ЯЗЫКИ СПЕЦИФИКАЦИЙ И ЛОГИЧЕСКОЕ ПРОГРАММИРОВАНИЕ
(Вычислительные системы)
1988 год Выпуск 124

УДК 519.712

ПОЛИНОМИАЛЬНАЯ СЛОЖНОСТЬ СХЕМ И АЛЬТЕРНИРОВАНИЕ С ПОЛИНОМИАЛЬНЫМ ВРЕМЕНЕМ

Н.К. Косовский

Настоящая статья продолжает один результат автора из [2] в направлении получения полиномиальных нижних оценок схемной сложности. Доказательства основаны на моделировании (с учетом верхней границы используемых ресурсов) одних типов вычислений другими.

Для любого положительного целого числа К предлагается предикат, вычислимый на машине Тьюринга на полиномиальном числе ячеек и не допускающий схемную реализацию с числом элементов, которое при некотором С не превосходит $(M-C)^K$, где М – число входов схемы. Этот предикат является Р–СПЭЙС–полным.

Предлагаемые предикаты представляют собой проверку истинности формул, начинающихся с любого стандартного префикса, состоящего из ограниченных кванторов и предшествующего утверждению о разрешимости синтаксически ограниченных логико–арифметических уравнений. Для предлагаемых предикатов полиномиальные верхние оценки числа элементов рассматриваемых схем следуют из предложения о равенстве класса предикатов Р и класса предикатов Р–СПЭЙС (вычислимых на ленте полиномиального объема от длины исходных данных). Доказательство или опровержение этого равенства является одной из труднейших проблем современной абстрактной теории сложности вычислений.

Важность задачи построения индивидуальных последовательностей булевых функций, которые нельзя просто реализовать в классе схем из функциональных элементов (с полиномиальной комбинационной сложностью при степени полинома больше 3) отмечали О.Б.Лупанов [4] и С.В.Яблонский [5]. История попыток решения этой задачи подробно изложена Р.Г.Нигматуллиным [3]. Ниже для каждого положитель-

ного целого числа К предлагается предикат, формулируемый в обще - математических терминах, вычислимый на машине Тьюринга с полино - миальным числом ячеек и не имеющий полиномиальной комбинационной схемной сложности реализации для полинома вида $(M-C)^K$ при некотором С, где М - число битовых входов схемы.

Каждый предлагаемый предикат может рассматриваться как последовательность булевых функций, каждая из которых не допускает схемной реализации с полиномиальным числом элементов в схеме (степень полинома зависит от предиката).

Одним из существенных этапов доказательства основного результата является моделирование логико-арифметическими уравнениями вычислений посредством недетерминированной машины Тьюринга, вычисляющей значения булевых функций, существование которых сформулировано ниже в лемме I.

Заметим, что получение нижних оценок комбинационной сложности в классе схем из функциональных элементов связано, как правило, с бо́льшими затруднениями, чем получение оценок такого же типа для машин Тьюринга; для них, например, сложность оценивается, как правило, с точностью до мультипликативной константы.

Каждый одноместный предикат будет задавать последовательность булевых функций, число аргументов у которых равно битовой длине аргумента.

Предлагается следующий способ представления предиката такой последовательностью (на основе М-битового ограничения одномест - ного предиката).

Буквы алфавита, в котором определяется предикат, дополняются пробелом и кодируются последовательностями нулей и единиц одной и той же длины. Для увеличения длин всех аргументов до одной (единственной для каждой булевой функции) величины к аргументу преди - ката слева приписываются пробелы. Состоящая из одних нулей кодировка самого левого пробела может иметь длину больше нуля, но меньше длины кодировки любой другой буквы (например, длину, равную единице). Все остальные пробелы должны иметь стандартную длину, как и кодировка любой другой буквы.

При таком представлении предиката последовательностью булевых функций с монотонно растущим числом аргументов каждая булева функция является подфункцией любой следующей в последовательности булевой функции (при фиксации начальных аргументов). В последовательности булевых функций, задающей предикат, присутствуют функ-

ции с числом аргументов, равным каждому натуральному числу (по существу, дополнительные начальные входы (аргументы) булевой функции служат для выделения предшествующих в последовательности подфункций, представляющей предикат).

Будем говорить, что M-местная булева функция является M-битовым ограничением одноместного предиката, если ее значения совпадают со значением предиката на аргументе, представляющем собой слово, получающееся последовательным приписыванием друг к другу кодов букв. Каждый код представляет собой слово в алфавите, состоящем из нулей и единиц, и начинается с единицы. Поэтому слово длины, не превосходящей T и записанное в 2^K буквенном алфавите, преобразуется в последовательность из $T\cdot(K+1)$ логических констант.

Все константы в приводимой ниже формулировке леммы I допускают существенное уточнение, но поскольку в дальнейшем используются константы только такого типа, то автор не ставил своей целью построение наилучших констант. Сказанное относится и к некоторым константам в формулировке теоремы.

Формулировка и доказательство теоремы. Ей предпошлем ряд лемм. Доказательство леммы I использует широко известный в математической кибернетике фундаментальный результат О.Б.Лупанова (о сложности схем из функциональных элементов, см., например, [3]) и трансляцию быстрорастущих оценок в медленнорастущие на основе добавления фиктивных аргументов булевой функции. Эту идею доказательства сообщил автору А.П.Бельтюков, доказавший с ее помощью более сильный результат.

ЛЕММА I. Каково бы ни было положительное число K, существует последовательность булевых функций такая, что, начиная с некоторого M, эти функции не реализуются схемами из не более чем M^K штрихов Шеффера, где M-местность булевой функции. При этом функции реализуются схемами из $3\cdot M^K$ штрихов Шеффера.

ДОКАЗАТЕЛЬСТВО. Прежде всего, начиная с некоторого M, установим существование булевой функции от M переменных, которая вычислима функциональной схемой с числом элементов, не превосходящим $2\cdot 2^M/M$, и невычислима с числом элементов, меньшим $2^M/M$. Действительно, во-первых, по теореме 3 из главы 4 монографии Р.Г.Нигма -

туллина [3, с.69] возможно построение по любой булевой функции функциональной схемы с числом элементов, не превосходящим $2 \cdot 2^M/M$. Во-вторых, при M, большем, чем 128, число элементов функциональной схемы будет больше, чем $2^M/M$. Это можно установить, изменив доказательство леммы 9, основывающейся на лемме 8 и служащей непосредственно для доказательства эффекта Шеннона в монографии Р.Г.Нигматуллина [3, с. 85].

Посредством T_K обозначим функцию, вычисляющую по M наибольшее Y такое, что Y^K не превосходит $2^M/M$. Для достаточно больших M построим булеву функцию от $T_K(M)$ переменных, которая зависит только от первых M переменных, на них значение этой булевой функции совпадает со значением той булевой функции, существование которой установлено в начале доказательства этой леммы.

Построенную сейчас булеву функцию можно, во-первых, реализовать схемой из $3(T_K(M))^K$ элементов. Действительно, по теореме 3 главы 4 из [3,с.69], начиная с некоторого M, достаточно $2 \cdot 2^M/M$ элементов, чтобы полученное значение не превосходило значения выражения $3(T_K(M))^K$, обеспечивающего требуемую оценку. Здесь используется то, что значение выражения $2X^K$ не превосходит $3(X-1)^K$, начиная с некоторого X.

Во-вторых, построенную булеву функцию нельзя реализовать функциональной схемой из $(T_K(M))^K$ элементов. Действительно, $(T_K(M))^K$ не превосходит $2^M/M$ (непосредственно следует из определения функции T_K). Лемма доказана.

Поразрядным умножением будем называть функцию, которая по двоичной записи чисел вычисляет число, в двоичной записи которого единица содержится только в том разряде, в котором одновременно в двоичной записи аргументов стоит единица. Если два числа, являющиеся аргументами, имеют разную длину, то для выравнивания их длин старшие разряды более короткого числа заполняются нулями. Тем самым поразрядное умножение определено над двоичными записями чисел аналогично логическому умножению, используемому во многих ЭВМ.

Логико-арифметическим уравнением будем называть уравнение вида $P+P'=0$, где P – полином с целыми коэффициентами, P' – сумма порязрядных умножений.

Для каждого положительного целого числа K через P_K обозначим предикат установления истинности замкнутых формул, начинающихся с ограниченных кванторов (используются ограничения сверху на длину записи в двоичной системе счисления, имеющей вид полиномов,

не содержащих переменных и являющихся одночленами степени не более чем 4К+К). Непосредственно за последовательностью ограниченных кванторов находится логико-арифметическое уравнение.

ЛЕММА 2. Можно построить детерминированную машину Тьюринга, которая по набору М логических констант вычисляет значение предиката P_K этого набора. При этом число используемых ячеек ленты машины Тьюринга не превосходит величины $\sim E \cdot M^{4K+5}$ при некотором Е.

ДОКАЗАТЕЛЬСТВО. В логико-арифметическом уравнении, используемом в определении предиката P_K, ограничение на длину решений не превосходит какой-либо константы, не превосходящей М и умноженной на M^{4K+4}, поскольку М не превосходит битовая длина любого записанного в двоичной системе числа, входящего в формулу для предиката P_K. Поэтому вычисление последнего можно осуществить на машине Тьюринга на ленте, число ячеек которой ограничено сверху константой, умноженной на M^{4K+5}. Лемма доказана.

ЛЕММА 3. Любой одноместный предикат с аргументом X, задаваемый недетерминированной машиной Тьюринга, которая выполняет число шагов, не превосходящее одночлена степени 4К+4 от длины X, выразим в виде

$$Y(\leq \Phi)(P(Y,X) + P'(Y) = 0), \qquad (*)$$

где Y - список переменных; Φ - одночлен степени 8К+8 от длины X, являющейся ограничением сверху на длину значения каждой переменной списка Y; P - полином с целыми коэффициентами; P' - сумма двух поразрядных умножений переменных. При устранении ограничения для квантора существования получается эквивалентное представление того же предиката. При этом длина формулы (*) может быть ограничена сверху

посредством 2M+H при некотором H, где M - битовая длина записи X.

ДОКАЗАТЕЛЬСТВО. Эта лемма, по существу, доказана автором в [2] как теорема о моделировании логико-арифметическими уравнениями недетерминированных вычислений за ограниченное число шагов. Поэтому достаточно проследить приведенное в [2] доказательство этой теоремы и убедиться в линейной зависимости от M оценки на длину записи логико-арифметического уравнения.

После этого можно добиться коэффициента 2 в линейном выражении, слегка преобразовав исходное уравнение так, чтобы непосредственно в уравнение переменная X входила единственный раз (второе вхождение - в ограничение на величину решений) за счет введения дополнительной переменной Y" (ограниченной, например, самой переменной) и приравняв нулю сумму квадрата левой части уравнения и выражения $(X-Y")^2$. (В этой записи уравнения используются скобки!)

ТЕОРЕМА. Каково бы ни было целое число K, большее единицы, существует целое число C такое, что каково бы ни было положительное целое число M, предикат P_K является P-СПЭЙС-полным и вычислимым на машине Тьюринга на ленте с не более чем полиномиальным числом ячеек (полином степени 4K+5). M-битовое ограничение предиката P_K для любого положительного целого числа M не допускает схемную реализацию с числом штрихов Шеффера, не превосходящим $(M-C)^K$, где M - число входов схемы.

ДОКАЗАТЕЛЬСТВО. Вычисление значений булевых функций из леммы I обладает требуемой нижней оценкой для числа функциональных элементов в реализующих эти функции схемах. Поэтому промоделируем вычисления значений этих булевых функций формулами из определения предиката P_K.

В этом моделировании для обеспечения достаточности ограничений на кванторы, используемые в определении предикатов P_K, битовая длина записи любой схемы, задаваемой последовательностью присваиваний пропозициональным переменным пропозициональных формул, в которых используется только штрих Шеффера, при некоторых T не превосходит выражения $T \cdot K \cdot M^{K+1}$ при достаточно больших M, если в

префиксной записи число штрихов Шеффера не превосходит $3 \cdot M^K$. Действительно, каждую схему, содержащую пропозициональную формулу с двумя или более присваиваниями, можно превратить в более длинную схему со штрихами Шеффера на два присваивания больше. Поэтому достаточно оценить сверху длину таких схем, в которых не используются пропозициональные формулы, содержащие два штриха Шеффера. В таких схемах число вхождений пропозициональных переменных равно утроенному числу присваиваний, в свою очередь, равному числу штрихов Шеффера.

Достаточной приближенной оценкой сверху в этом случае будет при некотором T' выражение $9 \cdot T' \cdot K \cdot M^{K+1}$, если суммарная длина записи всех переменных не будет превосходить $T' \cdot K \cdot M^{K+1}$ и трех битов будет достаточно для кодировки всех используемых знаков.

Значение булевой функции на наборе логических констант (число логических констант в наборе, равное M, задает число аргументов булевой функции, существование которой установлено в лемме I) равно истине в том и только в том случае, когда существует состоящая из не более чем $3 \cdot M^K$ штрихов Шеффера схема, являющаяся наименьшей в лексикографическом порядке по записи из всех таких формул и обладающая следующим свойством. Какова бы ни была состоящая из более чем M^K штрихов Шеффера схема B, существует набор логических констант Y, на котором различаются A(Y) и B(Y). При этом дополнительно проверяется, что A и B являются записями схем.

Осталось провести недетерминированные вычисления по проверке различия значений A(У) и B(У), а также проверить, являются ли A и Б записями схем. Все это выполняется на недетерминированной машине Тьюринга за число шагов, ограниченное сверху некоторой константой, умноженной на M^{2K+2}. Согласно лемме I найдется требуемая булева функция в виде схемы A. Наименьшая в лексикографическом порядке такая схема будет единственной. Свойство "быть наименьшей в лексикографическом порядке" также может быть промоделировано с требуемыми ограничениями на кванторы.

Наконец, вычисления, производимые недетерминированной машиной Тьюринга за ограниченное число шагов можно заменить решением логико-арифметических уравнений на основе леммы 3. При этом ограничения на кванторы будут не превосходить некоторой константы, умноженной на M^{4K+4}.

Тем самым для каждого положительного целого числа M вычисление булевой функции от M аргументов (имеющей наименьшую из сущест-

вующих по лемме I в лексикографическом порядке запись реализую - щей ее схемы) моделируется формулой с ограниченными кванторами. Проверка истинности этой формулы обеспечивается вычислением пре - диката П. При этом длина моделирующей формулы не превосходит ли- нейной функции от M, поскольку в записи формулы число перемен кванторов ограничено сверху и для некоторых идущих подряд кванто- ров одного типа можно использовать одно и то же ограничение свер- ху, выписав его только один раз.

Для окончательного доказательства необходимо теорему дока - зать прежде всего для всех достаточно больших M. Действительно, увеличив C, можно добиться, чтобы новое значение C годилось для всех M. Дальнейшее доказательство проводится методом от против - ного. Согласно предположению, что каково бы ни было рациональное число C,большее единицы, для бесконечно многих M имеется требуе- мая (при отрицании утверждения теоремы) схема B" из числа функ - циональных элементов менее, чем $(M/C)^K$. Следовательно, для та- ких M, согласно лемме I и результатам о моделировании недетер - минированных вычислений логико-арифметическими уравнениями, имеет место неравенство $M^K < (HM + H'/C)^K$ при некоторых H, H', что не- возможно, начиная с некоторого M при достаточно большом C.Дейст- вительно, на основе леммы 3, битовая длина логико-арифметического уравнения (используемого при моделировании вычисления сложной бу- левой функции, существование которой установлено по лемме I) вме- сте с записью ограниченных кванторов, предшествующих этому урав - нению, может быть ограничена сверху посредством $2M + H$, вход пе- ременных $X_1, \ldots, X_M$ можно подключить к входам схемы B",предназ- наченным для ввода записи (в двоичном виде) логико-арифметическо- го уравнения. К остальным входам схемы подключаются необходимые константные входы.

Наконец, вычисление предиката P_K можно реализовать на маши- не Тьюринга согласно лемме 2 на ленте с числом ячеек, ограничен - ным сверху требуемой величиной. Предикат P_K включает в себя как частный случай Р-СПЭЙС-полную задачу проверки истинности замкну - тых пропозициональных формул с кванторными префиксами. В этих фор- мулах кванторы используются для пропозициональных переменных.Дей- ствительно, кванторы в P_K могут быть ограничены единицей. Поли - ном будет моделировать пропозициональную формулу. Теорема доказа- на.

СЛЕДСТВИЕ. Если класс P (предикатов, вычислимых за полиномиальное число шагов на детерминированных машинах Тьюринга) совпадает с классом P-СПЭЙС (предикатов, вычислимых на детерминированных машинах Тьюринга, использующих не более полиномиального числа ячеек), то при каждом K предикат P_K из формулировки теоремы имеет верхнюю полиномиальную оценку числа шагов своего вычисления на детерминированных машинах Тьюринга и, следовательно, может быть реализован схемой с полиномиальным числом функциональных элементов.

Отметим, что в работе Б.Скарпеллини [6], посвященной построению сложных булевых функций, реализуемых с помощью сетей, доказывается лишь ограниченность сверху числа ячеек машины Тьюринга, вычисляющей сложные булевы функции. При этом в ней не рассматриваются сколь-нибудь конкретные сложные булевы функции и не оценивается степень полинома, являющегося верхней границей числа ячеек такой машины Тьюринга.

Если интересоваться только полиномиальными нижними оценками, а не P-СПЭЙС-полнотой предиката P_K, то в его определении достаточно ограничиться тремя переменами кванторов. При этом можно дополнительно потребовать, чтобы у всех формул, задающих предикат P_K, был одинаковый начальный квантор.

Основной результат настоящей статьи впервые анонсирован в [I].

Математические исследования, лежащие в основе настоящей статьи, в значительной степени стимулированы вопросами скоропостижно скончавшегося Р.Г.Нигматуллина, общение с которым оставило глубокие светлые воспоминания. Автор глубоко благодарен В.Ю.Сазонову и редактору, существенные критические замечания которых позволили придать большую ясность и точность полученным результатам и их доказательству.

Литература

I. КОСОВСКИЙ Н.К. Полиномиальная сложность любых схем, реализующих некоторые предикаты, вычислимые на полиномиальной ленте //УП Всесоюз. конф. "Проблемы теоретической кибернетики". Тез.докладов. Часть I. - Иркутск. - 1985. - С. 100-101.

2. КОСОВСКИЙ Н.К. Основы теории элементарных алгоритмов.-Л., 1987. - 153 с.

3. НИГМАТУЛЛИН Р.Г. Сложность булевых функций. -Казань,1983. - 208 с.

4. ЛУПАНОВ О.Б. О синтезе некоторых классов управляющих систем //Проблемы кибернетики. - М., 1963. - Вып. 10. - С. 88-96.

5. ЯБЛОНСКИЙ С.В. Обзор некоторых результатов в области дискретной математики //Всесоюз.конф. по проблемам теорет. киберн.: Информ. материалы, 5(42)/Научный совет по комплексной проблеме "Кибернетика". М., 1970. - С. 5-15.

6. SCARPELLINI B. Complex boolean networks obtained by dia - gonalization// Theoretical Computer Science.-1985.- Vol.36.-P.119-125.

Поступила в ред.-изд.отд.
24 июля 1987 года