ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том IX *1973* *Вып. 3*

КРАТКИЕ СООБЩЕНИЯ

УДК 519.14

УНИВЕРСАЛЬНЫЕ ЗАДАЧИ ПЕРЕБОРА

Л. А. Левин

В статье рассматривается несколько известных массовых задач «переборного типа» и доказывается, что эти задачи можно решать лишь за такое время, за которое можно решать вообще любые задачи указанного типа.

После уточнения понятия алгоритма была доказана алгоритмическая неразрешимость ряда классических массовых проблем (например, проблем тождества элементов групп, гомеоморфности многообразий, разрешимости диофантовых уравнений и других). Тем самым был снят вопрос о нахождении практического способа их решения. Однако существование алгоритмов для решения других задач не снимает для них аналогичного вопроса из-за фантастически большого объема работы, предписываемого этими алгоритмами. Такова ситуация с так называемыми переборными задачами: минимизации булевых функций, поиска доказательств ограниченной длины, выяснения изоморфности графов и другими. Все эти задачи решаются тривиальными алгоритмами, состоящими в переборе всех возможностей. Однако эти алгоритмы требуют экспоненциального времени работы и у математиков сложилось убеждение, что более простые алгоритмы для них невозможны. Был получен ряд серьезных аргументов в пользу его справедливости (см.[1, 2]), однако доказать это утверждение не удалось никому. (Например, до сих пор не доказано, что для нахождения математических доказательств нужно больше времени, чем для их проверки.)

Однако если предположить, что вообще существует какая-нибудь (хотя бы искусственно построенная) массовая задача переборного типа, неразрешимая простыми (в смысле объема вычислений) алгоритмами, то можно показать, что этим же свойством обладают и многие «классические» переборные задачи (в том числе задача минимизации, задача поиска доказательств и др.). В этом и состоят основные результаты статьи.

Функции $f(n)$ и $g(n)$ будем называть сравнимыми, если при некотором k

$$f(n) \leqslant (g(n)+2)^k \quad \text{и} \quad g(n) \leqslant (f(n)+2)^k.$$

Аналогично будем понимать термин «меньше или сравнимо».

Определение. Задачей переборного типа (или просто переборной задачей) будем называть задачу вида «по данному x найти какое-нибудь y длины, сравнимой с длиной x, такое, что выполняется $A(x, y)$», где $A(x, y)$ – какое-нибудь свойство, проверяемое алгоритмом, время работы которого сравнимо с длиной x. (Под алгоритмом здесь можно понимать, например, алгоритмы Колмогорова — Успенского или машины Тьюринга, или нормальные алгоритмы; x, y – двоичные слова). Квазипереборной задачей будем называть задачу выяснения, существует ли такое y.

Мы рассмотрим шесть задач этих типов. Рассматриваемые в них объекты кодируются естественным образом в виде двоичных слов. При этом выбор естественной кодировки не существен, так как все они дают сравнимые длины кодов.

Задача 1. Заданы списком конечное множество и покрытие его 500-элементными подмножествами. Найти подпокрытие заданной мощности (соответственно выяснить существует ли оно).

Задача 2. Таблично задана частичная булева функция. Найти заданного размера дизъюнктивную нормальную форму, реализующую эту функцию в области определения (соответственно выяснить существует ли она).

Задача 3. Выяснить, выводима или опровержима данная формула исчисления высказываний. (Или, что то же самое, равна ли константе данная булева формула.)

Задача 4. Даны два графа. Найти гомоморфизм одного на другой (выяснить его существование).

Задача 5. Даны два графа. Найти изоморфизм одного в другой (на его часть).

Задача 6. Рассматриваются матрицы из целых чисел от 1 до 100 и некоторое условие о том, какие числа в них могут соседствовать по вертикали и какие по горизонтали. Заданы числа на границе и требуется продолжить их на всю матрицу с соблюдением условия.

Пусть $f(n)$ — монотонная функция.

Теорема 1. *Если вообще существует какая-нибудь массовая задача переборного (квазипереборного) типа, неразрешимая за время, меньшее $f(n)$ при длине аргумента, сравнимой с n, то этим же свойством обладают задачи 1—6.*

Идея доказательства состоит в том, что задачи 1—6 являются «универсальными задачами перебора».

Определение. Пусть $A(x, y)$ и $B(x, y)$ определяют соответственно переборные задачи A и B. Мы говорим, что задача A сводится к B, если есть три алгоритма $r(x)$, $p(y)$ и $s(y)$, работающие за время, сравнимое с длиной аргумента, такие, что $A(x, p(y)) \equiv B(r(x), y)$ и $A(x, y) \equiv B(r(x), s(y))$ (т. е. по A – задаче x легко построить эквивалентную B задачу $r(x)$). Задача, к которой сводится любая задача перебора, называется «универсальной».

Таким образом, суть доказательства теоремы 1 состоит в следующей лемме.

Лемма 1. *Задачи 1—6 являются универсальными переборными задачами.*

Описанный метод, по-видимому, позволяет легко получить результаты типа теоремы 1 и леммы 1 для большинства интересных переборных задач. Однако остается проблема доказать условие, имеющееся в этой теореме. В этом направлении давно уже делаются многочисленные попытки и получен ряд интересных результатов (см., например, [3, 4]). Впрочем, универсальность различных массовых задач перебора можно устанавливать и без решения этой проблемы. В системе алгоритмов Колмогорова – Успенского может быть доказана также следующая

Теорема 2. *Для произвольной массовой переборной задачи $A(x, y)$ существует алгоритм, решающий ее за время, оптимальное с точностью до умножения на константу и прибавления величины, сравнимой с длиной x.*

Автор выражает искреннюю благодарность А. Н. Колмогорову, Б. А. Трахтенброту, Я. М. Барздиню, Ю. И. Альбртону и М. И. Дегтярю за ценное обсуждение.

ЛИТЕРАТУРА

1. Яблонский С. В. Об алгоритмических трудностях синтеза минимальных контактных схем. Сб. «Проблемы кибернетики», **2**. М., Физматгиз, 1959, 75—121.
2. Журавлев Ю. И. Теоретико-множественные методы в алгебре логики. Сб. «Проблемы кибернетики», 8. М., Физматгиз, 1962, 5—44.
3. Трахтенброт Б. А. Оптимальные вычисления и частотное явление Яблонского. Семинар. Новосибирск, «Наука», СО, 1965, **4**, *5*, 79—93.
4. Дегтярь М. И. О невозможности элиминации полного перебора при вычислении функций относительно их графиков. Докл. АН СССР, 1969, **189**, *4*, 748—751.

Поступила в редакцию
7 июня 1972 г.