

БЫСТРЫЕ КЛЕТОЧНЫЕ СХЕМЫ ДЛЯ УМНОЖЕНИЯ*)

Д. А. Жуков

Показано, что существует клеточная схема глубины $\Theta(\log n)$ и площади $\Theta(n^2 \log n)$, которая вычисляет произведение двух n -рядных чисел, заданных в двоичной системе счисления.

Введение

Рассматривается вычисление произведения двух целых чисел, заданных в двоичной системе счисления, клеточными схемами [3, 6]. Клеточная схема имеет вид прямоугольника на плоскости, составленного из клеточных элементов. Под сложностью клеточной схемы понимается занимаемая ею площадь. Будем считать, что длина клеточной схемы измеряется по горизонтали, а ширина — по вертикали. Длину схемы S обозначим через $l(S)$, а ширину — через $h(S)$. Тогда площадь схемы S равна $l(S)h(S)$. Клеточный элемент называется *функциональным*, если он реализует нетождественную булеву функцию, и *коммутационным*, если он реализует тождественные функции. Кроме функциональных и коммутационных элементов имеется изолирующий клеточный элемент без входов и выходов. Предполагается, что каждая булева функция, существенно зависящая не более чем от двух переменных, реализуется некоторым функциональным элементом.

Цепью в клеточной схеме называется последовательность клеточных элементов, в которой выход каждого элемента, кроме последнего, соединен с входом следующего. *Длиной* цепи называется число содержащихся в ней функциональных элементов. Цепь наибольшей длины, соединяющая некоторый вход схемы с ее выходом, называется *максимальной*. *Глубиной* клеточной схемы называется длина максимальной цепи в ней.

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 99–01–01175, 00–15–96103), программы «Университеты России» (проект 992206) и Федеральной целевой программы «Интеграция» (объединенный проект АО–110).

С. С. Кравцов в [3] описал метод построения клеточных схем, реализующих произвольные булевы функции от n переменных. Глубина построенной им схемы экспоненциальна по n , но легко может быть сделана линейной; при этом площадь схемы останется оптимальной по порядку. Н. А. Шкаликова в [6] исследовала сложность реализации булевых функций из специальных классов. В частности, она доказала, что площадь каждой клеточной схемы, осуществляющей умножение двух n -разрядных чисел, заданных в двоичной системе счисления, не меньше $\Theta(n^2)$, и привела пример схемы площади $\Theta(n^2)$ и глубины $\Theta(n)$. В данной статье предложен способ построения клеточной схемы для умножения двух n -разрядных чисел с глубиной $\Theta(\log n)$.

Теорема. *Произведение двух n -разрядных целых чисел, заданных в двоичной системе счисления, может быть вычислено клеточной схемой глубины $\Theta(\log n)$ и площади $\Theta(n^2 \log n)$, состоящей из двоичных клеточных элементов.*

Глубина полученной схемы оптимальна по порядку, но ее площадь несколько больше площади схемы из [6]. Известно [5], что существует схема из функциональных элементов, умножающая два n -разрядных числа со сложностью $\Theta(n \log n \log \log n)$ и глубиной $\Theta(\log n)$. Нетрудно убедиться [2], что по схеме из функциональных элементов глубины d и размера L можно построить клеточную схему площади L^2 с такой же глубиной, реализующую тот же булев оператор. Поэтому из теоремы Шенхаге — Штрассена [5] следует существование клеточной схемы для умножения n -разрядных чисел с глубиной $\Theta(\log n)$ и площадью $\Theta(n^2 \log^2 n \log^2 \log n)$.

Константа, стоящая перед логарифмом в оценке глубины схемы Шенхаге — Штрассена, достаточно велика. Развивая результат В. М. Храпченко [4], М. Paterson, N. Pippenger, U. Zwick в [7] доказали, что существуют схемы (из функциональных элементов) для умножения двух n -разрядных чисел с глубиной, асимптотически не превосходящей $4,57 \log_2 n$, и сложностью $\Theta(n^2)$. Их результат является наилучшей оценкой глубины схем для умножения из известных на данный момент. Метод, аналогичный изложенному ниже, можно использовать для моделирования схем из работы [7] клеточными схемами. Остается открытым вопрос, можно ли уменьшить площадь схемы для умножения двух чисел так, чтобы ее глубина осталась оптимальной по порядку.

Доказательство теоремы. Введем операцию объединения клеточных схем. Пусть даны схемы S и S' . Пусть в схеме S каким-либо образом выбраны горизонтальный и вертикальный отрезки α и β . Они делят схему S на четыре прямоугольника — подсхемы A, B, C, D (рис. 1, а). Раздвинем части A, B, C и D на такое расстояние, чтобы

между ними поместилась схема S' (рис. 1, b). Лежащие на границах схем A, B, C, D клеточные элементы соединяются друг с другом коммутационными элементами по тем же правилам, что и в схеме S . В зависимости от задачи на входы схемы S' могут подаваться как пограничные выходы подсхем A, B, C, D .

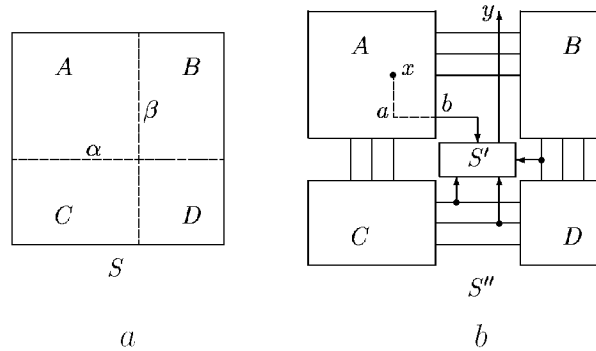


Рис. 1

На рис. 1, b приведен пример, как один такой вход соединить с внутренней вершиной x подсхемы A . При этом должно выполняться условие: на вертикальном участке от точки x до точки a находятся только элементы, изображенные на рис. 2, a или изолирующие, а на отрезке ab — только изображенные на рис. 2, b или изолирующие. Тогда, заменяя все клеточные элементы на штриховой линии от точки x до точки b на элементы приведенного на рис. 2, c вида, получим цепь из коммутационных элементов, соединяющую точку x с точкой b и не нарушающую других цепей в подсхеме A .

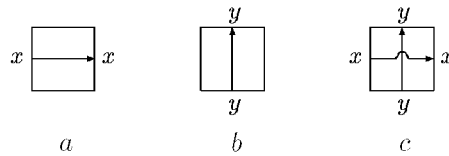


Рис. 2

Полученную схему S'' назовем *объединением* клеточных схем S и S' . Выходами схемы S'' могут быть как выходы схемы S — они по построению находятся на границе схемы S'' , так и выходы схемы S' , например отмеченный на рис. 1 выход y . Отметим также, что $l(S'') = l(S) + l(S')$ и $h(S'') = h(S) + h(S')$. Схему S можно разрезать на две, а не на четыре части, или не разрезать, добавляя к ней схему S' сбоку. Аналогично можно определить комбинацию, полученную добавлением к схеме S не одной, а нескольких схем, разрезая ее на большее число частей.

Следуя [4], назовем (n, k) -преобразователем всякую схему (клеточную или из функциональных элементов), у которой сумма k чисел на ее выходах равна сумме n чисел на ее входах. Удобно считать, что входы и выходы клеточного (n, k) -преобразователя не обязательно находятся на его границе.

Рассмотрим схему F с тремя входами и двумя выходами. На ее выходах появляются разряды суммы входов. Схема F — это так называемый счетчик разрядов. Легко видеть, что счетчик F реализуется клеточной схемой длины 5, ширины 6 и глубины 3. Указанные константы для дальнейшего изложения несущественны.

Способ построения простейшего $(n, 2)$ -преобразователя глубины $\Theta(\log n)$ основан на использовании схемы F . Объединим разряды (с одинаковым номером) трех m -разрядных чисел. Возьмем m экземпляров схемы F и подадим на вход каждого экземпляра соответствующую тройку разрядов. На выходах схем F появятся разряды двух чисел, сумма которых равна сумме трех исходных, т. е. получился $(3, 2)$ -преобразователь. Его особенность — линейная по m сложность и не зависящая от m глубина. С помощью $(3, 2)$ -преобразователя $(n, 2)$ -преобразователь легко строится по индукции. На первом шаге исходные n штук m -разрядных слагаемых разбиваются на группы по три, за исключением последней группы, которая может быть неполной. К каждой полной группе параллельно с другими применяется $(3, 2)$ -преобразование. В результате число слагаемых уменьшается примерно в 1,5 раза. Аналогично выполняются второй шаг, третий и т. д. Когда останутся два слагаемых, алгоритм заканчивает работу. Нетрудно видеть, что $(n, 2)$ -преобразователь имеет глубину $\Theta(\log n)$ и при его построении используется $\Theta(n^2)$ функциональных элементов, если $m = \Theta(n)$. Остается перенести этот алгоритм на плоскость, используя как можно меньше коммутационных элементов.

Лемма 1. Пусть имеется клеточная схема S , внутри которой в узлах прямоугольной решетки размера $n \times 3$ находятся разряды трех целых n -разрядных чисел x , y и z . Тогда объединением схемы S и n экземпляров счетчика F можно получить клеточный $(3, 2)$ -преобразователь S' , выходами которого будут разряды $(n + 1)$ -разрядных чисел a и b , сумма которых $a + b$ равна сумме $x + y + z$. Длина и ширина схемы S' удовлетворяют неравенствам

$$l(S') \leq l(S) + 6, \quad h(S') \leq h(S) + 10n + 4,$$

а ее глубина превышает глубину схемы S не более чем на 3.

Доказательство. Процесс построения схемы S' изображен на рис. 3. По условию разряды чисел x , y и z расположены внутри схемы S

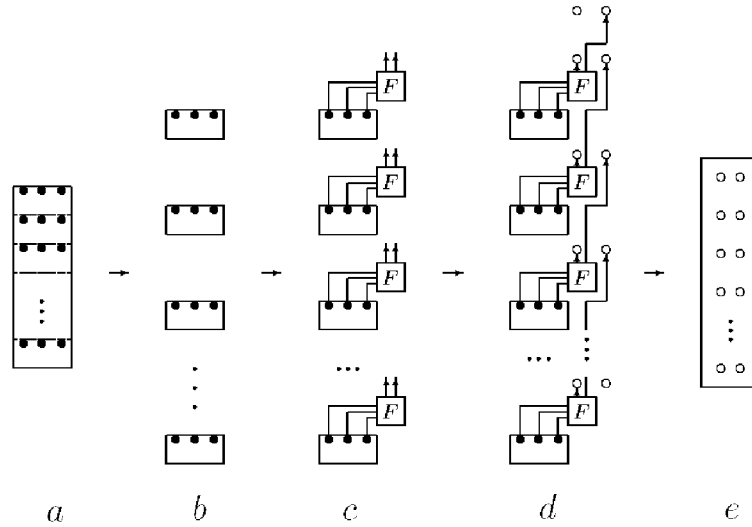


Рис. 3

так, что разряды с одинаковыми номерами лежат на одной горизонтальной прямой (рис. 3, *a*, разряды слагаемых отмечены закрашенными кружками).

Разрежем схему S на n не обязательно равных частей-подсхем, чтобы в каждой подсхеме было по три разряда и они лежали на ее границе (рис. 3, *b*). Объединим эти части с n экземплярами схемы F , соединив каждые три разряда с входами схемы F коммутационными элементами (рис. 3, *c*, связи между подсхемами для простоты не указаны). На выходах схем F получим $2n$ разрядов двух чисел, сумма которых равна сумме трех исходных. Пусть для определенности младшие разряды на выходах схем F находятся слева, а старшие — справа. Теперь сделаем так, чтобы, как и в исходной схеме, те разряды слагаемых, которые имеют одинаковые номера, лежали на одной горизонтальной прямой (рис. 3, *d*, полученные разряды отмечены незакрашенными кружками). При этом первый и последний разряды получившихся чисел оказываются непарными. Чтобы этого избежать, добавим к ним в пару фиктивные нулевые разряды (на рис. 3, *d* два незакрашенных кружка, к которым не подходят коммутационные элементы, обозначают функциональные элементы, реализующие константу 0). На рис. 3, *e* изображен общий вид полученной схемы S' .

Так можно встроить (3,2)-преобразователь в любую схему, если внутри нее разряды слагаемых расположены указанным образом. Оценки длины, ширины и глубины схемы S' следуют из приведенных рассуждений с учетом параметров схемы F . Лемма 1 доказана.

Лемма 2. Существует клеточный $(n, 2)$ -преобразователь, получающий из n штук m -разрядных слагаемых, $m = \Theta(n)$, два слагаемых с той же суммой и имеющий следующие параметры: глубина $\Theta(\log n)$, длина $\Theta(n)$, ширина $\Theta(n \log n)$ и, следовательно, площадь $\Theta(n^2 \log n)$.

Доказательство. Пусть на l -м шаге построена схема S_l . Она осуществляет $(n, N(l))$ -преобразование, где $N(l)$ — число слагаемых на шаге l , $N(0) = n$. На ее основе построим схему S_{l+1} . По предположению индукции разряды слагаемых расположены внутри схемы S_l в узлах прямоугольной решетки так, как изображено на рис. 4, а.

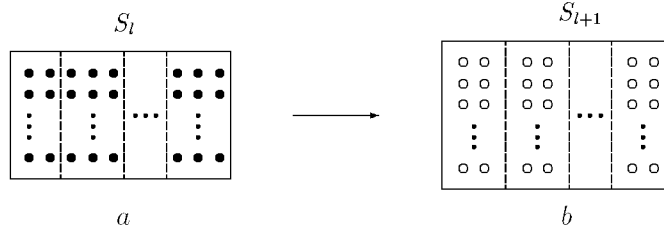


Рис. 4

Разрежем S_l вдоль штриховых линий на подсхемы так, чтобы в каждой подсхеме было по три слагаемых (в последней подсхеме их может быть меньше). К каждой подсхеме, за исключением, быть может, последней, применим $(3, 2)$ -преобразование, описанное в лемме 1. Если в последней подсхеме менее трех слагаемых, то выведем их разряды коммутационными элементами на соответствующие горизонтали, как в доказательстве леммы 1. Полученная схема S_{l+1} (рис. 4, б) имеет то же расположение выходов, что и схема S_l : разряды каждого слагаемого лежат на одной вертикальной прямой, разряды разных слагаемых с одинаковыми номерами — на одной горизонтальной. К схеме S_{l+1} снова можно применить шаг индукции.

Пусть $N(l)$ — число слагаемых в схеме S_l на l -м шаге. С ростом числа l число $N(l)$ уменьшается и для некоторого $l = \log_{3/2} n + O(1)$ станет равным двум. Полученная в этот момент схема S_l реализует $(n, 2)$ -преобразование. Отметим, что эта схема не является клеточной в строгом смысле, так как ее входы и выходы не расположены на границе. Тем не менее ее можно использовать как подсхему.

Оценим параметры полученной схемы. Нетрудно видеть, что

$$N(l+1) \leq \frac{2}{3}N(l) + 2.$$

Глубина построенного $(n, 2)$ -преобразователя пропорциональна $\log n$, так как на очередном шаге построенная до того схема объединяется с подсхемой, глубина которой не зависит от n , и число шагов равно

$\Theta(\log n)$. По построению на каждом шаге для длины и ширины схемы S_{l+1} выполнены неравенства (здесь используются конкретные размеры счетчика разрядов F , не влияющие на порядок роста результата)

$$l(S_{l+1}) \leq l(S_l) + 6N(l), \quad h(S_{l+1}) \leq h(S_l) + M(l) \cdot 10 + 4,$$

где $M(l)$ — наибольшее число разрядов в слагаемых на l -м шаге. На нулевом шаге схема S_0 содержит n слагаемых по $m = \Theta(n)$ разрядов в каждом. Следовательно, $l(S_0) = \Theta(n)$ и $h(S_0) = \Theta(n)$. Также ясно, что $M(l) = \Theta(n)$ для рассматриваемых значений l . Отсюда следует, что $l(S_l) = \Theta(n)$ и $h(S_l) = \Theta(n \log n)$ при $l = \Theta(\log n)$. Поэтому площадь $(n, 2)$ -преобразователя не превосходит $\Theta(n^2 \log n)$. Лемма 2 доказана.

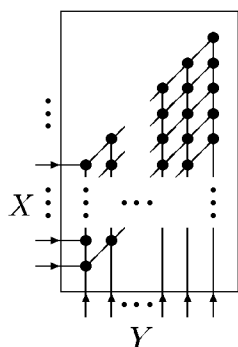


Рис. 5

Для завершения доказательства теоремы осталось заметить, что произведение n -разрядных чисел X и Y можно найти в три этапа. На первом этапе произведение представляется в виде суммы n штук $2n$ -разрядных чисел, как в алгоритме умножения «в столбик» (рис. 5). Полученная схема имеет размеры $\Theta(n) \times \Theta(n)$ и единичную глубину. Места недостающих разрядов заполняются нулями, и на следующем этапе к ней применяется $(n, 2)$ -преобразование, описанное в лемме 2. На завершающем этапе надо сложить два полученных

числа, сумма которых равна произведению XY . Как и в доказательстве леммы 1, соединим выходы $(n, 2)$ -преобразователя горизонтальными коммутационными элементами с его правой вертикальной стороной, и он станет полноценной клеточной схемой. Можно доказать [1], что существует клеточная схема длины $\Theta(\log n)$ и ширины $\Theta(n)$, определяющая сумму двух n -разрядных слагаемых (клеточный сумматор). Глубина этой схемы асимптотически оптимальна и равна $\log_2 n + \sqrt{2 \log_2 n} + 5 \sim \log_2 n$. Присоединив выходы $(n, 2)$ -преобразователя к входам такого сумматора, получим искомую схему для умножения двух чисел. Теорема доказана.

Автор выражает искреннюю благодарность А. В. Чашкину за постоянное внимание к работе и интересные обсуждения.

ЛИТЕРАТУРА

1. Жуков Д. А. Клеточные схемы для арифметических операций // Материалы Пятой молодежной научной школы по дискретной математике и ее приложениям (МГУ, ноябрь 2001 г.). М.: Изд-во мех.-мат. фак. МГУ, 2002. С. 50–52.

2. Колмогоров А. Н., Барздинь Я. М. О реализации сетей в 3-мерном пространстве // Проблемы кибернетики. Вып. 19. М.: Наука, 1967. С. 261–268.
3. Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. Вып. 19. М.: Наука, 1967. С. 285–293.
4. Храпченко В. М. Некоторые оценки для времени умножения // Проблемы кибернетики. Вып. 33. М.: Наука, 1978. С. 221–227.
5. Шенхаге А., Штрассен В. Быстрое умножение больших чисел // Кибернетический сборник. Нов. сер. Вып. 10. М.: Мир, 1973. С. 87–98.
6. Шкаликова Н. А. О реализации булевых функций схемами из клеточных элементов // Математические вопросы кибернетики. Вып. 2. М.: Наука, 1989. С. 177–197.
7. Paterson M. S., Pippenger N., Zwick U. Optimal carry save networks // Boolean function complexity. Cambridge: Cambridge Univ. Press, 1992. P. 174–201. (London Mathematical Society Lecture Note Series 169).

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьевы горы,
119992 Москва, Россия.
E-mail: oldbug@mail.ru

Статья поступила

27 мая 2002 г.