И. С. Сергеев (Москва)

О глубине схем для многократного сложения и умножения чисел[1]

В настоящей работе рассматривается подход к построению схем из функциональных элементов, реализующих многократное сложение и умножение чисел с небольшой глубиной. Обзорная лекция, посвященная минимизации глубины таких схем, была прочитана А. В. Чашкиным на одной из предыдущих школ этой серии [6]. Схемы строятся над базисом из всех двухвходовых элементов. Понятия сложности и глубины схем изложены в [3].

В начале 60-х гг. Ю. П. Офман [2] и ряд зарубежных авторов (см. [8]) предложили способ реализации умножения n-разрядных чисел схемой глубины $O(\log n)$. В этом способе умножение сводится к n-кратному сложению (как в школьном методе), которое, в свою очередь, сводится к обычному сложению при помощи схемы компрессоров.

Под (p, q)-компрессором, где $q < p$, понимается схема, по набору из p чисел вычисляющая q новых чисел с сохранением суммы, и имеющая глубину, не зависящую от разрядности слагаемых. Самым простым и наиболее популярным является (3,2)-компрессор. Он преобразует набор из трех чисел $X = [x_{k-1}, \ldots, x_0]$, $Y = [y_{k-1}, \ldots, y_0]$, $Z = [z_{k-1}, \ldots, z_0]$ в пару чисел $U = [u_k, \ldots, u_1, 0]$ и $V = [v_{k-1}, \ldots, v_0]$, таких, что $U + V = X + Y + Z$. Пара разрядов (u_{i+1}, v_i) вычисляется подсхемой, изображенной на рис. 1. Таким образом, k-разрядный (3,2)-компрессор имеет сложность $5k$ и глубину 3.

При оптимизации глубины схем из (3,2)-компрессоров существенно используется несимметричность глубин выходов компрессора относительно глубин входов. В стандартном способе из двух (3,2)-компрессоров строится (4,2)-компрессор, используя который несложно построить схему сведения n-кратного сложения к обычному с глубиной $4\lceil \log_2 n \rceil - 3$ (эта конструкция описана в [6] для другой интерпретации входов и с менее аккуратной оценкой глубины).

Обозначим через $D(n)$ глубину минимальной реализации сведения n-кратного сложения к обычному схемой из (3,2)-компрессоров.

[1]Материалы VI молодежной школы по дискретной математике и ее приложениям (Москва, 16–21 апреля 2007 г.) — М.: Изд-во ИПМ РАН, 2007. — Ч. II. — С. 40–45.

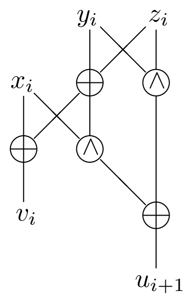

Рис. 1

В дальнейшем для упрощения изложения, под входами и выходами компрессора будут пониматься числа-слагаемые, глубину числа определяет разряд с наибольшей глубиной. Асимптотически точная оценка величины $D(n)$ была получена в [8]. Пусть $\lambda = 1,205\ldots$ — единственный вещественный корень уравнения $\lambda^3 + \lambda^2 - \lambda - 2 = 0$. Справедлива

Теорема 1 [8]. $\log_\lambda n - 3,3 < D(n) < \log_\lambda n + O(1)$.

Отметим, что $\log_\lambda n \approx 3,71 \log_2 n$. Нижняя оценка следует из соотношения $\lambda^{D(n)} + \lambda^{D(n)-1} \geq n$, которое вытекает из следующей простой леммы.

Лемма 1. *Пусть a, b, c — глубины входов $(3,2)$-компрессора; d и $d-1$ — глубины выходов, тогда $\lambda^d + \lambda^{d-1} \geq \lambda^a + \lambda^b + \lambda^c$.*

Верхняя оценка доказывается в [8] общим, но практически не эффективным методом. Константа, которая скрывается за обозначением $O(1)$, достаточно велика; кроме того, построенная методом [8] схема содержит примерно в шесть раз больше компрессоров, чем необходимо. На самом деле, верна

Теорема 2. *Для любого $n > 3$ выполнено: $D(n) > \log_\lambda n - 2,7$. Кроме того, существует схема Λ сведения n-кратного сложения к обычному, состоящая из $n-2$ компрессоров, глубина которой не превосходит $\log_\lambda n - 0,8$, а сложность — $5(nk + 4n - 2k)$, где k — разрядность суммируемых чисел.*

Перед тем, как дать пояснения к доказательству, введем некоторые понятия. Будем считать компрессор расположенным на глубине d, если его выходы имеют глубины $d+2$ и $d+3$. Пусть $T \subset \mathbf{N} \cup \{0\}$. Положим $\sigma(T) = \sum_{t \in T} \lambda^t$. Через S_r обозначим схему, образованную компрессорами схемы S, расположенными на глубинах, меньших r. Через $T(S_r)$ обозначим множество глубин выходов схемы S_r, в котором числа, меньшие r, заменены на r. Положим $\sigma(S_r) = \sigma(T(S_r))$. Из леммы 1 очевидно, что

$$n = \sigma(S_0) \leq \sigma(S_1) \leq \ldots \leq \sigma(S_{d-2}) = \lambda^d + \lambda^{d-1}, \qquad (*)$$

где n — число входов, а d — глубина схемы S.

Нижняя оценка теоремы 2 следует из $(*)$ и неравенств

$$\sigma(S_1) - \sigma(S_0) \geq n(\lambda - 1)/3, \quad \sigma(S_{d-2}) - \sigma(S_{d-6}) \geq \lambda^{d-5}(\lambda - 1),$$

справедливых для произвольной схемы S.

Для доказательства верхней оценки используется очевидный метод последовательного добавления компрессоров в схему, в котором каждый очередной компрессор располагается на возможно меньшей глубине. При оценке глубины построенной схемы Λ ключевой является следующая лемма, которая доказывается по индукции.

Лемма 2. *Пусть $r > 0$, а m_0, m_1 и m_2 — соответственно количество чисел r, $r+1$ и $r+2$ во множестве $T(\Lambda_r)$. Тогда выполнено:*

$$m_0 \leq 2m_1 + 2, \quad m_1 \leq 1,5m_0 + 2m_2, \quad m_2 \leq m_1.$$

Обозначим $\Delta_r = \sigma(\Lambda_{r+1}) - \sigma(\Lambda_r)$. По построению, $\Delta_r = a_r(\lambda - 1)\lambda^r$, $a_r \in \mathbf{Z}$. Из первого неравенства леммы следует, что $a_r \leq 2$. При этом, если $a_r = 2$, то, как легко убедиться, $a_{r+1} = 0$. Принимая во внимание $a_{d-4} \leq 1$ и $a_{d-3} = 0$ (где d — глубина Λ), получаем

$$\sigma(\Lambda_{d-2}) - \sigma(\Lambda_1) \leq (\lambda - 1) \sum_{i=1}^{d-4} \lambda^i,$$

что, с учетом $\Delta_0 \leq (\lambda-1)(2+n/3)$, приводит к окончательной оценке $d < \log_\lambda n - 0,8$.

Оценка сложности схемы Λ складывается из величины $5k(n-2)$, отвечающей числу компрессоров, и добавочного члена, отвечающего удлинению чисел-слагаемых с увеличением глубины. Последний оценивается величиной $20n$, что выводится из следующих легко проверяемых фактов: (1) количество компрессоров, расположенных на глубине r не превосходит $(\lambda+1)\lambda^{d-r-1}/(\lambda+2)$ и (2) выход некоторого компрессора, имеющий глубину r, является не более чем $(k+\lfloor r/3\rfloor)$-разрядным числом.

Нижняя оценка теоремы 2 показывает, что глубина постренной схемы не более чем на единицу отличается от оптимальной. Схема, построенная стандартным способом, имеет худшую глубину для всех n, кроме 4, 8, 16, 32, для которых оба метода дают одинаковый результат.

Для окончательного вычисления суммы выходы схемы компрессоров подаются на входы сумматора. Сумматор n-разрядных чисел, построенный методом В. М. Храпченко [4], имеет асимптотически оптимальную глубину $(1+o(1))\log_2 n$. Для n в пределах нескольких тысяч выгоднее использовать другие методы, например, метод М. И. Гринчука с верхней оценкой глубины $2\log_3(16\lfloor n/2\rfloor)$ (см. [1]). Так, для умножения справедливо

Следствие. *Существует схема умножения двух n-разрядных чисел сложности $O(n^2)$ и глубины не более* $5(\log_2 n+1)$.

Для сравнения, вариантом метода А. А. Карацубы [2] можно построить схему с асимптотически меньшим порядком сложности $n^{\log_2 3}$, но с глубиной $(11+o(1))\log_2 n$ (см. [6], но там приводится менее аккуратная оценка глубины). Метод Карацубы обычно не применяется при $n<300$. Вариант метода Шёнхаге—Штрассена [10] имеет сложность $O(n\log n\log\log n)$ и глубину $(9+o(1))\log_2 n$, однако почти не используется на практике.

Отметим, что компрессоры удобно использовать для вычислений по модулю 2^k-1 (перенося k-е разряды промежуточных слагаемых на место младших). В целях минимизации глубины для реализации заключительного модулярного сложения двух чисел можно использовать $2k$-разрядный сумматор.

В заключение несколько замечаний о применении более сложных компрессоров. Примеры компрессоров, асимптотически более эффективных, чем (3,2)-компрессор, приводились в работах [5] (для базиса $\{\wedge,\vee,\bar{\ }\}$) и [8]. Известны, например, (5,3)-компрессор и (6,3)-компрессор, из которых методом [8] строятся схемы сведения n-кратного сложения к обычному с глубиной асимптотически $3,65\log_2 n$ и $3,57\log_2 n$ соответственно. Можно также построить (11,5)-компрессор с показателем эффективности $3,55\log_2 n$. Для получения наилучшей известной асимптотической оценки $3,44\log_2 n$ [7] используются схемы из т. н. полукомпрессоров [9].

Методы [7–9] сугубо теоретические, однако предложенные компрессоры можно использовать для построения практических схем небольшой глубины. Используя (5,3) и (6,3)-компрессоры наряду с (3,2)-компрессорами, можно строить схемы меньшей глубины, чем описано выше, уже при малых n, в частности, при $n = 32$. Специальный (7,3)-компрессор позволяет реализовать умножение по методу Карацубы с глубиной $(10 + o(1)) \log_2 n$. Уменьшение глубины во всех случаях достигается ценой некоторого увеличения сложности: кажется, неизвестны (p, q)-компрессоры, у которых отношение сложности к $p - q$ меньше, чем $5k$, где k —разрядность слагаемых.

Автор признателен научному руководителю С. Б. Гашкову за постановку задачи и внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы «Ведущие научные школы» (проект НШ–5400.2006.1) и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

Список литературы

[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] Карацуба А. А., Офман Ю. П. Умножение многозначных чисел на автоматах. // Докл. АН СССР. — 1962. — Т. 145(2). — С. 293–294.

[3] Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд. МГУ, 1984.

[4] Храпченко В. М. Об асимптотической оценке времени сложения параллельного сумматора. // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 107–120.

[5] Храпченко В. М. Некоторые оценки для времени умножения. // Проблемы кибернетики. Вып. 33. — М.: Наука, 1978. — С. 221–227.

[6] Чашкин А. В. Быстрое умножение и сложение целых чисел. // В сб. «Дискретная математика и ее приложения». II. — М.: изд-во ЦПИ при мех.-мат. ф-те МГУ, 2001. — С. 91–110.

[7] Grove E. Proofs with potential. — Ph.D. thesis, U.C. Berkeley, 1993.

[8] Paterson M., Pippenger N., Zwick U. Optimal carry save networks. // LMS Lecture Notes Series. — V. 169. Boolean function Complexity. — Cambridge University Press, 1992. — P. 174–201.

[9] Paterson M., Zwick U. Shallow circuits and concise formulae for multiple addition and multiplication. // Comput. Complexity. — 1993. — V. 3. — P. 262–291.

[10] Schönhage A., Strassen V., Schnelle multiplikation großer zahlen. // Computing. — 1971. — V. 7. — P. 271–282. [Русский перевод: Шёнхаге А., Штрассен В. Быстрое умножение больших чисел. // Кибернетический сборник. Вып. 10. — М.: Мир, 1973. — С. 87–98].