточнение интуитивного понятия дискретной математической задачи, эффективно разрешимой посредством реально осуществимого алгоритмического процесса; в качестве такого уточнения, в соответствии с тезисом Д. Эдмондса [1], рассматривается понятие предиката, разрешимого на детерминированной машине Тьюринга за полиномиальное время.

В работе Р. Карпа дано также математическое уточнение общего понятия задачи, решение которой связано с определенного типа перебором показательного объема; в качестве такого уточнения рассматривается понятие предиката, разрешимого на недетерминированной машине Тьюринга за полиномиальное время. (Классы предикатов и функций указанных типов мы будем обозначать, также как и в работе Р. Карпа, через P, NP, П).

В настоящее время неизвестно, имеет ли место $P = NP$, хотя естественно предполагать, что $P \neq NP$. Согласно результатам указанной работы Р. Карпа, равенство $P = NP$ равносильно принадлежности классу P некоторых предикатов (называемых полными проблемами), связанных с разрешимостью ряда широко известных задач дискретной математики.

Математические уточнения понятий эффективной разрешимости введенные в работе Р. Карпа, естественны в тех случаях, когда ставится вопрос о свойствах единого алгоритма, разрешающего рассматриваемую задачу для дискретных объектов любой, сколь угодно большой сложности.

Однако можно представить себе и такую ситуацию, когда нас интересует решение рассматриваемой задачи лишь для „дискретных объектов ограниченной сложности; так, например, рассматривая решение каких-либо дискретных задач на вычислительной машине, естественно рассматривать лишь такие задачи, записи которых могут быть хотя бы в принципе введены в вычислительную машину (разница между указанными постановками задач рассмотрена в работе А. Мейера [3]). При такой постановке, по-видимому, более естественно рассматривать не единый алгоритм для решения задачи применительно к любым объектам, а брать в отдельности алгоритмы, решающие задачу для объектов каждой заданной сложности.

В этой работе вводятся математические уточнения указанных выше интуитивных понятий, отличающиеся от уточнений Р. Карпа и основанные на рассмотрении трудности разрешения дискретных задач по отдельности для дискретных объектов каждой фиксированной сложности. В качестве алгоритмического аппарата при рассмотрении разрешимости задач взят аппарат схем из функциональных элементов с обычным пониманием их сложности. Вводятся классы предикатов S и ES, аналогичные классам Р. Карпа P и NP, но отличающиеся от них (например, предикаты класса S могут быть даже не рекурсивными). Устанавливается, что классы S и ES обладают свойствами, аналогичными свойствам классов P и NP.

Остается открытым вопрос о том, имеет ли место $S = ES$, однако доказывается, что если $S \neq ES$ то $P \neq NP$ (вопрос об обратной импликации тоже остается открытым).

Устанавливается также, что если хотя бы один из предикатов, указанных в работе Р. Карпа в качестве полных проблем, принадлежит S, то $S = ES$.

Через $\sum^*$ будем обозначать множество всех конечных слов в алфавите $\{0, 1\}$. Будем рассматривать предикаты, определенные для множества $\sum^*$. Через $l(p)$ будем обозначать длину слова p.

Будем рассматривать схемы из функциональных элементов (или, сокращенно, ф-схемы), в каком-нибудь фиксированном полном базисе, например, $(\&, \vee, \neg)$ ([4], [5]).

Посредством $S^l_{k_1, \dots, k_n}$ будем обозначать функциональную схему с $k_1 + \dots + k_n$ входами и l выходами. Через $\overline{S}^l_{k_1, \dots, k_n}$ будем обозначать булев оператор, реализуемый ф-схемой $S^l_{k_1, \dots, k_n}$, а через $\|S^l_{k_1, \dots, k_n}\|$ — сложность ф-схемы $S^l_{k_1, \dots, k_n}$ (т. е. количество ее элементов и входов).

Говоря „полином", в дальнейшем всюду будем иметь в виду полином от одной переменной с целыми коэффициентами.

Определение 1. Предикат $p(x_1, \dots, x_n)$ называется *F-полиномиально разрешимым*, если существует полином T такой, что для всяких $m_1, \dots, m_n$ существует ф-схема $S^1_{m_1, \dots, m_n}$, удовлетворяющая условию

$$\|S^1_{m_1, \dots, m_n}\| \leq T(m_1 + \dots + m_n)$$

и такая, что при любых $x_1, \dots, x_n \in \sum^*$, если $l(x_1) = m_1, \dots, l(x_n) = m_n$, то

$$\overline{S}^1_{m_1, \dots, m_n}(x_1, \dots, x_n) = \begin{cases} 0, \text{ если } \neg p(x_1, \dots, x_n); \\ 1, \text{ если } p(x_1, \dots, x_n). \end{cases}$$

Класс полиномиально разрешимых предикатов будем обозначать через S.

Определение 2. Предикат $q(x_1, \dots, x_n)$ называется предикатом *F-переборного типа*, если существует F-полиномиально разрешимый предикат $p(y, x_1, \dots, x_n)$ и полином T, такие что

$$q(x_1, \cdots, x_n) \equiv \exists\, y_{l(y)=T(l(x_1)+\cdots+l(x_n))}\, p(y, x_1, \cdots, x_n).$$

Класс всех предикатов **F**-переборного типа будем обозначать через ES.

Через $D(x, t)$ будем обозначать такую функцию, что для каждого слова x $(x \in \Sigma^*)$ и для каждого натурального числа t имеет место соотношение:

$$D(x, t) = \begin{cases} \underbrace{0\,0 \cdots\cdots\cdots 0}_{2t \text{ раз}}, & \text{если } l(x) > t; \\ x\underbrace{0\cdots 0}_{t-l(x) \text{ раз}}\ \underbrace{1\cdots 1}_{l(x) \text{ раз}}\ \underbrace{0\cdots 0}_{t-l(x) \text{ раз}}, & \text{если } l(x) \leqslant t. \end{cases}$$

Определение 3. Пусть f есть функция типа $(\Sigma^*)^n \to \Sigma^*$. Будем говорить, что функция f ***F**-вычислима*, если существует полином T такой, что для всяких $m_1, \cdots, m_n$ существует ф-схема $S^{2t}_{m_1, \cdots, m_n}$, где

$$t = \max_{\substack{l(x_1)=m_1 \\ \cdots\cdots \\ l(x_n)=m_n}} l(f(x_1, \cdots, x_n)),$$

удовлетворяющая условиям

$$\|S^{2t}_{m_1, \cdots, m_n}\| \leqslant T(m_1 + \cdots + m_n) \quad \text{и}$$

$$\forall x_{1\, l(x_1)=m_1}\, \forall x_{2\, l(x_2)=m_2} \cdots \forall x_{n\, l(x_n)=m_n} (\overline{S}^{2t}_{m_1, \cdots, m_n}(x_1, \cdots, x_n) =$$

$$= D(f(x_1, \cdots, x_n), 2t)).$$

Класс всех **F**-вычислимых функций обозначим через F.

Легко видеть, что предикат p принадлежит классу S в том и только в том случае, когда его характеристическзя функция принадлежит классу F.

Определение 4. Пусть $p_1(x_1, \cdots, x_n)$ и $p_2(x_1, \cdots, x_r)$ — предикаты, определенные на множестве Σ^*. Скажем, что „p_1 ***F**-сводится к* p_2" ($p_1 \triangleright p_2$), если существуют n-местные функции $f_1, f_2, \cdots, f_r \in F$ такие, что при любых $x_1, \cdots, x_n \in \Sigma^*$

$$p_2(f_1(x_1, \cdots, x_n), \cdots, f_r(x_1, \cdots, x_n)) \Longleftrightarrow p_1(x_1, \cdots, x_n).$$

Определение 5. Пусть $\{a_0, \cdots, a_m\}$, $\{q_0, \cdots, q_n\}$ — внешний и внутренний алфавит машины Тьюринга A. Зафиксируем некоторое взаимно однозначное соответствие между символами $a_0, \cdots, a_m, q_0, \cdots$ $\cdots, q_n$ и некоторыми булевыми векторами длины r. Вектор, соответствующий символу a_i или q_j, будем называть *кодом* этого символа и обозначать через $K_r(a_i)$, или $K_r(q_j)$; условимся, что $K_r(a_0)$ есть нулевой булевый вектор.

Двоичным r-кодом масштаба l конфигурации $a_{j_1} \cdots a_{j_{t-1}} q_i a_{j_t} \cdots$ $\cdots a_{j_k}$ машины A, где $k \leqslant l-1$, назовем булев вектор, получаемый посредством соединения кодов

$$K_r(a_{j_1})\,K_r(a_{j_2})\cdots K_r(a_{j_{l-1}})\,K_r(q_l)\,K_r(a_{j_l})\cdots K_r(a_{j_k})\,\underbrace{K_r(a_0)\cdots K_r(a_0)}_{l-k-1\ \text{раз}},$$

этот код будем обозначать через

$$K_r^l(a_{j_1}\cdots a_{j_{l-1}}q_l\,a_{j_l}\cdots a_{j_k}).$$

Лемма 1. *Если* $p\in P$, *то* $p\in S$.

Доказательство. Метод доказательства аналогичен доказательству теоремы Кука [2], а именно, строится ф-схема, распознающая истинность p на словах ограниченной длины, аналогично тому, как в теореме Кука вопрос об истинности предиката p на словах ограниченной длины приводился к тождественной истинности некоторой дизъюнктивной нормальной формы.

Для простоты будем считать, что p есть одномерный предикат. Пусть $p\in P$, это значит, что существует детерминированная машина Тьюринга A с алфавитами $\{a_0,\cdots,a_m\}$, $\{q_0,\cdots,q_n\}$, которая распознает предикат p за полиномиальное время, то есть, машина A распознает предикат p, и существует такой полином T, что для каждого слова $x\in\sum^*\ t(x)\leqslant T(l(x))$, (где $t(x)$ — количество шагов работы A, исходя из входного слова x).

Пусть $D_l=(c^l_{i_1},\ c^l_{i_2},\cdots,\ c^l_{i_{k_l}})$ при $l=1,\ 2,\cdots,t(x)$ суть конфигурации, получаемые в процессе работы машины A при распознавании значения p на слове x.

Нам потребуется ф-схема, которая по каждому W коду конфигурации D_l (где $l<t(x)$) машины A в масштабе

$$d\ (\text{где}\quad d=\max_{l(x)=m}\ \max_{l=1,\cdots,t(x)} k_l;\ w=]\log_2(m+n+2)[)$$

дает код непосредственно следующей за D_l конфигурации D_{l+1} в том же масштабе. Пусть $K_w^d(D_l)=K_1K_2\cdots K_d$ для некоторого

$$l<t(x),\ K_w^d\ (D_{l+1})=K_1'K_2'\cdots K_d'.$$

Легко видеть, что при любом i, $1<i<d-1$ символ K_i' однозначно определяется (на основании программы рассматриваемой машины) символами K_{i-1}, K_i, K_{i+1}, K_{i+2}, кроме того символ K_1', однозначно определяется символами K_1, K_2, K_3; K_{d-1}' — символами K_{d-2}, K_{d-1}, K_d; K_d' — символами K_{d-1}, K_d. Пользуясь этим, построим ф-схему S_{4w}^w, которая по значениям K_{i-1}, K_i, K_{i+1}, K_{i+2} (или по сокращенным наборам значений для K_1', K_{d-1}', K_d') позволяет найти K_i'. Для одновременного нахождения всех K_i' $i=1,\cdots,d$ теперь достаточно соединить параллельно d схем S_{4w}^w и для нахождения последней конфигурации, исходя из начальной, нужно взять последовательно $\max\limits_{m=l(x)} t(x)$ схем. Если

сложность схемы S^w_{4w} обозначим через c (ясно, что S^w_{4w} и c зависят только от программы заданной машины, и не зависят от d и от входного слова x), в результате получается ф-схема со сложностью

$$cd \cdot \max_{l(x)=m} t(x);$$

эта схема будет в частности распознавать предикат p на словах длины $l(x)=m$. Так как $d \leqslant l(x)+T(l(x))$ и $t(x) \leqslant T(l(x))$, то сложность ф-схемы не превосходит

$$c \cdot T(l(x))\,[l(x)+T(l(x))].$$

Эта ф-схема представлена в блок-схеме 1 (рис. 1), где каждый

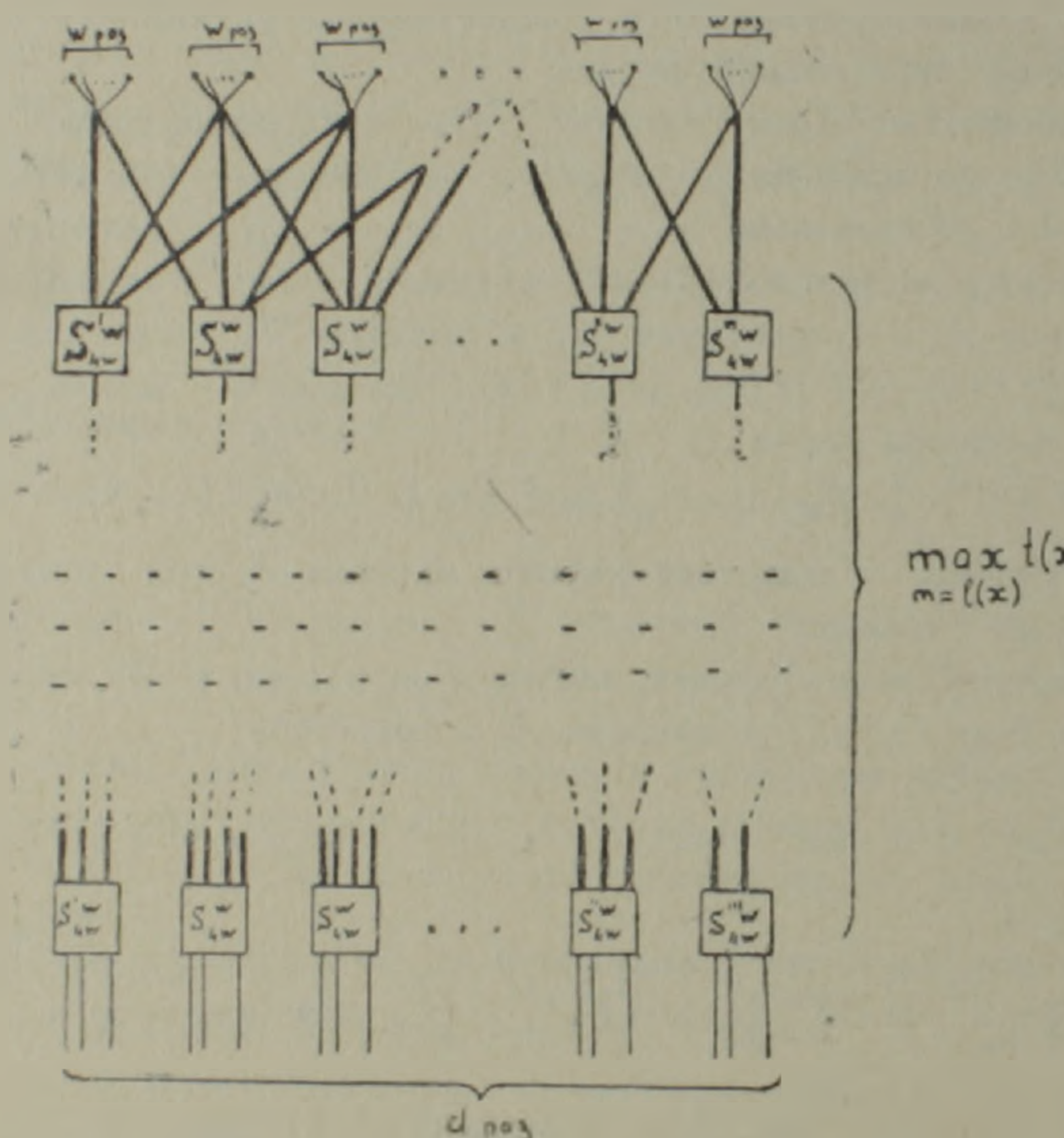

Рис. 1.

вход и выход, нарисованные жирными линиями, надо понимать как пучок, состоящий из w соединений.

Лемма доказана.

Лемма 2. *Предикат p представим в виде*

$$\exists x_{l(x)=T(l(y))}\, r(x, y) \tag{1}$$

(где $r \in S$, T — некоторый полином) в том и только в том случае, когда его можно представить в виде

$$\exists x_{l(x)\leqslant T'(l(y))}\, r'(x, y), \tag{2}$$

где $r' \in S$, T' — некоторый полином.

Доказательство. Предположим, что p представляется в виде (1)

$$p(y) \equiv \exists x_{l(x)=T(l(y))}\, r(x, y).$$

Легко проверить, что

$$p(y) \equiv \exists x_{l(x) \leqslant T(l(y))}\, r'(x, y),$$

где $r'(x, y) = r(x, y) \,\&\, (l(x) = T(l(y)))$.

Докажем обратное. Пусть

$$p(y) \equiv \exists x_{l(x) \leqslant T(l(y))}\, r(x, y)$$

и пусть x—слово в алфавите $\{0, 1\}$, и $l(x) \leqslant T(l(y))$. Обозначим через $\bar{x}$ слово $x * \underbrace{00 \cdots 0}_{T(l(x)) - l(x) - 1 \text{раз}}$ в алфавите $\{0, 1, *\}$. Перекодируем 0; 1; $*$ в алфавит $\{0, 1\}$ (например, 0 посредством 00, 1 посредством 11, $*$ посредством 01) и код слова, полученный в результате указанной перекодировки букв в слове $\bar{x}$, обозначим через $\bar{x}' \equiv \alpha_1\alpha_2 \cdots \alpha_{2T(l(y))}$.

Построим двуместную функцию φ, принадлежащую F и такую, что для любых x и y, если $l(x) \leqslant T(l(y))$, и $\bar{x}'$ есть слово, построенное исходя из x и y только что указанным образом, то $\varphi(\bar{x}', y) \equiv x$. Построим также двуместную функцию ψ, принадлежащую F и такую, что $\psi(z, y) = 0$, если $l(z) = 2T(l(y))$ и существует x такой, что $l(x) \leqslant T(l(y))$ и слово $\bar{x}'$, построенное указанным выше образом, исходя из x и y, совпадает с z, в противном случае $\psi(z, y) = 1$.

Легко проверить, что

$$p(y) \equiv \exists z_{l(z)=T'(l(y))}\, r'(z, y),$$

где $T'(n) = 2T(n)$,

$$r'(z, y) \equiv (\psi(z, y) = 0) \,\&\, r(\varphi(z, y), y).$$

Лемма доказана.

Лемма 3. *Если $p \in NP$, то $p \in ES$.*

Доказательство следует из определения класса NP, лемм 1 и 2.

Лемма 4. *Существует предикат p_0 такой, что $p_0 \in S$, но $p_0 \overline{\in} NP$.*

Доказательство. Ясно, что предикаты из классов P и NP рекурсивны.

Положим

$$p_0(x) = \begin{cases} И, & \text{если } x = 2^n - 1 \,\&\, p'(n) \\ Л & \text{в противном случае,} \end{cases}$$

где $p'(n)$ — какой-либо нерекурсивный предикат. Не существует машины Тьюринга, распознающей этот предикат. Но для каждого конкретного n существует ф-схема S_n^1, распознающая этот предикат и такая, что $\|S_n^1\| \leqslant 2n$. В самом деле, $p'(n) = И$ или $p'(n) = Л$, когда $p'(n) = Л$, то соответствующую схему можно представить в виде

$x_1 \& \neg x_1$, а когда $p'(n) = И$, то $p_0(x) = И$ при $l(x) = n$ только для $x = \underbrace{0\cdots 0}_{n \text{ раз}}$ и требуемую схему можно построить в виде $\neg x_1 \& \neg x_2 \& \cdots$ $\cdots \& \neg x_n$.

Лемма доказана.

Лемма 5. *Если $f \in \Pi$, то $f \in F$.*

Лемма доказывается таким же образом, как лемма 1, только к выходам схемы, построенной так же, как в доказательстве леммы 1, добавляется еще одна схема $C^{2w\cdot l_f^m}_{w\cdot l_f^m}$, которая преобразует код $K_w^{l_f^m}(f(x))$ в код $K_w^{l_f^m}(f(x))\, K_w^{l_f^m}(\underbrace{1 \cdots 1}_{l(f(x)) \text{ раз}})$ (здесь $l_f^m = \max\limits_{l(x)=m} l(f(x))$; $w =]\log_2(m+n+2)[$, где $m+n+2$ — мощность суммы внешнего и внутреннего алфавитов машины Тьюринга, реализующей функцию f).

Блок-схема ф-схемы, реализующей функцию f, показана на рис. 2.

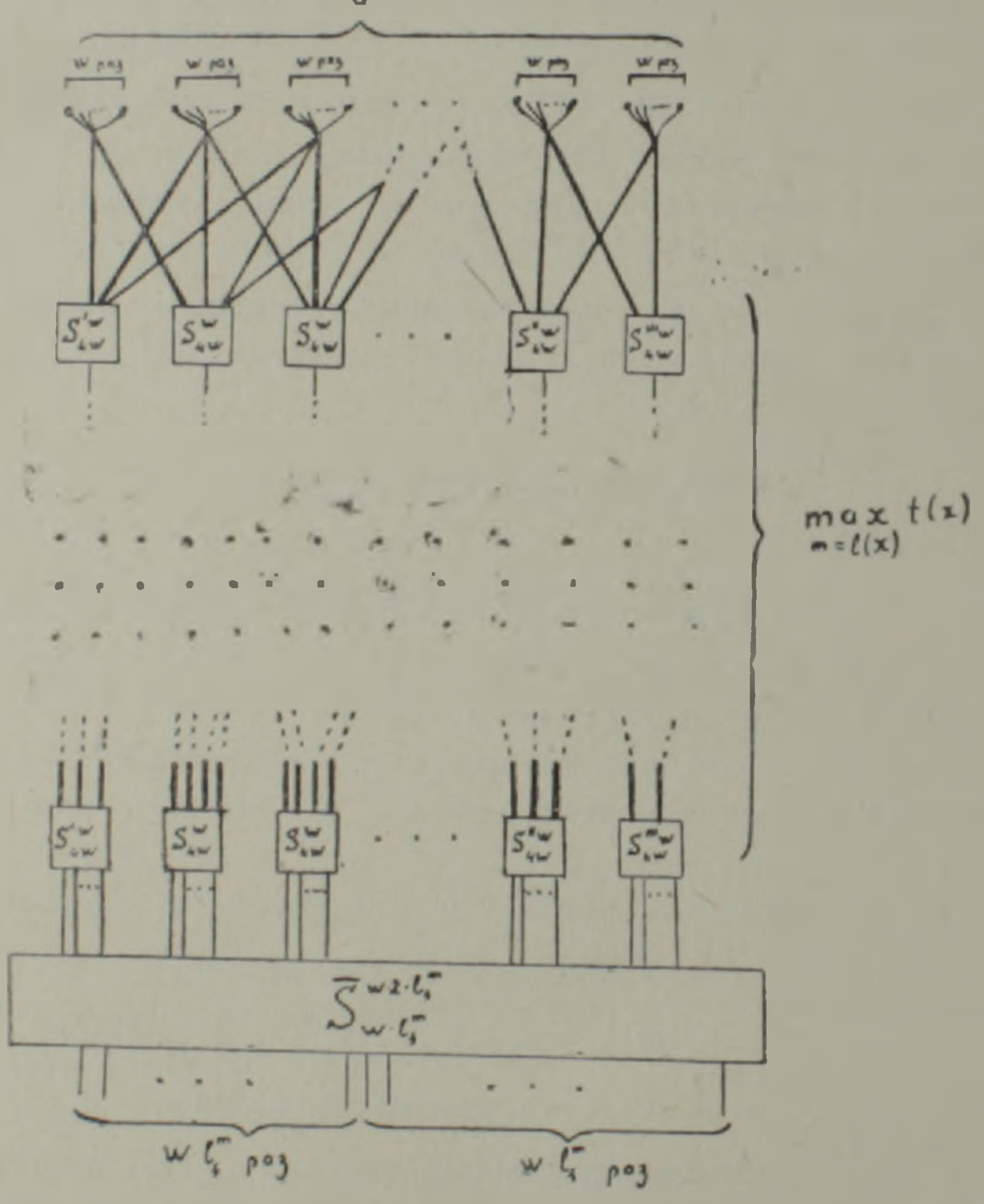

Рис. 2.

Определение 6. Предикат p называется **F**-полиномиально полным, если

1. $p \in ES$;
2. $\forall q\,(q \in ES \supset q \rhd p)$.

Лемма 6. *Если* $p_1 \infty p_2$, *то* $p_1 \vdash p_2$.

Доказательство проводится на основании леммы 5.

Лемма 7. *Если* $p_1 \rhd p_2$ & $p_2 \in S$, *то* $p_1 \in S$.

Для простоты будем считать, что p_1 и p_2 — одноместные предикаты. Пусть $p_1 \vdash p_2$. Это значит, что существует $f \in F$ такая, что

$$p_2(f(x)) <=> p_1(x)$$

и для всякого m существует ф-схема $(S'^{2l_f^m \cdot w}_{l_f^m \cdot w})'$ (где $l_f^m = \max\limits_{l(x)=m} l(f(x))$), реализующая функцию f для слов длины m.

Имеем $p_2 \in S$, а потому для всякого n существует ф-схема S_n^1, распознающая p_2 на словах длины n, при этом

$$\|(S'^{2l_f^m \cdot w}_{l_f^m \cdot w})'\| \leqslant T(l_f^m \cdot w),$$

$$\|S_n^1\| \leqslant T'(n),$$

где T и T' — некоторые полиномы.

Для разных слов x одинаковой длины m, длина $f(x)$ может быть разной, и величина $f(x)$ может изменяться от 0 до $\max\limits_{l(x)=m} l(f(x)) = l_f^m$, поэтому построим ф-схемы $S_0^1, S_w^1, \cdots, S_{wl}^1$, распознающие предикат p_2 на словах длины соответственно $0, w, 2w, \cdots, l_f^m w$.

Блок-схема общей схемы $S^1_{l_f^m \cdot w}$, распознающей $p_2(f(x))$, дана на

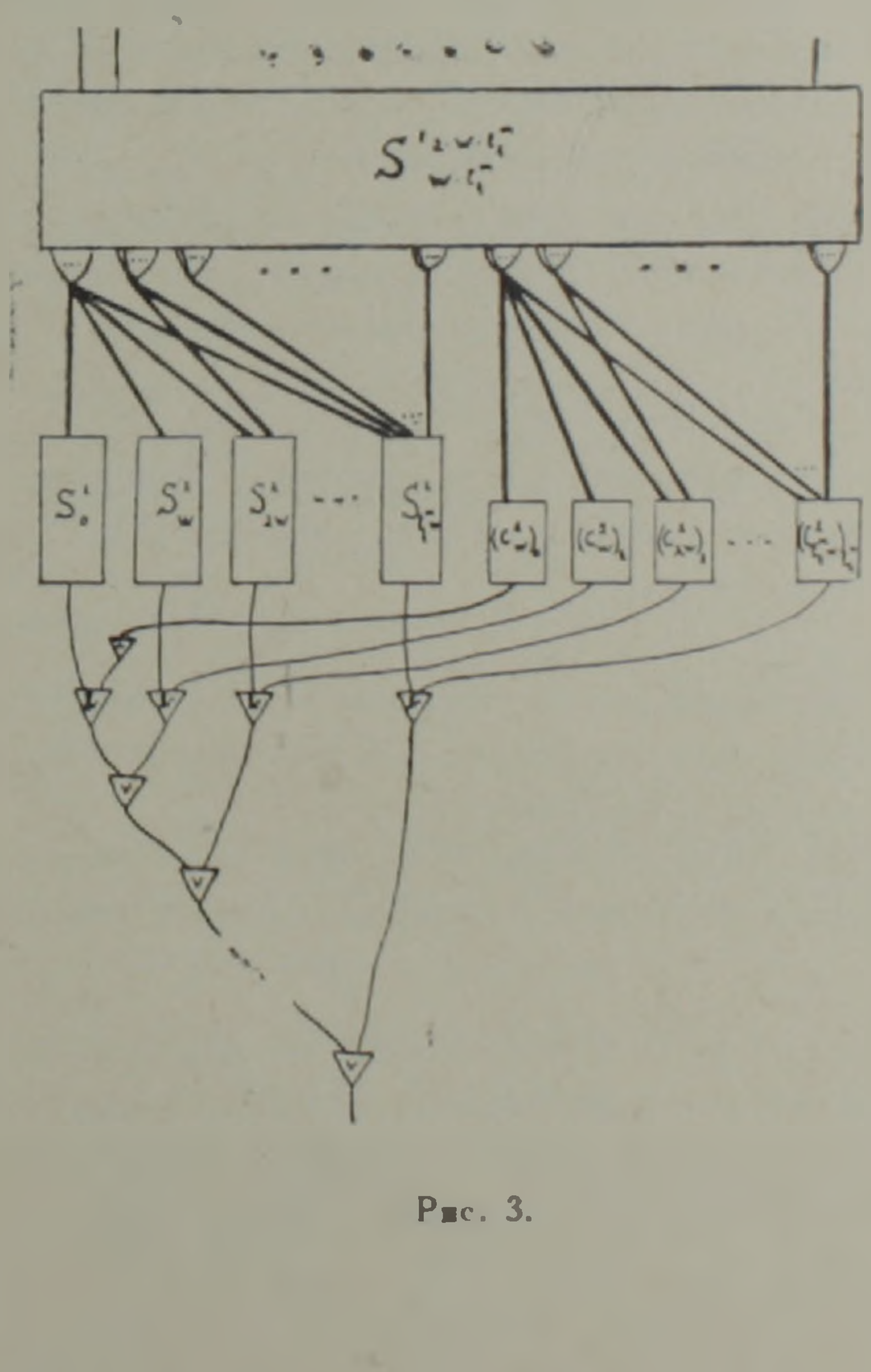

Рис. 3.

рис. 3. Каждая ф-схема $(c^{1}_{w l^m_f})_i$ проверяет равна ли $w \cdot i$ длина слова $K^{l(f(x))}_{w}(f(x))$; через c_i обозначим сложность этой схемы.

Сложность общей схемы $S^{l^m_f}_{w}$ не превосходит

$$T(l^m_f \cdot w) + T'(0) + T'(w) + T'(2w) + \cdots + T'(w \cdot l^m_f) +$$
$$+ c_1 + \cdots + c_{l^m_f} + 2 l^m_f - 1 = T^*(w \cdot l^m_f),$$

где T^* — некоторый полином.

Лемма доказана.

„Преобразованием Цейтина“ будем называть алгоритм Ц, который по всякой схеме s из функциональных элементов &, V, $\neg$ выдает конъюнктивную нормальную форму Ц(s), получаемую по следующим правилам (этот алгоритм введен Г. С. Цейтиным в работе [6], стр. 235—236):

1. Каждому элементу ф-схемы s сопоставляется некоторая пропозициональная переменная, при этом различным элементам сопоставляются различные переменные, входам схемы $x_1, \cdots, x_n$ сопоставляются они сами. Вместо „элемент, которому сопоставлена переменная z“, в дальнейшем будем говорить „элемент z“.

2. Наряду с пропозициональными переменными, каждому элементу ф-схемы сопоставляется некоторый набор элементарных дизъюнкций, составленных из этих элементов по следующим правилам: если элемент z_i есть элемент, реализующий конъюнкцию, входы которого соединены с выходами элементов z_j и z_h, то элементу z_i сопоставляются три элементарных дизъюнкции

$$(\neg z_j \vee \neg z_h \vee z_i),\ (\neg z_i \vee z_j),\ (\neg z_i \vee),\ (\neg z_h),$$

если элемент z_i есть элемент, реализующий дизъюнкцию, то ему сопоставляются три элементарные дизъюнкции

$$(\neg z_j \vee z_i),\ (\neg z_h \vee z_i),\ (\neg z_i \vee z_j \vee z_h),$$

если элемент z_i есть элемент, реализующий отрицание, вход которого соединен с выходом элемента z_j, то элементу z_i сопоставляются две элементарные дизъюнкции

$$(z_j \vee z_i),\ (\neg z_i \vee \neg z_j).$$

3. Берется конъюнкция всех построенных элементарных дизъюнкций и пропозициональной переменной, сопоставленной выходу схемы s; полученная к.н.ф. и есть Ц(s).

Лемма 8 (см. [6]). *Пусть f—булева функция, реализуемая схемой s, f'—булева функция, реализуемая формулой Ц(s). Тогда*

$$f \not\equiv 0 \Longleftrightarrow f' \not\equiv 0.$$

Доказательство легко следует из рассмотрений работы [6].

Будем считать, что зафиксирован какой-либо естественный способ кодирования пропозициональных формул в виде слов в Σ (например, такой же, какой принят в работе Р. Карпа [1]).

Лемма 9. *Для любой схемы s из функциональных элементов* $\&, \vee, \neg$

$$l(Ц(s)) \leqslant c_0 \|s\| \cdot \log \|s\|,$$

где c_0 — постоянная, зависящая лишь от принятого способа кодирования пропозициональных формул.

Доказательство очевидно на основании определения преобразования Ц.

Посредством ВЫП будем обозначать одноместный предикат, определенный на словах из Σ^* и такой, что ВЫП (x) имеет место тогда и только тогда, когда x есть код к.н.ф., определяющей булеву функцию, отличную от тождественного нуля.

Теорема 1. *Если $p \in ES$, то $p \rhd$ ВЫП.*

Доказательство. Пусть $p \in ES$. Для простоты будем предполагать, что p — одноместный предикат. Имеем

$$p(y) \equiv \exists x_{l(x) = T(l(y))} r(x, y),$$

где $r \in S$, и T — некоторый полином.

Для доказательства теоремы нам нужно доказать существование функции $f \in F$, такой что при любом y

$$\text{ВЫП}(f(y)) <=> p(y).$$

Опишем как строится слово $f(y_0)$ при заданном $y_0 \in \Sigma^*$. Обозначим $l(y_0)$ через n. Ввиду $r \in S$ существует ф-схема $S^1_{T(n)+n}$, распознающая истинность предиката r на парах слов (x, y), где $l(y) = n$, $l(x) = T(n)$, и такая, что $\|S^1_{T(n)+n}\| \leqslant T_1(n)$, где T_1 — некоторый полином. Теперь построим схему, распознающую предикат $r(x, y_0)$ на всевозможных словах x длины $T(n)$. Для получения этой ф-схемы к каждому входу схемы $S^1_{T(n)+n}$, соответствующему переменной $x_{T(n)+i}$, где $1 \leqslant i \leqslant n$, подключим схему вида $x_1 \& \neg x_1$ или $x_1 \vee \neg x_1$ в случаях, когда соответствующая буква $y_0^{(i)}$ слова $y_0 = y_0^{(1)} y_0^{(2)} \cdots y_0^{(n)}$ есть 0 или 1. Так построенную схему обозначим через $(S^1_{T(n)})'$. Ясно, что $\|(S^1_{T(n)})'\| \leqslant T_2(n)$, где T_2 — некоторый полином.

При помощи преобразования Цейтина построим к.н.ф. $Ц((S^1_{T(n)})')$. Согласно лемме 9, длина кода $Ц((S^1_{T(n)})')$ не превосходит

$$c_0 \|(s^1_{T(n)})'\| \cdot] \log (s + \|(s^1_{T(n)})'\|)[\leqslant T_3(n),$$

где T_3 — некоторый полином. Функция, которая данному y_0 ставит в соответствие код формулы $(Ц(S^1_{T(n)})')$, будет требуемой функцией f. В самом деле, соотношение

$$\text{ВЫП}(f(y_0)) \leftrightarrow p(y_0)$$

немедленно следует из построения функции f, принадлежность f классу F вытекает из того, что для каждого фиксированного n и для каждого y_0, где $l(y_0) = n$, код $Ц((S^1_{T(n)})')$ состоит из двух частей, из которых первая (соответствующая $\underset{\sim}{\text{Ц}}(S^1_{T(n)+n})$) не зависит от y_0 и имеет длину, не превосходящую $T_3(n)$, а вторая, соответствующая частям схемы $\underset{\sim}{\text{Ц}}((S^1_{T(n)})')$, добавленным при переходе от $S^1_{T(n)+n}$ к $S^1_{T(n)}$, получается из y_0 посредством очевидных преобразований, проводимых по отдельности для каждой буквы слова y_0 и реализуемых посредством однотипных функциональных схем с полиномиально ограниченной сложностью.

Теорема доказана.

Следствие 1. Предикат ВЫП F-полиномиально полный.

Следствие 2. Если ВЫП $\triangleright p$, то p F-полиномиально полный.

Следствие 3. Если предикат p полон в смысле определения 5 из [1], то p является F-полиномиально полным.

Следствие 4. Если некоторый предикат p полон в смысле определения 5 из [1] и $p \in S$, то $S = ES$.

Доказательство. Пусть p полон в смысле определения 5 из [1], это значит, что

$$\text{ВЫП} \infty p.$$

Согласно лемме 5, ВЫП $\triangleright p$, а так как $p \in S$, то, согласно лемме 6, ВЫП $\in S$, следовательно

$$S = ES.$$

Теорема 2. *Если*

$$S \neq ES, \text{ то } P \neq NP.$$

Доказательство. Предположим, что $S \neq ES$, это значит, что ВЫП $\overline{\in} S$, в противном случае, согласно лемме 7, было бы $S = ES$.

Из ВЫП $\overline{\in} S$ следует, что ВЫП $\overline{\in} P$ согласно лемме 1; из этого, в свою очередь, следует, что $P \neq NP$, поскольку ВЫП $\in NP$.

Теорема доказана.

Следствие. Если $P = NP$, то $S = ES$.

Краткое изложение результатов настоящей статьи было опубликовано в [7].

Ереванский государственный университет

Поступила 6.VII.1976

Գ. Զ. ՍԱՐԳՍՅԱՆ. Թվաբանական ֆունկցիաների և պրեդիկատների ֆունկցիոնալ տարրերից կազմված սխեմաներով որոշվող արդյունավետ հաշվարկելիություն (ամփոփում)

Սահմանվում են թվաբանական պրեդիկատների դասեր S և ES այնպես, որ S-ին պատկանող պրեդիկատները n երկարության երկուական կոդ ունեցող թվերի վրա իրացվում են $T(n)$ բարդության ֆունկցիոնալ սխեմաներով, որտեղ $T(n)$-ը ինչ-որ բազմանդամ է. ES դասերին պատկանող պրեդիկատները ստացվում են սահմանափակ գոյության քվանտորի միջոցով S դասի պրեդիկատներից։ Ապացուցվում է, որ S, ES և [1]-ում սահմանված P, NP դասերը նման հատկություններ ունեն, սակայն $S \neq P$, $ES \neq NP$։ Մասնավորապես ապացուցվում է, որ եթե $S \neq ES$, ապա $P \neq NP$։

C. Z. SARGISIAN. *The effective computability of arithmetic predicates and functions treated on the base of schemes from functional elements* (summary)

The classes S and ES of arithmetic predicates are defined so that predicates from S can be computed on the binary numbers of length n using schemes of functional elements with the complexity $T(n)$ where $T(n)$ is a polynom; the predicates belonging to ES are obtained from these belonging to S by the limited existential quantification. It is proved that S and ES have properties similar to these of the classes P and NP described in [1], however. $P \neq S$, $NP \neq ES$. For example, it is proved that if $S \neq ES$, then $P \neq NP$.

ЛИТЕРАТУРА

1. *R. M. Karp.* Reducibility among cambinatorial problems, complexity of computer computations, ed. by R. E. Miller and J. W. Thatcher plenum press, N. Y., 1972, 85—104. (Русский перевод: Карп Р. М. Сводимость комбинаторных проблем, „Кибернетический сборник", вып. 12, М., изд. „Мир", 1975).
2. *S. A. Cook.* The complexity of theorem-proving procedure, Proc. 3d Annual ACM Symposium on the Theory of Computing, Shaker Heights. Ohio, 1971, 151—159. (Русский перевод: Кук С. А. Сложность процедур вывода теорем. „Кибернетический сборник", вып. 12, М., изд. „Мир", 1975).
3. *A. R. Meyer.* The inherent computational complexity of Theories of Ordered Sets, A Brief Survey, Mass. Inst. of Technology, USA, 1974.
4. *О. Б. Лупанов.* О синтезе некоторых классов управляющих систем, сб. „Проблемы кибернетики", вып. 10, М., Физматгиз, 1963, 63—97.
5. *О. Б. Лупанов.* Об одном подходе к синтезу управляющих систем—принципе локального кодирования, сб. „Проблемы кибернетики", вып. 14, М., Физматгиз, 1965, 31—110.
6. *Г. С. Цейтин.* О сложности вывода в исчислении высказываний, Записки научных семинаров ЛОМИ, т. 8, Исследования по конструктивной математике и математической логике II, Л., 1968.
7. *Г. З. Саркисян.* Об одном понятии эффективной разрешимости предикатов, журн. „Молодой научный работник", 2 (22), Ереван, ЕГУ, 1975.