ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Март—апрель 2008. Том 15, № 2. 12–22

УДК 519.95

УТОЧНЕНИЕ ВЕРХНЕЙ ОЦЕНКИ ГЛУБИНЫ СУММАТОРА И КОМПАРАТОРА

М. И. Гринчук

Посвящаю памяти О. Б. Лупанова, своего учителя

В статье доказывается верхняя оценка $\log_2 n + \log_2 \log_2 n + \mathrm{const}$ для глубины операторов сложения и сравнения n-битовых чисел в базисе $\{\&, \vee, \sim\}$.

Введение

Поиск оптимальных в том или ином смысле способов реализации конкретных арифметических операторов — задача одновременно и классическая, и не теряющая актуальности в связи с постоянным возникновением новых приложений, требующих эффективных аппаратных методов вычислений. Даже для простейших на вид операторов таких, как целочисленное сложение или сравнение $x < y$, построение простых и (или) быстродействующих схем, а тем более доказательство их оптимальности, оказывается весьма нетривиальным.

Для схемной сложности [2] компараторов и сумматоров известны неулучшаемые результаты (для компаратора они достаточно очевидны, тогда как для сумматора требуют весьма сложной техники, разработанной Н. П. Редькиным в [3]), но в обоих случаях простейшие схемы имеют линейную глубину. Схемы асимптотически минимальной глубины были построены В. М. Храпченко более 40 лет тому назад: в работе [4] дан метод синтеза n-разрядных сумматоров в базисе $\{\&, \vee, \sim\}$ с глубиной $\log_2 n + \sqrt{2 \log_2 n} + O(1)$, вошедший в учебники (см., например, [10], с. 276–283) и остававшийся лучшим известным (для больших n) до недавнего времени. В последние годы было предложено несколько практических методов синтеза [1, 6, 7, 9], которые позволяют строить схемы меньшей глубины при малых n, но асимптотически проигрывают методу Храпченко. Наконец, автором был предложен алгоритм синтеза [8], обобщающий

методы из [1, 6, 7, 9]. Анализ схем, построенных новым методом, дал основание предполагать, что их глубина имеет вид $\log_2 n + O(\log_2 \log_2 n)$. В настоящей работе приводится доказательство такой оценки: показано, что даже несколько ухудшенный (но зато позволивший выразить глубину аналитически) вариант упомянутого алгоритма гарантирует глубину не более $\log_2 n + \log_2 \log_2 n + O(1)$.

Интересно сравнить полученную верхнюю оценку с недавним результатом В. М. Храпченко. В [5] он показал, что глубина n-битового сумматора не может быть меньше $\log_2 n + 0{,}15 \log_2 \log_2 \log_2 n + \mathrm{const}$ (это первая нетривиальная нижняя оценка глубины сумматора; в ней коэффициент 0,15, как отмечено в той же статье [5], можно повышать до сколь угодно близкого значения к 1).

1. Базовые неравенства для глубины

Известно (см., например, [1, 5]), что глубина*) k-битового сумматора и (или) компаратора определяется (с точностью до $O(1)$) глубиной функций вида

$$f_m(x_0, \ldots, x_m) = x_0 \,\&\, (x_1 \vee x_2 \,\&\, (x_3 \vee \ldots x_m \ldots)),$$

где $m = 2k + O(1)$.

Для оценки глубины функций f_m перейдём к более широкому (двухпараметрическому) семейству функций. А именно, пусть семейство функций $f_{2n,m}$ и $f^*_{2n,m}$ задано (при неотрицательных n и m) следующим образом:

1) через $f_{0,m}$ обозначим упомянутую выше функцию f_m, а через $f^*_{0,m}$ — функцию, двойственную к ней; иначе говоря, положим

$$\begin{aligned}
&f_{0,0}(x_0) = f^*_{0,0}(x_0) = x_0, \\
&f_{0,m}(x_0, \ldots, x_m) = x_0 \,\&\, f^*_{0,m-1}(x_1, \ldots, x_m), && m > 0, \\
&f^*_{0,m}(x_0, \ldots, x_m) = x_0 \vee f_{0,m-1}(x_1, \ldots, x_m), && m > 0;
\end{aligned}$$

2) при $n > 0$ и $m \geqslant 0$ положим

$$\begin{aligned}
f_{2n,m}(x_0, \ldots, x_{2n+m}) &= x_0 \,\&\, f_{2n-2,m}(x_2, x_3, \ldots, x_{2n+m}), \\
f^*_{2n,m}(x_0, \ldots, x_{2n+m}) &= x_0 \vee f^*_{2n-2,m}(x_2, x_3, \ldots, x_{2n+m}).
\end{aligned}$$

*) Определение глубины булевых функций и схем из функциональных элементов можно найти, например, в [2].

Другими словами,

$$\begin{aligned} f_{2n,m}(x_0,\dots,x_{2n+m}) &= x_0 \,\&\, x_2 \,\&\, \dots \,\&\, x_{2n-2} \\ &\quad \& \, x_{2n} \,\&\, (x_{2n+1} \vee x_{2n+2} \,\&\, (x_{2n+3} \vee x_{2n+4} \,\&\, (\dots x_{2n+m} \dots))), \\ f^*_{2n,m}(x_0,\dots,x_{2n+m}) &= x_0 \vee x_2 \vee \dots \vee x_{2n-2} \vee x_{2n} \\ &\quad \vee x_{2n+1} \,\&\, (x_{2n+2} \vee x_{2n+3} \,\&\, (x_{2n+4} \vee \dots x_{2n+m} \dots)) \end{aligned}$$

(при чётном m самая внутренняя операция в первом соотношении есть дизъюнкция, во втором — конъюнкция; при нечётном m самая внутренняя операция в первом соотношении есть конъюнкция, во втором — дизъюнкция).

Через $d(2n,m)$ обозначим глубину реализации функции $f_{2n,m}$ в базисе из двуместных операций $\{\&,\vee\}$. Функция $f^*_{2n,m}$, как двойственная к $f_{2n,m}$, также имеет глубину $d(2n,m)$.

Лемма 1. *Справедливы неравенства* $d(2n,m+1) \geqslant d(2n,m)$ *и* $d(2n+2,m) \geqslant d(2n,m)$.

Доказательство. Легко видеть, что подходящая подстановка константы вместо последней переменной превращает $f_{2n,m+1}$ в $f_{2n,m}$ ($f^*_{2n,m+1}$ в $f^*_{2n,m}$); подстановка константы 1 вместо первой переменной превращает $f_{2n+2,m}$ в $f_{2n,m}$ (двойственную функцию $f^*_{2n+2,m}$ подстановка константы 0 вместо первой переменной превращает в $f^*_{2n,m}$). Лемма 1 доказана.

Лемма 2. *Справедливо неравенство*

$$d(2n+2k,m) \leqslant 1 + \max(\lceil \log_2 n \rceil, d(2k,m)).$$

Справедливость искомого соотношения следует из разложения

$$\begin{aligned} &f_{2n+2k,m}(x_0,x_1,\dots,x_{2n+2k+m}) \\ &\qquad = (x_0 \,\&\, x_2 \,\&\, \dots \,\&\, x_{2n-2}) \,\&\, f_{2k,m}(x_{2n},x_{2n+1},\dots,x_{2n+2k+m}), \end{aligned}$$

равно как и из соответствующего двойственного разложения для f^*.

Лемма 3. *Имеет место неравенство*

$$d(2n,2k+m+1) \leqslant 1 + \max(d(2n,2k),d(2k,m)).$$

Доказательство. Искомое неравенство вытекает из следующих из-

вестных*) разложений:

$$f_{2n,2k+m+1}(x_0, x_1, \ldots, x_{2n+2k+m+1}) = f_{2n,2k}(x_0, x_1, \ldots, x_{2n+2k}) \\ \& \, f^*_{2k,m}(x_{2n+1}, x_{2n+2}, \ldots, x_{2n+2k+m+1}), \quad (1)$$

$$f^*_{2n,2k+m+1}(x_0, x_1, \ldots, x_{2n+2k+m+1}) = f^*_{2n,2k}(x_0, x_1, \ldots, x_{2n+2k}) \\ \vee f_{2k,m}(x_{2n+1}, x_{2n+2}, \ldots, x_{2n+2k+m+1}). \quad (2)$$

Для полноты изложения приведём доказательство разложений (1) и (2) полностью. Воспользуемся двойной индукцией: сперва по k, затем по n. При $n = k = 0$ (база индукции) в силу определения функций f и f^* соотношения (1) и (2) превращаются в истинные тождества

$$f_{0,m+1}(x_0, x_1, \ldots, x_{m+1}) = f_{0,0}(x_0) \,\&\, f^*_{0,m}(x_1, x_2, \ldots, x_{m+1}),$$
$$f^*_{0,m+1}(x_0, x_1, \ldots, x_{m+1}) = f^*_{0,0}(x_0) \vee f_{0,m}(x_1, x_2, \ldots, x_{m+1})$$

(напомним, что $f_{0,0}(x_0) = f^*_{0,0}(x_0) = x_0$).

Далее, пусть (1) и (2) доказаны при $n = 0$ и $k = K$; докажем их для $k = K + 1$, т. е. покажем, что имеет место соотношение

$$f_{0,2K+m+3}(x_0, x_1, \ldots, x_{2K+m+3}) \\ = f_{0,2K+2}(x_0, x_1, \ldots, x_{2K+2}) \,\&\, f^*_{2K+2,m}(x_1, x_2, \ldots, x_{2K+m+3}) \quad (3)$$

(и двойственное ему).

Для этого преобразуем (3) с использованием разложений, имеющих место по определению функций f и f^*:

$$f_{0,2K+m+3}(x_0, x_1, \ldots) = x_0 \,\&\, (x_1 \vee f_{0,2K+m+1}(x_2, \ldots)),$$
$$f_{0,2K+2}(x_0, x_1, \ldots) = x_0 \,\&\, (x_1 \vee f_{0,2K}(x_2, \ldots)),$$
$$f^*_{2K+2,m}(x_1, \ldots) = x_1 \vee f^*_{2K,m}(x_3, \ldots);$$

при этом получится соотношение, равносильное соотношению (3),

$$x_0 \,\&\, (x_1 \vee f_{0,2K+m+1}(x_2, x_3, \ldots, x_{2K+m+3})) \\ = x_0 \,\&\, (x_1 \vee f_{0,2K}(x_2, x_3, \ldots, x_{2K+2})) \,\&\, (x_1 \vee f^*_{2K,m}(x_3, x_4, \ldots, x_{2K+m+3})),$$

*) В несколько иной форме эти разложения приведены в [1] (стр. 39, 2-я снизу ненумерованная выключная формула), а в частном случае $n = 0$ (тривиально обобщающемся на полный) — уже в [4].

справедливость которого при $x_0 = 0$ и $x_0 = x_1 = 1$ проверяется непосредственно, а при $x_0 = 1$ и $x_1 = 0$ оно совпадает (с учётом другого обозначения переменных) с предположением индукции:

$$f_{0,2K+m+1}(x_0, x_1, \dots, x_{2K+m+1}) \\ = f_{0,2K}(x_0, x_1, \dots, x_{2K}) \;\&\; f^*_{2K,m}(x_1, x_2, \dots, x_{2K+m+1}).$$

Двойственное к (3) разложение доказывается аналогично.

Для завершения доказательства разложений (1) и (2) заметим, что увеличение на единицу параметра n сводится к увеличению на 2 индексов переменных и добавлением члена x_0 к обеим частям соответствующего равенства (в случае (1) он присоединяется конъюнкцией, в случае (2) — дизъюнкцией). Лемма 3 доказана.

2. Верхняя оценка для $d(0, m)$

Обозначим через $m(d, n)$ максимальное решение относительно m неравенства $d(2n, m) \leqslant d$. Величину $m(d, n)$ назовём *ёмкостью*. Она показывает, сколь много переменных в «знакопеременной» части могут иметь функции $f_{2n,m}$ и $f^*_{2n,m}$ при заданном ограничении глубины d и заданной длине n «ассоциативной» части.

Лемма 4. *Для ёмкости $m(d, n)$ справедливы следующие утверждения*:

(i) *имеет место неравенство* $m(d, n) \geqslant 0$;

(ii) *ёмкость $m(d, n)$ определена только при* $0 \leqslant n < 2^d$;

(iii) *имеет место неравенство* $m(d, n) \leqslant 2^d - n - 1$.

Доказательство. Утверждение (i) очевидно.

Для доказательства (ii) и (iii) прежде всего заметим, что функции $f_{2n,m}$ и $f^*_{2n,m}$ имеют $n + m + 1$ существенных переменных.

(ii) При $0 \leqslant n < 2^d$ функции $f_{2n,0}$ и $f^*_{2n,0}$ — это конъюнкция и дизъюнкция $n + 1$ переменной, имеющие глубину $\lceil \log_2(n + 1) \rceil \leqslant d$, т. е. при этом условии значение $m(d, n)$ существует; если $n \geqslant 2^d$, то при любом m число существенных переменных функций $f_{2n,0}$ и $f^*_{2n,0}$ будет больше 2^d, т. е. глубины d не хватит.

(iii) Как было сказано выше, число существенных переменных у функций $f_{2n,m}$ и $f^*_{2n,m}$ равно $n+m+1$. С другой стороны, оно не превышает 2^d. Поэтому $m \leqslant 2^d - n - 1$. Лемма 4 доказана.

Замечание 1. Легко видеть, что по определению ёмкости и в силу леммы 1 неравенство $d(2n, m) \leqslant d$ выполнено также при всех неотрицательных m, $m < m(d, n)$.

Несложно найти значения ёмкости $m(d,n)$ при малых d (в ряде случаев для этого достаточно проанализировать число существенных переменных соответствующих функций).

Пусть $d = 0$. Тогда $m(0,0) = 0$, поскольку среди монотонных булевых функций нулевую глубину имеют только функции с одной существенной переменной, что в терминах рассматриваемых функций $f_{2n,m}$ и $f^*_{2n,m}$ означает, что $n = m = 0$.

Пусть $d = 1$. Тогда $m(1,0) = 1$ и $m(1,1) = 0$, поскольку глубина 1 эквивалентна наличию ровно двух существенных переменных — в наших терминах это означает, что $n + m = 1$.

Пусть $d = 2$. Тогда $m(2,0) = m(2,1) = 2$, $m(2,2) = 1$ и $m(2,3) = 0$. В этом случае глубина определяется не только числом существенных переменных (их может быть как 3, так и 4, откуда для $m(2,n)$ извлекается лишь оценка $n - 3 \leqslant m(2,n) \leqslant n - 2$), но и видом функций $f_{2n,m}$ и $f^*_{2n,m}$. Рассмотрим случаи $m = 1, 2, 3$ по отдельности:

а) $m(2,0) \neq 3$, поскольку $f_{0,3}$ есть $x_0 \mathbin{\&} (x_1 \vee x_2 \mathbin{\&} x_3)$ — эта функция симметрична только относительно перестановки $x_2 \leftrightarrow x_3$, тогда как любая монотонная функция глубины 2 с четырьмя существенными переменными должна сохраняться при большем числе перестановок: общий вид подобных функций есть $(a * b) * (c * d)$, где звездочки могут быть заменены (в любых комбинациях) на знаки конъюнкции и дизъюнкции — коммутативных булевых операций;

б) $m(2,1) > 1$, так как $f_{2,2} = (x_0 \mathbin{\&} x_2) \mathbin{\&} (x_3 \vee x_4)$;

в) $m(2,2) > 0$, так как $f_{4,1}$ есть конъюнкция четырёх переменных;

г) $m(2,3) = 0$ в силу неотрицательности значений $m(d,n)$.

При бо́льших d оценим значения ёмкости $m(d,n)$ снизу. Для этого введём величину $M(d,n)$, определённую при $0 \leqslant d < 3$ и $0 \leqslant n < 2^d$ явно, $M(0,0) = 0$, $M(1,0) = M(1,1) = 0$, $M(2,0) = M(2,1) = 2$, $M(2,2) = M(2,3) = 0$, а при $d \geqslant 3$ и $0 \leqslant n < 2^d$ — рекурсивно:

$$M(d+1,n) = \begin{cases} M(d,n) + M(d, M(d,n)/2), & 0 \leqslant n < 2^d; \\ M(d, n - 2^d), & 2^d \leqslant n < 2^{d+1}. \end{cases}$$

(Данное определение корректно, поскольку, как легко проверить индукцией по d, значения $M(d,n)$ чётные и не превосходят 2^d.)

Центральным моментом нашего доказательства является переход от «содержательной» величины — ёмкости $m(d,n)$ — к «формально числовой» функции $M(d,n)$. Данный переход выражает следующая лемма.

Лемма 5. *$M(d,n) \leqslant m(d,n)$ при $d \geqslant 0$ и $0 \leqslant n < 2^d$.*

Доказательство. При $d < 3$ неравенство $m(d,n) \geqslant M(d,n)$ проверяется непосредственно (все существующие значения обеих величин были перечислены выше). Для $d \geqslant 3$ воспользуемся индукцией. Пусть при некотором d, $d \geqslant 3$, и всех n, $0 \leqslant n < 2^d$, неравенство $m(d,n) \geqslant M(d,n)$ доказано. Оценим снизу $m(d+1,n)$ при $0 \leqslant n < 2^{d+1}$.

Пусть $n < 2^d$. Положим $k = M(d,n)/2$, $m = M(d,k)$, $m' = 2k + m + 1 \geqslant M(d+1,n)$. В силу леммы 3 значение $d(2n,m') = d(2n, 2k + m + 1)$ не превосходит $1 + \max(d(2n,2k), d(2k,m))$. В силу сделанного выбора параметров и предположения индукции оба значения, из которых выбирается максимальное, не превосходят d:

$$\begin{aligned} d(2n,2k) &= d(2n, M(d,n)) \leqslant d(2n, m(d,n)) = d,\\ d(2k,m) &= d(2k, M(d,k)) \leqslant d(2k, m(d,k)) = d, \end{aligned}$$

так что $d(2n,m') \leqslant d+1$. Поэтому $m(d+1,n) \geqslant m' \geqslant M(d+1,n)$.

Случай $n \geqslant 2^d$ рассматривается аналогично. Положим $n' = 2^d$, $k = n - 2^d$, $m = M(d,k)$. По лемме 2 значение $d(2n,m) = d(2n' + 2k, m)$ не превосходит $1 + \max(\lceil \log_2 n' \rceil, d(2k,m)) = 1 + \max(d, d(2k, M(d,k)))$. В силу сделанного выбора параметров и предположения индукции имеем $d(2k,m) = d(2k, M(d,k)) \leqslant d(2k, m(d,k)) = d$, так что $d(2n,m) \leqslant d+1$. Тем самым $m(d+1,n) \geqslant m = M(d,k) = M(d+1,n)$. Лемма 5 доказана.

Следующие две леммы носят технический характер: от рекуррентно определенных величин $M(d,n)$ переходим к более простым явным выражениям и на их основе получаем явную оценку для $d(0,m)$.

Лемма 6. *При $d \geqslant 2$ и $0 \leqslant n < 2^d$ справедливо неравенство*

$$M(d,n) \geqslant \frac{2^d - 2 - n}{d}. \tag{4}$$

Доказательство. При $d \leqslant 4$ неравенство (4) проверяется непосредственно:

значения $M(2,n)$, $n = 0,\ldots,3$, суть $2, 2, 0, 0$ (см. выше), тогда как оценка (4) даёт $1, 1/2, 0, -1/2$;

значения $M(3,n)$, $n = 0,\ldots,7$, суть $4, 4, 2, 2, 2, 2, 0, 0$, что вычисляется непосредственным применением определения величины M; оценка (4) даёт $2, 5/3, 4/3, 1, 2/3, 1/3, 0, -1/3$;

значения $M(4,n)$, $n = 0,\ldots,15$, суть 6, 6, 6, 6, 6, 6, 4, 4, 4, 4, 2, 2, 2, 2, 0, 0, что вычисляется тем же способом; оценка (4) даёт 7/2, 13/4, 3, 11/4, 5/2, 9/4, 2, 7/4, 3/2, 5/4, 1, 3/4, 1/2, 1/4, 0, −1/4.

Пусть теперь неравенство (4) выполнено для некоторого d, $d \geqslant 4$. Оценим $M(d+1,n)$.

Пусть $0 \leqslant n < 2^d$. Запишем

$$x + M\left(d, \frac{x}{2}\right) \geqslant \frac{2^d - 2}{d} + \left(1 - \frac{1}{2d}\right)x,$$

подставим $M(d,n)$ вместо x и, пользуясь тем, что коэффициент при x в последнем выражении неотрицателен, получим

$$\begin{aligned} M(d+1,n) = M(d,n) + M\left(d, \frac{M(d,n)}{2}\right) &\geqslant \frac{2^d-2}{d} + \left(1 - \frac{1}{2d}\right)\frac{2^d - 2 - n}{d} \\ &= \frac{2^d-2}{d}\left(2 - \frac{1}{2d}\right) - \frac{n}{d}\left(1 - \frac{1}{2d}\right). \end{aligned}$$

Последнее выражение при $d \geqslant 4$ и $0 \leqslant n \leqslant 2^{d+1} - 2$ не меньше $(2^{d+1} - 2 - n)/(d+1)$, что несложно проверить, например, сравнив значения этих двух линейных функций на концах указанного отрезка, т. е. в точках $n = 0$ и $n = 2^{d+1} - 2$. Поэтому при $0 \leqslant n < 2^d$ неравенство $M(d+1,n) \geqslant (2^{d+1} - 2 - n)/(d+1)$ доказано.

Случай $2^d \leqslant n \leqslant 2^{d+1} - 2$ существенно проще:

$$\begin{aligned} M(d+1,n) &= M(d, n - 2^d) \\ &\geqslant \frac{2^d - 2 - (n - 2^d)}{d} = \frac{2^{d+1} - 2 - n}{d} \geqslant \frac{2^{d+1} - 2 - n}{d+1}. \end{aligned}$$

Случай $n = 2^{d+1} - 1$ самый простой: величина $M(d+1,n)$ по определению является неотрицательной, а искомая оценка отрицательна. Лемма 6 доказана.

Лемма 7. *При $m \geqslant 2$ имеет место неравенство*

$$d(0,m) \leqslant \log_2 m + \log_2 \log_2 m + 2.$$

Доказательство. При $n = 0$ и $d = d(0,m)$ из лемм 5 и 6 следует неравенство $m \geqslant (2^d - 2)/d$. Запишем его в виде

$$d \leqslant \log_2(md + 2). \tag{5}$$

Подставив в правую часть этого неравенства оценку $d \leqslant m$, непосредственно вытекающую из определения функций $f_{0,m}$ и $f^*_{0,m}$, получим $d \leqslant \log_2(m^2 + 2)$; при $m \geqslant 2$ отсюда следует, что $d < 2\log_2 m + 1$.

Подставив полученную оценку для d в правую часть неравенства (5), получим

$$
\begin{aligned}
d &< \log_2(m(2\log_2 m + 1) + 2) \\
&= \log_2 m + \log_2\log_2 m + \log_2\left(2 + \frac{1}{\log_2 m} + \frac{2}{m\log_2 m}\right) \\
&\leqslant \log_2 m + \log_2\log_2 m + 2.
\end{aligned}
$$

Лемма 7 доказана.

3. Новые верхние оценки глубины сумматора и компаратора

Обозначим через $D_{add}(n)$ глубину (в базисе $\{\&, \vee, \sim\}$) n-разрядного сумматора, т. е. набора $Z = [z_n, \ldots, z_0]$ двоичных разрядов суммы $Z = A + B$ двух n-разрядных чисел $A = [a_{n-1}, \ldots, a_0]$ и $B = [b_{n-1}, \ldots, b_0]$.

Теорема 1. *При $n \geqslant 2$ справедливо неравенство*

$$D_{add}(n) \leqslant \log_2 n + \log_2\log_2 n + 7. \tag{6}$$

Доказательство. Известно (см., например, [1, 5]), что задача сложения по существу эквивалентна вычислению функций вида $f_{0,m}$ в том смысле, что глубина сумматора лишь на небольшую константу отличается от глубины функции $f_{0,m}$ с тем же числом входов. Действительно, положим $a_n = b_n = 0$; тогда каждый разряд z_i суммы выражается в виде $(a_i \oplus b_i) \oplus c_i$, где c_i есть i-й разряд переноса:

$$
\begin{aligned}
&c_0 = 0, \\
&c_1 = a_0 b_0, \\
&c_2 = a_1 b_1 \vee (a_1 \vee b_1) c_1, \\
&c_3 = a_2 b_2 \vee (a_2 \vee b_2) c_2, \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
&c_{i+1} = a_i b_i \vee (a_i \vee b_i) c_i, \\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

Нетрудно видеть, что

$$c_{i+1} = f^*_{0,2i}(a_i b_i, a_i \vee b_i, a_{i-1} b_{i-1}, a_{i-1} \vee b_{i-1}, \ldots, a_1 b_1, a_1 \vee b_1, a_0 b_0).$$

Поэтому $D_{add}(n) \leqslant d(0, 2n-2) + 4$: глубина увеличивается на 1 при вычислении значений переменных функции f^*, и не более чем на 3 при

вычислении $(a_i \oplus b_i) \oplus c_i$. Далее воспользуемся леммой 7 и заметим, что при $n \geqslant 2$ имеет место неравенство

$$\log_2(2n-2) + \log_2\log_2(2n-2) \leqslant \log_2 n + \log_2\log_2 n + 1.$$

Теорема 1 доказана.

Обозначим через $D_{cmp}(n)$ глубину (снова в базисе $\{\&, \vee, \sim\}$) n-разрядного компаратора — функции $2n$ булевых переменных, истинной (равной 1) при $A < B$, где $A = [a_{n-1}, \ldots, a_0]$ и $B = [b_{n-1}, \ldots, b_0]$, и ложной (равной 0) в противном случае.

Теорема 2. *При $n \geqslant 2$ имеет место неравенство*

$$D_{cmp}(n) \leqslant \log_2 n + \log_2\log_2 n + 6. \tag{7}$$

Доказательство. Сравнение $A < B$ реализуется, например, посредством

$$f^*_{0,2n-2}(a_{n-1} < b_{n-1}, a_{n-1} = b_{n-1}, a_{n-2} < b_{n-2}, a_{n-2} = b_{n-2}, \\ \ldots, a_1 < b_1, a_1 = b_1, a_0 < b_0),$$

так что $D_{cmp}(n) \leqslant d(0, 2n-2) + 3$ (не более трех единиц глубины будет затрачено на вычисление переменных функции f^*). Переход от этого неравенства к (7) делается в точности так же, как в теореме 1. Теорема 2 доказана.

Замечание 2. Аддитивные константы в (6) и (7) сильно завышены, уточнение их значений не было целью настоящей статьи.

4. Заключительное замечание

Полученные верхние оценки вида $\log_2 n + \log_2\log_2 n + O(1)$ сильно отличаются от нижней оценки В. М. Храпченко [5]:

$$D_{add}(n) \geqslant \log_2 n + 0{,}15\log_2\log_2\log_2 n + O(1).$$

Вероятно, ближе к окончательной является верхняя оценка: проводившиеся автором вычислительные эксперименты свидетельствуют в пользу того, что по крайней мере в классе схем в монотонном базисе $\{\&, \vee\}$ величина $m(d, 0)$ ведёт себя как $\frac{2^d}{d}(C + o(1))$, где $4 < C < 5$. Поэтому существенного (более чем на $O(1)$) снижения глубины сумматоров и компараторов (если оно вообще возможно) следует искать, видимо, в классе существенно немонотонных методов вычисления функций f^*.

Автор пользуется случаем выразить благодарность А. А. Болотову и С. Б. Гашкову за многолетнее внимание к работе и полезные обсуждения, а И. С. Сергееву и С. В. Грибку за то, что они своим активным интересом к проблеме побудили автора быстрее довести исследования до в какой-то мере завершённого вида.

ЛИТЕРАТУРА

1. **Гашков С. Б., Гринчук М. И., Сергеев И. С.** О построении схем сумматоров малой глубины // Дискретный анализ и исследование операций. Серия 1. 2007. Т. 14, №1. С. 27–44.
2. **Лупанов О. Б.** Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.
3. **Редькин Н. П.** О минимальной реализации двоичного сумматора // Проблемы кибернетики. Вып. 38. М.: Наука, 1981. С. 181–216.
4. **Храпченко В. М.** Об асимптотической оценке времени сложения параллельного сумматора // Проблемы кибернетики. Вып. 19. М.: Наука, 1967. С. 107–122.
5. **Храпченко В. М.** Об одной из возможностей уточнения оценок для задержки параллельного сумматора // Дискрет. анализ и исслед. операций. Сер. 1. 2007. Т. 14, № 1. С. 87–93.
6. **Gashkov S. B., Andreev A. E., Lu A.** Optimization of comparator architecture / United States patent 6691283. 10.2.2004.
7. **Gashkov S. B., Andreev A. E., Lu A.** Optimization of adder based circuit architecture / United States patent 6934733. 23.8.2005.
8. **Grinchuk M. I.** Low depth circuit design. United States patent application. 2008.
9. **Grinchuk M. I., Bolotov A. A.** Process for designing comparators and adders of small depth / United States patent 7020865. 28.3.2006.
10. **Savage J. E.** The complexity of computing. New York etc.: Wiley-Interscience, 1976.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьёвы горы,
119992 Москва,
Россия.
E-mail: grinchuk@att.net

Статья поступила
15 февраля 2008 г.