КВАДРАТИЧНАЯ НИЖНЯЯ ОЦЕНКА СЛОЖНОСТИ, ОСНОВАННАЯ НА НЕПРЕРЫВНОСТИ ВТОРОЙ ПРОИЗВОДНОЙ

В. М. ХРАПЧЕНКО

(МОСКВА)

В заметке [1] для произвольной (в частности, не всюду определенной) функции алгебры логики $\varphi(x_1, \ldots, x_n)$ было доказано неравенство

$$L_\pi(\varphi) \geqslant \frac{|R_\varphi|^2}{|M_\varphi^1||M_\varphi^0|}, \tag{1}$$

где M_φ^1 — некоторое подмножество вершин (n-мерного единичного куба), на которых φ равна 1, M_φ^0 — некоторое подмножество вершин, на которых φ равна 0, и R_φ — множество всех ребер, соединяющих вершины из M_φ^1 с вершинами из M_φ^0 (как обычно, $|M|$ обозначает мощность множества M). На ряде примеров в заметке [1] было показано, что неравенство (1) позволяет получать квадратичные (относительно n) нижние оценки сложности П-схем, а значит и формул в базисе $\{\vee, \&, ^-\}$, реализующих функцию φ. Здесь приводится еще один пример такого рода.

Рассматривается приближенное вычисление функции действительного переменного $y = f(x)$ в промежутке $[a, b]$, которое сводится к нахождению n старших двоичных цифр y по n старшим двоичным цифрам x. Сделав упрощающие запись предположения: $[a, b] \subset [0, 1)$ и $y \in [0, 1)$ при всех $x \in [a, b]$, будем иметь

$$x = \sum_{i=1}^{\infty} x_i 2^{-i},$$

$$y = f(x) = \sum_{i=1}^{\infty} y_i(x) 2^{-i},$$

где каждая из цифр x_i и $y_i(x)$ $(1 \leqslant i < \infty)$ есть 0 или 1. При x, пробегающем все значения $\sum_{i=1}^{n} x_i 2^{-i} \in [a, b]$, цифры $y_1(x), \ldots, y_n(x)$ представляют собой неполностью определенные функции алгебры логики от аргументов $x_1, \ldots, x_n$.

Теорема. *Если в некотором промежутке $[a', b'] \subseteq [a, b]$ функция $f(x)$ имеет непрерывную вторую производную $f''(x) \not\equiv 0$, то при $m = m(n) \to \infty$ $(m(n) \leqslant n)$ справедлива оценка*

$$L_\pi(y_m) \gtrsim m^2.$$

В частности, если $m \asymp n$, то

$$L_\pi(y_m) \gtrsim n^2.$$

Доказательство сводится к оценке величин, входящих в неравенство (1). Очевидно, что $|M_{y_m}^1| \leqslant 2^n$ и $|M_{y_m}^0| \leqslant 2^n$. Остается оценить снизу $|R_{y_m}|$.

Каждому двоичному набору $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$ сопоставим число $\sigma = \sum_{i=1}^{n} \sigma_i 2^{-i}$. Очевидно, что при $\sigma_j = 0$ числа σ и $\sigma + 2^{-j}$ соответствуют соседним наборам. Поэтому если $\sigma \in [a, b]$, $\sigma_j = 0$ и $\sigma + 2^{-j} \in [a, b]$, то ребро, исходящее из вершины $\tilde{\sigma}$ в j-м направлении, будет принадлежать R_{y_m} всегда, когда

$$y_m(\sigma + 2^{-j}) \neq y_m(\sigma). \tag{2}$$

В промежутке $[a', b']$ для проверки (2) можно воспользоваться формулой Тейлора

$$f(\sigma + 2^{-j}) = f(\sigma) + 2^{-j} f'(\sigma) + 2^{-(2j+1)} f''(\xi), \tag{3}$$

где $\xi = \xi(\sigma) \in [a', b']$. В силу условия теоремы существуют такое, $\varepsilon > 0$ и такой промежуток $[a'', b''] \subseteq [a', b']$, что при всех $x \in [a'', b'']$ справедливо неравенство

$$|f''(x)| \geqslant \varepsilon. \tag{4}$$

В промежутке $[a'', b'']$ производная $f'(x)$ монотонна, и, следовательно, существует промежуток $[c, d] \subseteq [a'', b'']$, в котором $f'(x)$ сохраняет знак. В этом промежутке сохраняет знак и $f''(x)$ (см. (4)). Ограничившись рассмотрением промежутка $[c, d]$, мы упростим исследование формулы (3).

В зависимости от того, какие знаки в $[c, d]$ имеют $f'(x)$ и $f''(x)$, возможны 4 случая. Рассмотрим подробно случай, когда в этом промежутке $f'(x) > 0$ и $f''(x) > 0$. Пусть

$$f'(x) = \sum_{i=-r}^{\infty} y'_i(x) 2^{-i},$$

$$f''(x) = \sum_{i=-s}^{\infty} y''_i(x) 2^{-i},$$

где r и s — некоторые неотрицательные числа, а каждая из цифр $y'_i(x)$ и $y''_i(x)$ есть 0 или 1. Пользуясь в промежутке $[c, d]$ формулой (3), нетрудно убедиться в том, что для выполнения (2) достаточно, чтобы сумма

$$\sum_{i=m+1}^{\infty} y_i(\sigma) 2^{-i} + 2^{-j} \sum_{i=m-j}^{\infty} y'_i(\sigma) 2^{-i} + 2^{-(2j+1)} \sum_{i=m-(2j+1)}^{\infty} y''_i(\xi) 2^{-i} \tag{5}$$

содержала в m-м разряде после запятой цифру 1. Зная, что при одновременном сложении трех чисел перенос в старший разряд не превосходит двух, легко обнаружить, что m-й разряд суммы (5) содержит цифру 1, если, например, при «сложении столбиком» слагаемых из (5) возникает ситуация:

номера разрядов:	m	$m+1$	$m+2$	$\cdots$
		0	$\cdot$	$\cdots$
	1	0	0	$\cdots$
	0	0	0	$\cdots$

т. е.

1°) $y_{m+1}(\sigma) = 0$,

2°) $y'_{m-j}(\sigma) = 1,\quad y'_{m-j+1}(\sigma) = 0,\quad y'_{m-j+2}(\sigma) = 0$,

3°) $y''_{m-(2j+1)}(\xi) = y''_{m-2j}(\xi) = y''_{m-(2j-1)}(\xi) = 0$,

или ситуация:

номера разрядов:	m	$m+1$	$m+2$	$\cdots$
		1	$\cdot$	$\cdots$
	0	1	0	$\cdots$
	0	0	0	$\cdots$

т. е.

1$^{\circ\circ}$) $y_{m+1}(\sigma)=1$,

2$^{\circ\circ}$) $y'_{m-j}(\sigma)=0, \quad y'_{m-j+1}(\sigma)=1, \quad y'_{m-j+2}(\sigma)=0$,

3$^{\circ\circ}$) $y''_{m-(2j+1)}(\xi)=y''_{m-2j}(\xi)=y''_{m-(2j-1)}(\xi)=0$.

Таким образом, нам осталось для каждого $\sigma=\sum\limits_{i=1}^{n}\sigma_i 2^{-i}\in[c, d]$ оценить снизу число тех значений j, при которых $\sigma_j=0$, $\sigma+2^{-j}\in[c, d]$ и выполняются либо условия 1°, 2° и 3° либо условия 1$^{\circ\circ}$, 2$^{\circ\circ}$ и 3$^{\circ\circ}$.

Очевидно, что для любого $\sigma=\sum\limits_{i=1}^{n}\sigma_i 2^{-i}$ либо условие 1° либо условие 1$^{\circ\circ}$ выполнено (но не оба сразу). Далее, если ввести

$$l=\left[\frac{m}{2}+\log_2 m\right] \tag{6}$$

и ограничиться рассмотрением значений

$$j>l,$$

то (при достаточно больших n) будут выполнены условия 3° и 3$^{\circ\circ}$ (здесь используется ограниченность $f''(x)$ сверху в $[c, d]$) и для почти всех $\sigma=\sum\limits_{i=1}^{n}\sigma_i 2^{-i}\in[c, d]$ будет выполняться соотношение $\sigma+2^{-j}\in[c, d]$. Поэтому теперь желательно оценить снизу число значений $j>l$, при которых $\sigma_j=0$ и выполнено условие 2°, и число значений $j>l$, при которых $\sigma_j=0$ и выполнено условие 2$^{\circ\circ}$, причем эти оценки достаточно получить не для всех, а лишь для почти всех $\sigma=\sum\limits_{i=1}^{n}\sigma_i 2^{-i}\in[c, d]$.

В каждом наборе $\tilde{\sigma}=(\sigma_1, \ldots, \sigma_n)$ выделим поднабор $\tilde{\sigma}'=(\sigma_1, \ldots, \sigma_l)$ и покажем, что для почти всех $\sigma'=\sum\limits_{i=1}^{l}\sigma_i 2^{-i}\in[c, d]$ набор $(y'_0(\sigma'), \ldots$ $\ldots, y'_{m-l+1}(\sigma'))$

1) равен набору $(y'_0(x), \ldots, y'_{m-l+1}(x))$ при всех $x\in[\sigma', \sigma'+2^{-l})$,

2) содержит не менее $\frac{m}{48}-o(m)$ подпоследовательностей (100),

3) содержит не менее $\frac{m}{48}-o(m)$ подпоследовательностей (010).

Обозначим число различных $\sigma'=\sum\limits_{i=1}^{l}\sigma_i 2^{-i}\in[c, d]$, для которых

$$(y'_{-r}(\sigma'), \ldots, y'_0(\sigma'), \ldots, y'_{m-l+1}(\sigma'))=\tilde{\tau} \tag{7}$$

(здесь $\tilde{\tau}$ — некоторый фиксированный набор), через $k(\tilde{\tau})$. Заметим, что когда $\sigma'\in[c, d]$, тогда $\tau\in(f'(c)-2^{-(m-l+1)}, f'(d)]$. Пользуясь тем, что $f''(x)$ ограничена в промежутке $[c, d]$ снизу (см. (4)) и сверху, и учитывая (6), нетрудно установить, что

$$k(\tilde{\tau})\asymp\frac{2^{-(m-l+1)}}{2^{-l}}\asymp m^2 \tag{8}$$

для всех $\tau\in(f'(c)-2^{-(m-l+1)}, f'(d)]$, кроме двух крайних значений τ, для которых $k(\tilde{\tau})$ может быть меньше. Поскольку среди чисел σ', удовлетворяющих (7), самое большее одно (максимальное) не обладает свойством 1), из (8) свойство 1) следует для почти всех $\sigma'\in[c, d]$.

Разбивая всевозможные двоичные наборы $\tilde{\tau}=(\tau_{-r}, \ldots, \tau_0, \ldots$ $\ldots, \tau_{m-l+1})$ длины $\lambda=m-l+r+2$ на подпоследовательности из трех цифр и применяя теорему Бернулли (см., например, [2]), нетрудно убедиться в том, что почти все наборы $\widetilde{\tau}$ содержат не менее чем по $\frac{\lambda}{24}$ — $o(\lambda)$ троек (100) и не менее чем по $\frac{\lambda}{24} - o(\lambda)$ троек (010). В силу (6) и конечности r отсюда следует, что для почти всех $\widetilde{\tau}$ набор $(\tau_0, \ldots, \tau_{m-l+1})$ обладает свойствами 2) и 3). Благодаря тому, что разность $f'(d) - f'(c)$ фиксирована (и отлична от нуля), это же положение справедливо для почти всех $\tau \in [f'(c), f'(d)]$, а благодаря (8) и для почти всех $\sigma' \in [c, d]$, если принять $(\tau_0, \ldots, \tau_{m-l+1}) = (y'_0(\sigma'), \ldots, y'_{m-l+1}(\sigma'))$.

Легко заметить, что если набор $\widetilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$ начинается таким поднабором $\widetilde{\sigma}' = (\sigma_1, \ldots, \sigma_l)$, что σ' обладает свойствами 1), 2) и 3), то для σ как условие 2°, так и условие 2°° выполнены не менее чем при $\frac{m}{48} - o(m)$ значениях j, удовлетворяющих соотношению $l + 1 \leqslant j \leqslant m$. В силу теоремы Бернулли для почти всех таких σ как среди одних, так и среди других значений j встретится не менее $\frac{m}{96} - o(m)$ значений, при которых $\sigma_j = 0$. Следовательно, для почти всех $\sigma \in [c, d]$ существует $\frac{m}{96} - o(m)$ значений $j > l$, при которых $\sigma_j = 0$ и выполнено условие 2°, и $\frac{m}{96} - o(m)$ значений $j > l$, при которых $\sigma_j = 0$ и выполнено условие 2°°. Отсюда следует, что почти из каждой вершины $\widetilde{\sigma}$, для которой $\sigma \in [c, d]$, исходит $\frac{m}{96} - o(m)$ ребер, принадлежащих R_{y_m}, и, значит,

$$|R_{y_m}| \gtrsim m2^n.$$

В тех случаях, когда $f'(x)$ и $f''(x)$ имеют в промежутке $[c, d]$ другие знаки, оценка числа сумм (5), содержащих в m-м разряде цифру 1, получается из рассмотрения других ситуаций (см. таблицу).

	$f''(x) > 0$	$f''(x) < 0$
$f'(x) > 0$	0 ... 1 ... 100 ... и 010 ... 000 ... 000 ...	0 ... 1 ... 101 ... и 011 ... 000 ... 000 ...
$f'(x) < 0$	0 ... 1 ... 011 ... и 101 ... 000 ... 000 ...	0 ... 1 ... 010 ... и 100 ... 000 ... 000 ...

Применяя неравенство (1), мы завершаем доказательство теоремы.

Условиям теоремы удовлетворяют (при соответствующих масштабах функции и аргумента) все нелинейные аналитические функции, в частности, $y = x^2$ и $y = \frac{1}{x}$. Поэтому полученные оценки справедливы для формул в базисе $\{\vee, \&, {}^{-}\}$, вычисляющих цифры произведения и частного.

ЛИТЕРАТУРА

[1] Храпченко В. М., Об одном методе получения нижних оценок сложности П-схем, Матем. заметки 10, 1 (1971), 83—92.

[2] Боев Г. П., Теория вероятностей, М.— Л., Гостехиздат, 1950.

Поступило в редакцию 26 VII 1970