A QUADRATIC COMPLEXITY LOWER BOUND BASED ON THE CONTINUITY OF THE SECOND DERIVATIVE*

V. M. KHRAPCHENKO

(MOSCOW)

In a note [1], for any Boolean function $\varphi(x_1, \ldots, x_n)$ (in particular, for a partially defined), the inequality

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

was proved. Here, M_φ^1 is some subset of vertices (in the n-dimensional Boolean cube) on which φ takes the value 1, M_φ^0 is a subset of vertices on which φ takes the value 0, and R_φ is a set of all edges connecting vertices from M_φ^1 with vertices from M_φ^0 (as usual, $|M|$ stands for the cardinality of the set M). In [1], it was shown on a number of examples that the inequality (1) allows one to obtain quadratic (with respect to n) lower bounds for the complexity of Π-circuits, and hence of formulae over the basis $\{\vee, \&, {}^-\}$, implementing a function φ. Here, one more such example is presented.

We consider an approximate computation of a real function $y = f(x)$ on an interval $[a, b]$. This reduces to the computation of n most significant binary digits of y from the given n most significant binary digits of x. To simplify notations, let us assume $[a, b] \subset [0, 1)$, and $y \in [0, 1)$ for all $x \in [a, b]$. Then,

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

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

where any x_i and $y_i(x)$ $(1 \leqslant i < \infty)$ is either 0 or 1. Given that x takes any value $x = \sum_{i=1}^{n} x_i 2^{-i} \in [a, b]$, the digits $y_1(x), \ldots, y_n(x)$ may be viewed as the partially defined Boolean functions of variables $x_1, \ldots, x_n$.

*Originally published in Russian in "Problemy kibernetiki" ("Problems of cybernetics"), Vol. 26. Moscow, Nauka, 1973, 203–206.

T h e o r e m. *If in some subinterval* $[a', b'] \subseteq [a, b]$*, a function* $f(x)$ *has a continuous second derivative* $f''(x) \not\equiv 0$*, then for* $m = m(n) \to \infty$ $(m(n) \leqslant n)$*,*

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

In particular, for $m \asymp n$*,*

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

The p r o o f goes by bounding the quantities involved in the inequality (1). Obviously, $|M^1_{y_m}| \leqslant 2^n$, and $|M^0_{y_m}| \leqslant 2^n$. It remains to lower bound $|R_{y_m}|$.

Let us associate with every binary vector $\widetilde{\sigma} = (\sigma_1, \dots, \sigma_n)$ the number $\sigma = \sum_{i=1}^n \sigma_i 2^{-i}$. Clearly, for $\sigma_j = 0$, the numbers σ and $\sigma + 2^{-j}$ correspond to adjacent vertices. Therefore, if $\sigma \in [a, b]$, $\sigma_j = 0$, and $\sigma + 2^{-j} \in [a, b]$, then an edge outgoing from the vertex $\widetilde{\sigma}$ in j-th direction belongs to R_{y_m} iff

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

To verify (2) in an interval $[a', b']$, we use the Taylor's formula

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

where $\xi = \xi(\sigma) \in [a', b']$. By the condition of the theorem, there exist such $\varepsilon > 0$ and a subinterval $[a'', b''] \subseteq [a', b']$ that the inequality

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

holds for all $x \in [a'', b'']$. Since the derivative $f'(x)$ is monotone on $[a'', b'']$, there exist a subinterval $[c, d] \subseteq [a'', b'']$ where $f'(x)$ preserves its sign. On this subinterval, $f''(x)$ preserves the sign as well (see (4)). To simplify the analysis of the formula (3), we restrict ourselves to considering of the subinterval $[c, d]$.

There are 4 possibilities depending on the signs of $f'(x)$ and $f''(x)$ on $[c, d]$. We choose to consider in details the case when $f'(x) > 0$ and $f''(x) > 0$. Let

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

where r, s are nonnegative integers, and digits $y'_i(x)$, $y''_i(x)$ take values 0 and 1. By applying of the formula (3) with respect to the interval $[c,\ d]$, it can be easily deduced that to satisfy (2) it is sufficient for the sum

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

to contain 1 in m-th position after comma. Note that when adding three numbers, a carry to the most significant position does not exceed 2. Thus, as easy to observe, the m-th digit of the sum (5) is 1, e.g. if "addition by columns" of the summands from (5) leads to a configuration

digit positions:	m	$m+1$	$m+2$	$\cdot$	$\cdot$	$\cdot$
		0	$\cdot$	$\cdot$	$\cdot$	$\cdot$
	1	0	0	$\cdot$	$\cdot$	$\cdot$
	0	0	0	$\cdot$	$\cdot$	$\cdot$

meaning that

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

or to a configuration

digit positions:	m	$m+1$	$m+2$	$\cdot$	$\cdot$	$\cdot$
		1	$\cdot$	$\cdot$	$\cdot$	$\cdot$
	0	1	0	$\cdot$	$\cdot$	$\cdot$
	0	0	0	$\cdot$	$\cdot$	$\cdot$

meaning that

1°°) $y_{m+1}(\sigma) = 1$,

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

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

So, we are left for any $\sigma = \sum_{i=1}^{n} \sigma_i 2^{-i} \in [c,\ d]$ to lower bound the number of values j satisfying $\sigma_j = 0$, $\sigma + 2^{-j} \in [c,\ d]$, and either conditions 1°, 2°, 3°, or conditions 1°°, 2°°, 3°°.

It is clear that for any $\sigma = \sum_{i=1}^{n} \sigma_i 2^{-i}$, either condition 1° or condition 1°° holds (but not both). Let

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

In what follows, we only consider values

$$j > l.$$

Then (for large enough n) conditions 3° and 3°° are satisfied (here we exploit the fact that $f''(x)$ is bounded from above in $[c,\, d]$), and for almost all $\sigma = \sum_{i=1}^{n} \sigma_i 2^{-i} \in [c,\, d]$, the condition $\sigma + 2^{-j} \in [c,\, d]$ is fulfilled. Therefore, it is desirable now to lower bound the number of values $j > l$ satisfying $\sigma_j = 0$ and 2°, and the number of values $j > l$ satisfying $\sigma_j = 0$ and 2°°. It suffices to obtain such bounds not for all but just for almost all $\sigma = \sum_{i=1}^{n} \sigma_i 2^{-i} \in [c,\, d]$.

In any vector $\widetilde{\sigma} = (\sigma_1, \dots, \sigma_n)$, take a subvector $\widetilde{\sigma}' = (\sigma_1, \dots, \sigma_l)$. We are going to show that for almost every $\sigma' = \sum_{i=1}^{l} \sigma_i 2^{-i} \in [c,\, d]$, the vector $(y'_0(\sigma'), \dots, y'_{m-l+1}(\sigma'))$

1) equals to $(y'_0(x), \dots, y'_{m-l+1}(x))$ for any $x \in [\sigma',\, \sigma' + 2^{-l})$,

2) contains at least $\frac{m}{48} - o(m)$ substrings (100),

3) contains at least $\frac{m}{48} - o(m)$ substrings (010).

Let $k(\widetilde{\tau})$ denote the number of different values $\sigma' = \sum_{i=1}^{l} \sigma_i 2^{-i} \in [c,\, d]$ satisfying

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

(here $\widetilde{\tau}$ is a fixed vector). Note that if $\sigma' \in [c,\, d]$, then $\tau \in (f'(c) - 2^{-(m-l+1)},\, f'(d)]$. Due to the fact that $f''(x)$ is bounded from below (see (4)) and from above in $[c,\, d]$, and in the view of (6), it can be easily deduced that

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

holds for all $\tau \in (f'(c) - 2^{-(m-l+1)},\, f'(d)]$, except for the two boundary values of τ, when $k(\widetilde{\tau})$ may be smaller. Since among all values σ' satisfying (7), at most one (the largest) value does not satisfy 1), it follows from (8) that the property 1) holds for almost all $\sigma' \in [c,\, d]$.

Consider splitting of a binary vector $\widetilde{\tau} = (\tau_{-r}, \dots, \tau_0, \dots, \tau_{m-l+1})$ of length $\lambda = m - l + r + 2$ into three digit substrings. Applying the Bernoulli theorem (see e.g. [2]), it is easy to obtain that almost all vectors $\widetilde{\tau}$ contain at least $\frac{\lambda}{24} - o(\lambda)$ triples (100) and at least $\frac{\lambda}{24} - o(\lambda)$ triples (010). Since (6) holds, and r is a finite constant, it follows that for almost all $\widetilde{\tau}$, vectors $(\tau_0, \dots, \tau_{m-l+1})$ satisfy properties 2) and 3). Due to the fact that $f'(d) - f'(c)$ is fixed (and is different from zero), the same holds for almost all $\tau \in [f'(c),\, f'(d)]$, and in the view of (8), also for almost all $\sigma' \in [c,\, d]$, given that $(\tau_0, \dots, \tau_{m-l+1}) = (y'_0(\sigma'), \dots, y'_{m-l+1}(\sigma'))$.

Suppose that $\widetilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$ starts with a subvector $\widetilde{\sigma}' = (\sigma_1, \ldots, \sigma_l)$, where σ' satisfies properties 1), 2), and 3). Then, as easy to notice, each of the conditions 2° and 2°° holds for at least $\frac{m}{48} - o(m)$ values of j satisfying $l + 1 \leqslant j \leqslant m$. By the Bernoulli theorem, for almost all such σ, both among the former group of values j, and among the latter group, there will be at least $\frac{m}{96} - o(m)$ values providing $\sigma_j = 0$. Consequently, for almost all $\sigma \in [c, d]$, there exist $\frac{m}{96} - o(m)$ values $j > l$ ensuring $\sigma_j = 0$ and the condition 2°, and $\frac{m}{96} - o(m)$ values $j > l$ ensuring $\sigma_j = 0$ and the condition 2°°. It follows that almost every vertex $\widetilde{\sigma}$ satisfying $\sigma \in [c, d]$ has $\frac{m}{96} - o(m)$ outgoing edges belonging to R_{y_m}, hence

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

In the cases when $f'(x)$ and $f''(x)$ have other signs on $[c, d]$, in order to bound the number of sums (5) containing 1 in m-th position, we consider other configurations (look at the table).

	$f''(x) > 0$					$f''(x) < 0$				
$f'(x) > 0$	0	…		1	…	0	…		1	…
	100	…	and	010	…	101	…	and	011	…
	000	…		000	…	000	…		000	…
$f'(x) < 0$	0	…		1	…	0	…		1	…
	011	…	and	101	…	010	…	and	100	…
	000	…		000	…	000	…		000	…

Applying the inequality (1), we complete the proof of the theorem.

The conditions of the theorem (under an appropriate scaling of functions and arguments) are satisfied by all nonlinear analytic functions, in particular, by $y = x^2$ and $y = \frac{1}{x}$. Thus, the obtained bounds hold for the formulae over the basis $\{\vee, \&, \bar{}\}$ computing digits of the product, and of the quotient.

LITERATURE

[1] K h r a p c h e n k o V. M., A method of obtaining lower bounds for the complexity of Π-schemes, Math. Notes Acad. of Sci. USSR **10**, 1 (1971), 474–479.

[2] B o e v G. P., Probability theory, Moscow–Leningrad, Gostechizdat, 1950 (in Russian).

Submitted 26 VII 1970