Д. Ю. Черухин (Москва)

Об обратимых схемах из функциональных элементов

Обратимые схемы из функциональных элементов были рассмотрены автором при обдумывании одной нерешённой проблемы теории сложности. Речь идёт о проблеме отыскания эффективных нелинейных нижних оценок сложности булевых функций или операторов в классе схем из функциональных элементов (СФЭ). Понятие эффективной нижней оценки неформально, суть его состоит в следующем: оцениваемая функция должна быть задана достаточно явно, вычисление её значения на каждом конкретном входном наборе не должно сводиться к перебору множества функций, для которого данная нижняя оценка выводится мощностным способом.

Мы будем рассматривать схемы из многополюсных функциональных элементов над произвольным базисом — полной конечной системой булевых операторов $B = \{F_1, \ldots, F_k\}$, F_i: $\{0,1\}^{n_i} \to \{0,1\}^{m_i}$. Сложностью схемы S считаем число входящих в неё элементов, сложностью булева оператора F в базисе B называем минимальную из сложностей схем в базисе B, реализующих оператор F. Сложность оператора F в базисе B обозначим через $L_B^{\text{СФЭ}}(F)$. Известно, что сложность любого оператора в классе схем из функциональных элементов по порядку не зависит от базиса, поэтому достаточно ограничиться рассмотрением сложности в одном базисе. В качестве стандартного базиса выберем базис из всех двуместных булевых функций; сложность оператора F в стандартном базисе обозначим через $L^{\text{СФЭ}}(F)$.

В настоящее время известны не более чем линейные эффективные нижние оценки сложности функций и операторов в классе СФЭ. Сложность функции оценивается относительно числа её входных переменных, сложность оператора — относительно суммы числа входов и выходов. Задача получения нелинейной эффективной нижней оценки для оператора проще аналогичной задачи для функции с одним выходом, но даже она не решена. Предыдущими исследователями данной задачи был намечен возможный путь её решения, который мы далее опишем в виде последовательности шагов.

1. В качестве оператора, сложность которого предполагалось оценить снизу, был взят оператор умножения двоичных чисел MUL_n: $\{0,1\}^{2n} \to \{0,1\}^{2n}$. Его входы разбиты на две группы по n входов, значения входов являются двоичными записями двух натуральных чисел — x и y, значения $2n$ выходов образуют двоичную запись произведения чисел x и y. Известна верхняя оценка сложности оператора умножения: $L^{\text{СФЭ}}(\mathrm{MUL}_n) = O(n \log n \log\log n)$. Оператор умножения

задан явно, поэтому его нижняя оценка будет эффективной, более того, он представляет самостоятельный интерес ввиду практической значимости умножения чисел в электронных схемах. Точное значение сложности этого оператора, по-видимому, лежит в пределах от $n \log n$ до $n \log n \log\log n$ по порядку.

2. Вторым шагом была идея рассмотреть оператор сдвига. Есть два варианта оператора сдвига (при фиксированном направлении сдвига, например, влево) — сдвиг с добавлением нулей и циклический сдвиг. Первый является частным случаем умножения (умножение на степени двойки), поэтому нижняя оценка его сложности также будет нижней оценкой для умножения; второй вариант — RLC_n — будет удобнее для наших исследований, поэтому мы его мозьмём за основу. Оба оператора сдвига имеют по порядку равные сложности. У оператора RLC_n имеется две группы входов: первая состоит из n входов, называемых рабочими; вторая — из $\lceil \log n \rceil$ входов, называемых управляющими; кроме того имеются n выходов. Набор значений на выходах получается из набора значений рабочих входов циклическим сдвигом влево на y разрядов, где y — число, двоичную запись которого образуют управляющие входы. Сложность оператора сдвига допускает верхнюю оценку $L^{\text{СФЭ}}(\mathrm{RLC}_n) = O(n \log n)$, которая, по-видимому, является точной.

3. Третья идея состоит в следующем: подставив вместо управляющих переменных фиксированный набор констант, являющийся двоичной записью числа, меньшего n, мы получим перестановочный оператор с n входами и n выходами; набор значений его выходов дублирует набор значений входов со сдвигом на некоторое число разрядов; с точностью до перестановки выходов это — тождественный оператор. Из информационных соображений кажется очевидным, что в схеме, реализующей тождественный оператор, должны существовать попарно непересекающиеся пути, соединяющие каждый вход с соответствующим ему выходом. Если бы это было действительно так, то, рассмотрев такие пути для всевозможных сдвигов, мы бы получили нижнюю оценку $n \log n$ сложности оператора сдвига, а следовательно, и умножения (см., например, [1]). К сожалению, это не так; имеется пример схемы (рис. 1), реализующей тождественный $(2,2)$-оператор, в которой любой путь (пути всюду предполагаются ориентированными), соединяющий вход x с выходом x, пересекается с любым путём, соединяющим вход y с выходом y. Добавив после элемента E_1 тождественный элемент, можно добиться, чтобы любые такие пути рёберно пересекались.

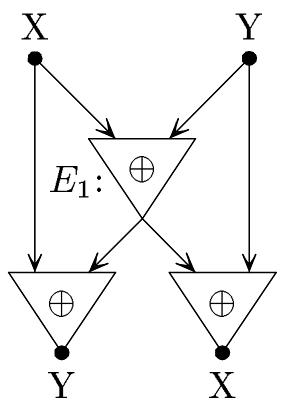

Рис. 1

4. После неудачи на третьем шаге пришла идея рассмотреть не одиночные пути, соединяющие фиксированный вход с фиксированным выходом, а множество непересекающихся путей, соединяющих данное множество входов с соответствующим множеством выходов, не требуя при этом, чтобы каждый путь соединял вход с одноимённым выходом. Из информационных соображений можно показать, что в схеме, реализующей тождественный оператор, для любого множества входов и соответствующего множества выходов найдутся непересекающиеся пути, соединяющие данное множество входов с данным множеством выходов в некотором порядке. Возникло предположение, что наличие таких множеств путей (с учётом всевозможных сдвигов) позволяет дать нелинейную оценку числу рёбер в сети, составляющей основу схемы, а значит и нелинейную оценку сложности оператора сдвига. Данная идея также оказалась ошибочной. Были построены примеры сетей с n входами и n выходами, в которых каждое подмножество входов можно соединить множеством непересекающихся путей с любым равномощным ему множеством выходов, но в то же время число рёбер в сети линейно относительно n. Впервые пример такого рода был построен Э. И. Нечипоруком, но не опубликован. Впоследствии такие объекты исследовались за рубежом под названием "суперконцентраторы".

Автору представляется, что необходимо вернуться к поиску одиночных путей, но для избежания контрпримеров, подобных изображённому на рис. 1, ограничить класс рассматриваемых схем. Разумеется, ограничение следует выбрать так, чтобы сложность интересующих нас операторов не возросла по порядку. В качестве возможного ограничения предлагается рассмотреть класс обратимых схем. Обозначим через B_3 базис, состоящий из всех обратимых $(3,3)$-операторов (биекций) и двух отдельных операторов — разделителя и соединителя. Разделитель имеет один вход и два выхода, на оба выхода подаётся значение входа; соединитель имеет два входа и один выход, на который подаётся дизъюнкция значений входов. Схема S в базисе B_3 называется *обратимой*, если выполнены следующие условия:

а) каждый вход схемы и каждый выход каждого элемента либо является выходом схемы, либо подаётся на вход ровно одного элемента (ветвления выходов не допускаются; для ветвления нужно использовать разделитель, сложность схемы при этом не изменяется по порядку);

б) для любого набора значений входных переменных схемы и любого соединителя, значения, подаваемые на два его входа, совпадают (благодаря этому разледитель и соединитель переходят друг в друга при обращении схемы).

Заметим, что в определении обратимой схемы обратимые $(3,3)$-операторы нельзя заменить обратимыми $(2,2)$-операторами, потому, что любой обратимый $(2,2)$-оператор линеен, следовательно, схема, составленная из них, может реализовать только линейный обратимый оператор. В то же время, справедлива

Лемма 1. *Любой обратимый оператор F реализуется обратимой схемой.*

Сложность оператора F в классе обратимых схем обозначим через $L^{\text{ОБ}}(F)$. Основным свойством обратимых схем является возможность обращения схемы. Обращение схемы состоит в следующем: направление каждого ребра заменяется не противоположное; входы схемы становятся выходами, выходы — входами; то же происходит с входами и выходами каждого элемента; каждый $(3,3)$-оператор заменяется на обратный; разделитель становится соединителем, соединитель — разделителем. При этом, если исходная схема реализовала обратимый оператор F, то обратная к ней схема реализует обратный оператор F^{-1}. Очевидно, сложности схемы и обратной к ней совпадают. Таким образом, справедлива

Лемма 2. *Для любого обратимого оператора F выполнено*

$$L^{\text{ОБ}}(F) = L^{\text{ОБ}}(F^{-1}).$$

В криптографии известны примеры "односторонних" операторов F, таких, что F вычислим просто (с полиномиальной сложностью), но задача вычисления оператора F^{-1} является NP-полной, т. е. гипотетически имеет неполиномиальную сложность. Лемма 2 показывает, что в классе обратимых схем такого эффекта не наблюдается, а значит сложность в классе обратимых схем гипотетически существенно отличается от сложности в классе СФЭ.

Очевидно, что всякая обратимая схема является схемой в обычном понимании над базисом B_3, поэтому $L^{\text{СФЭ}}(F) = O(L^{\text{ОБ}}(F))$. Следующая лемма устанавливает двустороннее соотношение между сложностью обратимых схем и сложностью СФЭ.

Лемма 3. *Для любого обратимого оператора F верно*

$$L^{\text{ОБ}}(F) \asymp \max\{L^{\text{СФЭ}}(F), L^{\text{СФЭ}}(F^{-1})\}.$$

Усовершенствуем оператор сдвига RLC_n так, чтобы он стал обратимым. А именно, добавим $\lceil \log n \rceil$ новых выходов и продублируем на них значения управляющих входов. Усовершенствованный оператор обозначим через RLC'_n. Очевидно, что данное усовершенствование не меняет сложности оператора в классе СФЭ, но позволяет реализовать его в классе обратимых схем. Обратный к RLC'_n оператор — циклический сдвиг вправо — отличается от RLC'_n лишь заменой выходов, поэтому сложности операторов RLC'_n и $RLC'_n{}^{(-1)}$ в классе СФЭ равны. Таким образом, имеем цепочку равенств

$$L^{\text{ОБ}}(\mathrm{RLC}'_n) \asymp \max\{L^{\text{СФЭ}}(\mathrm{RLC}'_n), L^{\text{СФЭ}}(\mathrm{RLC}'_n{}^{(-1)})\} =$$

$$= L^{\text{СФЭ}}(\mathrm{RLC}'_n) = L^{\text{СФЭ}}(\mathrm{RLC}_n). \tag{1}$$

Следовательно, оценив сложность усовершенствованного оператора сдвига в классе обратимых схем, мы оценим и сложность оператора сдвига в классе СФЭ.

Автор выдвигает следующую гипотезу.

Гипотеза. *В любой обратимой схеме, реализующей тождественный (n,n)-оператор, найдутся n реберно-непересекающихся ориентированных путей, i-й из которых соединяет i-й вход схемы с i-м выходом, $i = 1, \ldots, n$.*

В случае справедливости гипотезы можно, используя результат работы [1] и равенство (1), получить нижнюю оценку вида $O(n \log n)$ для сложности оператора сдвига и оператора умножения классе СФЭ. Гипотеза доказана при $n = 2$.

Автор благодарит чл.-корр. РАН О. Б. Лупанова, сообщившего ему о неопубликованных результатах предшественников, упомянутых в данной статье.

Работа выполнена при финансовой поддержжке РФФИ (проект 99–01–01175), ФЦП "Интеграция" (проект АО–110), Программы "Университеты России" (проект 992206) и Программы поддержки ведущих научных школ РФФИ (проект 00–15–96103).

Литература

[1] Черухин Д. Ю. Нижние оценки сложности коммутационных сетей // Материалы VII Международного семинара "Дискретная математика и её приложения". Ч. I. — М.: Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001. — С. 89–90.