Отдельный оттиск

ПРОБЛЕМЫ КИБЕРНЕТИКИ

ВЫПУСК ДЕВЯТНАДЦАТЫЙ

МОСКВА · 1967

КЛАСС «ПОЧТИ ВСЕХ» ФУНКЦИЙ С НЕЛИНЕЙНОЙ СЛОЖНОСТЬЮ ПРИ РЕАЛИЗАЦИИ П-СХЕМАМИ

В. А. МАЛЫШЕВ

(МОСКВА)

В этой работе мы будем рассматривать реализацию функций алгебры логики формулами в базисе &, $\vee$, —. Под *сложностью* L (F) *формулы* F будем понимать число вхождений переменных в нее, под *сложностью* L (f) *функции* f — минимум сложности всех реализующих ее формул.

В работах [1] и [2] построены примеры функций алгебры логики с нелинейной относительно числа переменных сложностью. Представляет интерес задача о выделении таких «функциональных» свойств функций алгебры логики, по выполнению или невыполнению которых сразу можно было бы судить о сложности функции. Здесь выделяется одно такое свойство, называемое дифференцируемостью порядка m, доказывается, что при достаточно малом m им обладают «почти все» функции от n переменных (теорема 1), и выводится нижняя нелинейная оценка сложности функций, обладающих этим свойством (теорема 2).

Доказательство теоремы 1 изложено в части II работы, а доказательство теоремы 2— в части III.

I

В согласии с терминологией из работы [3] назовем *производной порядка* m *функции* f $(x_1, \ldots, x_k)$ любую функцию, полученную из функции f подстановкой некоторых констант на место некоторых m переменных. Функцию от n переменных назовем *дифференцируемой порядка* m $(m < n)$, если любая ее производная порядка m существенно зависит от $n - m$ переменных. Класс дифференцируемых функций порядка m $(m < n)$ от n переменных обозначим $W_{n,m}$. Число функций из этого класса обозначим символом $w_{n,m}$.

Очевидно, что $W_{n,m} \supset W_{n,m+1}$ при $2 < m + 1 < n$. Из приведенного ниже примера видно, что $W_{n,m} \neq W_{n,m+1}$ ни при каком m.

Пример. Функция $f_k(x_1, \ldots, x_n) = \sum x_{i_1} \ldots x_{i_k}$; $k = 1, \ldots, n$, где суммирование производится по всем системам индексов при фиксированном k и при условии: $i_1 < i_2 < \ldots < i_k$,— принадлежит классу $W_{n,n-k}$, а также любому классу $W_{n,m}$ с $m \leqslant n - k$. Эта функция не принадлежит ни одному классу $W_{n,m}$, для которого $m > n - k$.

В частности, при $k = 1$ получаем линейную функцию. Она дифференцируема $n - 1$ раз.

Пусть f $(x_1, \ldots, x_s)$ — произвольная функция. Назовем вектор переменных *нормальным относительно функции* f (соответственно относительно формулы F), если он состоит из переменных, не обязательно всех, функции f (или соответственно из переменных, входящих в формулу F), взятых по одному разу.

Рассмотрим набор $v=(x_{i_1}, \ldots, x_{i_q})$, нормальный относительно функции f, и набор констант $\sigma=(\sigma_1, \ldots, \sigma_q)$. Под ${}^{\sigma}f^{v}$ будем понимать функцию, полученную из функции f подстановкой вместо переменных $x_{i_1}, \ldots, x_{i_q}$ соответственно констант $\sigma_1, \ldots, \sigma_q$. В дальнейшем нам понадобится также символ ${}^{\sigma}F^{v}$. Им мы будем обозначать формулу, полученную из формулы F подстановкой на место вхождений переменных, составляющих набор v, констант набора σ соответственно.

II

Пусть f — произвольная функция от переменных $x_1, \ldots, x_n$, v — нормальный относительно нее набор длины q и x_j — переменная, не вошедшая в набор v. Скажем, что *функция f обладает свойством C (j, v)*, если ${}^{\sigma}f^{v}$ зависит от x_j при любом наборе σ. Рассмотрим класс W_n (j, v) всех функций от переменных $x_1, \ldots, x_n$, обладающих свойством C (j, v). Число всех функций множества W_n (j, v) обозначим через w_n (j, v).

Лемма 1.

$$w_n(j, v)=2^{2^n}\left(1-\frac{1}{2^{2^{n-q-1}}}\right)^{2^q} \tag{1}$$

где q — длина набора v.

Доказательство. Не ограничивая общности, можно предположить, что $v=(x_1, x_2, \ldots, x_m)$, а $j=m+1$. Определим сначала число функций вида $f(y, z_1, \ldots, z_i)$, $i \geqslant 0$, существенно зависящих от y. Оно равно $2^{2^i}(2^{2^i}-1)$. Действительно, число различных функций, зависящих от переменных $z_1, \ldots, z_i$, равно 2^{2^i}. Число упорядоченных пар различных функций от переменных $z_1, \ldots, z_i$ равно $2^{2^i}(2^{2^i}-1)$. Задание же функции вида $f(y, z_1, \ldots, z_i)$, существенно зависящей от y, равносильно заданию упорядоченной пары $[f(0, z_1, \ldots, z_i), f(1, z_1, \ldots, z_i)]$ различных функций от переменных $z_1, \ldots, z_i$. Теперь рассмотрим функции от переменных $x_1, \ldots, x_n$ и для удобства обозначим $y=x_{m+1}$, $z_i=x_{m+1+i}$. Задание функции $f(x_1, \ldots, x_m, y, z_1, \ldots, z_{n-m-1})$ равносильно заданию функций $f(0, 0, \ldots, 0, y, z_1, \ldots, z_{n-m-1}), \ldots, f(1, 1, \ldots, 1, y, z_1, \ldots, z_{n-m-1})$. По доказанному для каждого набора констант $\tau_1, \ldots, \tau_m$ существует $2^{2^{n-m-1}}(2^{2^{n-m-1}}-1)$ возможных вариантов функции $f(\tau_1, \ldots, \tau_m, y, z_1, \ldots, z_{n-m-1})$. Следовательно, число различных функций рассматриваемого вида равно $(2^{2^{n-m-1}}(2^{2^{n-m-1}}-1))^{2^m}$, что равно числу, указанному в формулировке леммы.

Лемма доказана.

Теорема 1. *Пусть $m_1, m_2, \ldots, m_n, \ldots$ — произвольная последовательность целых чисел, удовлетворяющих неравенству*

$$m_n \leqslant n-(1+\varepsilon)\log_2 n, \tag{2}$$

где $\varepsilon > 0$ произвольно мало. Тогда

$$\lim_{n\to\infty}\frac{w_{n, m_n}}{2^{2^n}}=1.$$

Доказательство. Рассмотрим функцию $f(x_1, \ldots, x_n)$. Фиксируем некоторый нормальный относительно нее набор v длины q. Пусть $x_{j_1}, \ldots, x_{j_{n-q}}$ — все переменные функции f, не вошедшие в v. Пусть функция f такова, что функция ${}^{\sigma}f^{v}$, где σ — некоторый набор констант длины q, не зависит хотя бы от одной из переменных $x_{j_1}, \ldots, x_{j_{n-q}}$ (для некоторого τ не удовлетворяет свойству $C(j_\tau, v)$). Рассмотрим множество $Z_n(v)$ всех таких функций.

Пусть $Z_n(j_\tau, v)$, где $1 \leqslant \tau \leqslant n-q$, — множество функций, не удовлетворяющих свойству $C(j_\tau, v)$. Тогда

$$Z_n(v) = \bigcup_{\tau=1}^{n-q} Z_n(j_\tau, v). \tag{3}$$

Пусть теперь $\zeta_n(v)$ — число функций множества $Z_n(v)$ и $\zeta_n(j_\tau, v)$ — число функций множества $Z_n(j_\tau, v)$.

Очевидно, что $w_n(j_\tau, v) + \zeta_n(j_\tau, v) = 2^{2^n}$. Отсюда и из равенства (1) получим:

$$\zeta_n(j_\tau, v) = 2^{2^n}\left(1 - \left(1 - \frac{1}{2^{2^{n-m-1}}}\right)^{2^m}\right). \tag{4}$$

Но из (3) следует $\zeta_n(v) \leqslant \sum\limits_{\tau=1}^{n-q} \zeta(j_\tau, v)$. Тогда отсюда и из равенства (4) будем иметь:

$$\zeta_n(v) \leqslant (n-q)\, 2^{2^n}\left(1 - \left(1 - \frac{1}{2^{2^{n-q-1}}}\right)^{2^m}\right). \tag{5}$$

Рассмотрим теперь объединение $Z_{n,q}$ всех множеств вида $Z_n(v)$ с различными наборами v длины q. Очевидно, пересечение множеств $Z_{n,q}$ и $W_{n,q}$ пусто и каждое из них дополняет другое до множества всех функций от n переменных. Пусть $\zeta_{n,q}$ — число функций в множестве $Z_{n,q}$. Тогда

$$\zeta_{n,q} = 2^{2^n} - w_{n,q}. \tag{6}$$

Но число различных нормальных наборов длины q из чисел $1, \ldots, n$ равно C_n^q. Отсюда и в силу неравенства (5) имеем:

$$2^{2^n} - w_{n,q} = \zeta_{n,q} \leqslant C_n^q (n-q) \cdot 2^{2^n}\left[1 - \left(1 - \frac{1}{2^{2^{n-q-1}}}\right)^{2^q}\right]. \tag{7}$$

Пусть теперь m_n — некоторое фиксированное число, удовлетворяющее неравенству (2), тогда очевидно, что для m_n выполняется неравенство

$$\frac{1}{2^{2^{n-m_n-1}}} < \frac{1}{2^{m_n}}. \tag{8}$$

Положим $q = m_n$. В силу (8) выполняется неравенство

$$1 - \left(1 - \frac{1}{2^{2^{n-m_n-1}}}\right)^{2^{m_n}} < \frac{2^{m_n}}{2^{2^{n-m_n-1}}}\text{*)}.$$

Кроме того, очевидно, что $C_n^{m_n}(n-m) \leqslant n2^n$. Воспользовавшись этими последними неравенствами и равенством (7), получим:

$$1 - \frac{w_{n,m_n}}{2^{2^n}} \leqslant n2^n \frac{2^{m_n}}{2^{2^{n-m_n-1}}}. \tag{9}$$

Но в силу (2) правое выражение неравенства (9) ограничено величиной $n2^{2n - \frac{1}{2}n^{1+\varepsilon}}$, стремящейся к нулю с ростом n. Теорема доказана.

*) Известно, что при целом $k > 0$ и $0 < x < \frac{1}{k}$ имеет место неравенство

$$1 - (1-x)^k \leqslant kx.$$

ния переменной x. Не теряя общности, можем предположить, что $\varphi_{i1}=x^{\sigma_i}$. Поскольку F_i — нормальная формула, ее подформула φ_{i2} не эквивалентна константе и не содержит вхождений переменного x. Обозначим символом $v^{(i)}$ — множество переменных формулы φ_{i2}, выписанных в любом порядке. Если теперь $\circ$ есть & (есть $\vee$), то за $\sigma^{(i)}$ примем набор констант для переменных из $v^{(i)}$ такой, что ${}^{\sigma^{(i)}}\varphi_{i2}^{v^{(i)}}$ реализует нуль (реализует единицу). Таким образом ${}^{\sigma^{(i)}}\varphi^{v^{(i)}}$ реализует константу σ'. Заменим теперь в формуле ${}^{\sigma^{(i)}}F_i^{v^{(i)}}$ подформулу ${}^{\sigma^{(i)}}\varphi_i^{v^{(i)}}$ константой σ'. Получим формулу F'_{i+1}. Формулу F_{i+1} получим из формулы F'_{i+1} приведением к нормальному виду.

Будем говорить, что определенная таким образом последовательность формул $F_1, \ldots, F_{k'}$ *порождена формулой F и переменной x*. Она обладает следующими свойствами:

1) $k_i \leqslant k-i+1$, где k_i — число вхождений переменной x в формулу F_i;

2) $k' \leqslant k+1$;

3) длина набора $v^{(i)}$ не больше, чем $L(\varphi_i)-1$.

Эти свойства очевидны. Четвертое, менее очевидное, доказывает

Лемма 3. *Пусть формула F удовлетворяет условию A_r, где $r \geqslant 2$, и содержит k вхождений переменной x и пусть $F_1, \ldots, F_{k'}$ — последовательность формул, порожденная формулой F и переменной x. Тогда*

1) расширение любого вхождения переменного x в формулу F_i содержит не более чем r^i-r^{i-1} вхождений,

2) существуют набор $v_{k'}$, не содержащий переменного x, и набор $\sigma_{k'}$, длина которых не больше, чем $r^{k'-1}-k'$, такие, что эквивалентна ${}^{\sigma_{k'}}F^{v_{k'}}$.

Будем доказывать лемму по индукции.

1. $i=1$. Рассмотрим формулу F_1. Пусть $\varphi_1 \overset{-}{\underset{-}{\circ}} (\varphi_{11} \circ \ldots \circ \varphi_{1s_1})$ — расширение некоторого вхождения x в F_1 и пусть, например, φ_{11} есть x^{σ}. Покажем, что $L(\varphi_1) \leqslant r-1$. Действительно, предположим противное, т. е. что $L(\varphi_1) \geqslant r$. Рассмотрим формулу ${}^{\tau}F^x$, где τ — забивающее значение вхождения переменной x из подформулы φ_1. Преобразуем ее к нормальному виду следующим образом. В формуле ${}^{\tau}F_1^x$ заменим подформулу ${}^{\tau}\varphi_1^x$ эквивалентной ей формулой τ^{σ} и полученную формулу приведем к нормальному виду любым способом. Получим формулу F_1'. Ввиду $L(\varphi_1) \geqslant r$ получим:

$$L(F_1') \leqslant L(F_1)-L(\varphi_1) \leqslant L(F_1)-r,$$

т. е. для формулы F_1 и наборов $v(x)$, $\sigma=(\tau)$ нарушается неравенство (11). Но это противоречит выполнению условия A_r для F_1. Таким образом, для F_1 утверждение леммы доказано.

2. Предположим, что лемма доказана для всех формул $F_1, \ldots, F_i$, где $i<k'$. Докажем ее для формулы F_{i+1}. Определим сначала наборы $v_{i+1}=v^{(1)}v^{(2)}\ldots v^{(i)}$ и $\sigma_{i+1}=\sigma^{(1)}\sigma^{(2)}\ldots\sigma^{(i)}$, где наборы $v^{(j)}$ и $\sigma^{(j)}$ при $1 \leqslant j \leqslant i$ являются наборами, при помощи которых из формулы F_j строится формула F_{j+1}. Очевидно, формула F_{i+1} получается приведением к нормальному виду формулы ${}^{\sigma_{i+1}}F^{v_{i+1}}$. Найдем длину q_{i+1} набора v_{i+1}. Ввиду выполнения утверждения леммы для всякой формулы F_j, где $1 \leqslant j \leqslant i$, длина набора $v^{(j)}$ для $1 \leqslant j \leqslant i$ по свойству 3 рассматриваемой последовательности формул не больше, чем $r^j-r^{j-1}-1$. Следовательно, $q_{i+1} \leqslant (r-1)+(r^2-r)+\ldots+(r^i-r^{i-1})-i$ и

$$q_{i+1} \geqslant r^i-i-1. \tag{12}$$

Но для формулы F выполняется условие A_r, следовательно,

$$L(F_{i+1}) < L(F) - q_i. \tag{13}$$

Пусть теперь $\varphi_{i+1} \overline{\underline{\circ}} (\varphi_{i+1,1} \circ \ldots \circ \varphi_{i+1,s_{i+1}})$ — расширение некоторого вхождения $x^{\sigma_{i+1}}$ формулы F_{i+1}. Покажем, что $L(\varphi_{i+1}) \leqslant r^{i+1} - r^i$. Действительно, пусть $L(\varphi_{i+1}) \geqslant r^{i+1} - r + 1$. Рассмотрим формулу ${}^{\tau_{i+1}}F^x$, где τ_{i+1} — забивающее значение рассматриваемого вхождения переменной x. Преобразуем формулу ${}^{\tau_{i+1}}F^x_{i+1}$ к нормальному виду, причем на первом шаге заменим подформулу ${}^{\tau_{i+1}}\varphi^x_{i+1}$ формулы ${}^{\tau_{i+1}}F^x_{i+1}$ константой $\tau^{\sigma_{i+1}}_{i+1}$ и полученную формулу приведем к нормальному виду. Получим некоторую нормальную формулу F'_{i+1}, для которой

$$L(F'_{i+1}) \leqslant L(F_{i+1}) - (r^{i+1} - r^i + 1).$$

Отсюда, используя (13), получим:

$$L(F'_{i+1}) \leqslant L(F) - q_i - (r^{i+1} - r^i + 1).$$

Очевидно, формулы F'_{i+1} и ${}^{\sigma_{i+1}\tau}F^{v_{i+1}x}$ эквивалентны и в силу выполнения для F условия A_r

$$L(F'_{i+1}) > L(F) - (q_i + 1) r.$$

Но система из двух последних неравенств и неравенства (12) противоречива при $r \geqslant 2$. Следовательно, предположение индукции для F_{i+1} выполняется. Этим первый пункт леммы доказан.

Второй пункт легко вытекает из неравенства (12) при $i = k' - 1$. Лемма доказана.

Лемма 3. *Если $f \in W_{NM}$, $M \geqslant \frac{m}{2}$, то любая формула F, реализующая функцию f, не удовлетворяет условию A_{r_m}, где*

$$r_m = \frac{\log_2 m}{\log_2 \log_2 m}.$$

Доказательство. Пусть $F_1, \ldots, F_{k'}$ — последовательность формул, порожденная формулой F и некоторой переменной x из F. Если теперь F удовлетворяет условию A_{r_m}, то по пункту 2 предыдущей леммы найдем наборы $v_{k'}$ и $\sigma_{k'}$, длина $q_{k'}$ которых не больше $r^{k'-1} - k'$, такие, что ${}^{\sigma_{k'}}F^{v_{k'}}$ эквивалентна $F_{k'}$. В силу замечания 3 и свойства 2) рассматриваемой последовательности формул $k' \leqslant r_m$, и, следовательно, $q_{k'}$ не больше, чем $r_m^{r_m - 1}$.

При $M \geqslant \frac{m}{2} \geqslant 4$ имеем $r_m^{r_m-1} < M$. Но $F_{k'}$ по определению рассматриваемой последовательности не содержит вхождений переменной x. Мы получили противоречие с тем, что $f \in W_{N,M}$.

Теперь приступим непосредственно к доказательству теоремы 2.

Рассмотрим $f \in W_{n,m}$ и произвольную реализующую ее формулу $F \in \mathfrak{A}$. Обозначим f символом f_0 и F символом F_0. В силу леммы 3 для F_0 условие A_{r_m} не выполняется. Тогда существует такой нормальный относительно f_0 набор v_1 и набор констант σ_1 длины $q_1 \geqslant 1$, что для некоторой нормальной формулы F_1 для функции $f_1 = {}^{\sigma_1}f_0^{v_1}$ имеет место

$$L(F_1) \leqslant L(F_0) - q_1 r_m. \tag{14_0}$$

Если $q_1 < \frac{m}{2}$, то для формулы F_1 по лемме 3 не выполняется условие A_{r_m}. Найдем нормальный относительно F_1 набор v_2 и набор констант σ_2 длины $q_2 \geqslant 1$ и формулу F_2, эквивалентную формуле ${}^{\sigma_2}F_1^{v_2}$, для которых

$$L(F_2) \leqslant L(F_1) - q_2 r_m. \tag{14_1}$$

Если при этом $q_1+q_2 \geqslant \frac{m}{2}$, то процесс обрываем, если же $q_1+q_2<\frac{m}{2}$, то F_2 не удовлетворяет условию A_{r_m} (по лемме 3) и строим аналогично предыдущему формулу F_3 и т. д. Получим последовательность формул $F_0, F_1, \ldots, F_i$ и последовательность чисел $q_1, \ldots, q_i$ такие, что для любого j, $j<i$, выполняется неравенство

$$L(F_{j+1}) \leqslant L(F_j)-q_{j+1}r_m. \qquad (14_j)$$

Если $q_1+\ldots+q_i<\frac{m}{2}$, то F_i не удовлетворяет свойству A_{r_m} и построим аналогично предыдущему формулу F_{i+1}. В силу того, что все $q_j \geqslant 1$, найдется такое i_0, что

$$q_1+q_2+\ldots+q_{i_0} \geqslant \frac{m}{2}.$$

Складывая теперь почленно неравенства (14_0), (14_1), ..., (14_{i_0}) и подставив в результат выражение для r_m, получим неравенство (11). Теорема доказана.

Замечание 4. Пусть $f \in W_{n,m}$. Методом работы [1] можно доказать, что

$$L(f) \geqslant \frac{n^{3/2}}{\sqrt{n-m}}. \qquad (15)$$

Таким образом,

$$L(f) \geqslant \max\left\{\frac{n^{3/2}}{\sqrt{n-m}}, \frac{m}{2}\frac{\log_2 m}{\log_2\log_2 m}\right\}.$$

Если $0<c_1<c_2<1$ и $c_1 n \leqslant m \leqslant c_2 n$, то при всех достаточно больших n оценка (11) лучше оценки (15).

ЛИТЕРАТУРА

1. Субботовская Б. А., О реализации линейных функций формулами в базисе &, $\vee$, $^-$, ДАН СССР **136**, 3, 1961, 553—555.
2. Кричевский Р. Е., Сложность контактных схем, реализующих одну функцию алгебры логики, ДАН СССР **151**, 4, 1963, 803—806.
3. Субботовская Б. А., О сравнении базисов при реализации функций алгебры логики формулами, ДАН СССР **149**, 4, 1963, 784—787.
4. Мучник Б. А., Оценка сложности реализации линейной функции формулами в некоторых базисах, Кибернетика (в печати).

Поступило в редакцию 8 VI 1966