историю. Еще в 1942 году Дж.Риордан и К.Шеннон показали, что почти все булевы функции требуют для своей реализации схем экспоненциальной сложности. Однако для конкретных последовательностей булевых функций удается установить лишь очень невысокие нижние оценки сложности – и это несмотря на значительные усилия целого ряда исследователей.

Основной вопрос, на который пытался ответить Рошаль Габдулхаевич – Почему не удается получать высокие нижние оценки для конкретных последовательностей булевых функций? Вначале он исследовал различные аксиоматические системы, пытаясь доказать невыводимость в них высоких нижних оценок. Однако на этом пути возникли принципиальные трудности, которые преодолеть не удалось (подробнее см. § I.2). Этот подход был оставлен, автор пошел по другому пути. Исследовав практически все известные доказательства нижних оценок сложности, он предложил две модели доказательств нижних оценок сложности, в которые вкладывается подавляющее большинство известных доказательств. В рамках этих моделей он предложил понятие "эффективных" нижних оценок, дал единую трактовку известных доказательств, установил связь величины нижних оценок со сложностью универсальных функций или схем и, в частности, показал невыводимость высоких нижних оценок для схем в полных базисах.

Автор написал рукопись в 1986 г. К сожалению, он не успел сам подготовить ее к печати. При редактировании мы стремились сохранить исходный авторский текст, внося лишь минимальные поправки.

Издание книги не могло бы состояться без помощи и поддержки О.Б.Лупанова, С.В.Яблонского, В.М.Храпченко, коллектива кафедры теоретической кибернетики КГУ и ее заведующего Р.Г.Бухараева, а также семьи Рошаля Габдулхаевича.

С.Кузнецов
Н.Нурмеев

ВВЕДЕНИЕ

Проблема нижних оценок сложности – одна из наиболее острых и трудных открытых проблем в математике. Она представляет глубокий интерес как для теории, так и для практики.

В теоретическом плане ее решение означало бы разработку принципиально новых методов, качественно превосходящих по своим возможностям известные ныне методы доказательства нижних оценок сложности. В случае отрицательного решения проблемы это означало бы познание пределов возможностей математики.

В прикладном плане решение проблемы нижних оценок сложности способствовало бы разработке более эффективных алгоритмов и созданию методики по оценке качества алгоритмов и программ.

Проблема нижних оценок сложности состоит в том, чтобы доказать высокие (например, неполиномиальные) нижние оценки сложности вычисления индивидуальных функций или распознавания индивидуальных языков. В этой фразе ряд выражений нуждается в уточнении. Эти уточнения и позволяют вскрыть существо проблемы.

Почему в формулировке проблемы нижних оценок сложности говорится об индивидуальной задаче или индивидуальном языке и что это такое? Дело в том, что без требования индивидуальности проблема решается, причем без больших трудностей. Это достигается, например, применением мощностного метода Шеннона [8I] или диагонализации. Названные методы позволяют доказать существование сложных функций и языков. Однако они не применимы ни к каким конкретным (индивидуальным) функциям и языкам. По этой причине решения, даваемые мощностным методом Шеннона и диагонализацией, не интересны и хотелось бы исключить их из рассмотрения. С этой целью при формулировке проблемы нижних оценок сложности говорят только об индивидуальных задачах и языках.

Мы пояснили, что такое индивидуальная функция и индивидуальный язык, но это не более, чем пояснение. Оно не может претендовать на роль определения, и последующий ход событий подтвердил это. В

ряде работ [57, 67, 73, 87, 5I] были построены "явные" функции и языки, имеющие большую сложность. Ввиду явного задания эти функции и языки могут претендовать на право считаться индивидуальными, но наша интуиция противится признанию такого права. Дело в том, что во всех названных работах задание функций и языков только формально можно считать явным. Фактически же эти функции и языки остаются так же "неосязаемыми", как и сложные функции, построенные мощностным методом Шеннона. Не случайно, что доказательство высоких нижних оценок сложности в работах [5I, 57, 67, 73, 87] опирается на мощностной метод Шеннона или диагональный метод.

Итак, все названные выше доказательства при формальном подходе решают проблему нижних оценок сложности, но эти решения были признаны неудовлетворительными. Эти доказательства называют неэффективными. При решении проблемы нижних оценок сложности их обычно исключают из рассмотрения. Для этого требуется уточнение понятия "эффективное доказательство нижней оценки сложности", без которого невозможна аккуратная формулировка проблемы нижних оценок.

В вышеуказанной формулировке проблемы нижних оценок сложности еще одно выражение требует уточнения. Это - "сложность вычисления". Дело в том, что сложность вычисления зависит от модели вычислений. Среди этих моделей есть так называемые "сильные" и "слабые". Для слабых моделей (например, дизъюнктивных нормальных форм) проблема нижних оценок сложности трудностей не вызывает. Наиболее трудна она для сильных. В качестве примеров таких моделей можно назвать машины Тьюринга, нормальные алгорифмы, машины с произвольным доступом к памяти (РАМ-машины), схемы из функциональных элементов и т.п. Поскольку для сильных моделей трудности решения проблемы нижних оценок сложности примерно одни и те же, то можно ограничиться рассмотрением одной такой модели. В данной работе мы берем в качестве представителя сильных моделей схемы из функциональных элементов (СФЭ), а в качестве объекта вычисления - булевы функции.

Такой выбор нисколько не ограничивает общности, поскольку все основные трудности доказательства высоких нижних оценок для этой модели не только сохраняются, но и предстают наиболее выпукло. В уточненных терминах проблему нижних оценок сложности можно сформулировать следующим образом: <u>доказать высокие эффективные нижние оценки сложности вычисления булевых функций схемами из функциональных элементов</u>. Напоминаем, что понятие эффективности доказательства пока понимается в интуитивном смысле, исключающем из рассмотрения доказательства из [5I, 57, 67, 73, 87] и им подобные.

В чем же заключается трудность проблемы нижних оценок сложности? Почему уже на протяжении нескольких десятилетий нет сколько - нибудь заметного прогресса в решении этой проблемы? Так, все эффективные в интуитивном смысле доказательства (см., например, [5,I2, 39, 40, 43, 55, 6I, 62, 76, 83, 84, 88]) дают всего лишь линейные (от числа переменных функций) нижние оценки сложности, что только в константу раз выше тривиальной оценки и экспоненциально ниже неэффективных нижних оценок. Почему столь низки эффективные нижние оценки сложности? Что мешает их повышать? Эти вопросы возникают, если задуматься о возможности отрицательного решения проблемы нижних оценок сложности.

Помимо заведомо сильных и заведомо слабых моделей вычислений есть модели, занимающие по силе промежуточное положение. В качестве примеров можно назвать булевы формулы и синхронные СФЭ. Про эти модели не доказано, что они полиномиально эквивалентны схемам из функциональных элементов. Поэтому мы не можем причислить их к сильным. Казалось бы, на этих моделях проблема нижних оценок сложности должна решаться легче. Хотя для них действительно получены несколько более высокие нижние оценки сложности [23,48,49,64 и др.], но на качественном уровне проблема нижних оценок сложности остается для них в той же мере нерешенной, сколь и для схем из функциональных элементов.

В то же время для ряда других моделей вычислений, занимающих по силе промежуточное положение, проблема нижних оценок сложности решается положительно. Эти модели получаются из схем функциональных элементов путем наложения некоторого ограничения, почему и называются моделями с ограничениями. Примерами ограничений являются запрет нулевых цепей (см. п.2.9), ограничение на глубину (п.2.I0) и т.д. Булевы формулы и синхронные схемы тоже можно рассматривать как схемы с ограничениями. Почему же для одних моделей с ограничениями проблема нижних оценок сложности решается, а для других нет? Для решения проблемы нижних оценок сложности требуется и на этот вопрос дать вразумительный ответ.

Итак, мы выявили ряд вопросов, которые в совокупности характеризуют проблему нижних оценок сложности. Резюмируем сказанное.

<u>Вопрос первый</u>. Как провести разграничение эффективных и неэффективных доказательств нижних оценок сложности?

<u>Вопрос второй</u>. Почему для одних моделей с ограничениями высо-

кие нижние оценки сложности получаются легче, для других (например, схем в монотонном базисе) труднее, а для третьих вообще не получаются?

Вопрос третий. Можно ли прогнозировать возможности доказательства высоких нижних оценок сложности для новых, еще не исследованных моделей вычислений?

В данной работе делается попытка ответить на эти вопросы.

Длительные неудачи при попытках решения проблемы нижних оценок сложности дают основания предполагать наличие принципиальных трудностей, мешающих решению проблемы, и тем самым ставить вопрос об отрицательном ее решении. Именно под таким углом зрения эта проблема рассматривается в данной работе. Работа имеет метаматематический характер. В ней анализируется большое число доказательств нижних оценок сложности и на основе этого анализа предлагаются математические модели этих доказательств. Они названы в работе универсальными доказательствами.

Модели нацелены на то, чтобы увидеть пределы возможностей эффективных доказательств нижних оценок сложности. Они позволяют делать заключение о невозможности решения проблемы нижних оценок сложности, если ограничиться универсальными доказательствами. Этот вывод не следует абсолютизировать, поскольку он получен всего лишь для модели. В то же время полученные результаты можно трактовать как указание на серьезные трудности при решении проблемы нижних оценок сложности. Результаты могут оказаться полезными также при попытках положительного решения проблемы.

Предложенные модели доказательств нижних оценок сложности позволяют ответить на сформулированные выше три вопроса. Выясняется, что решающее значение для разрешимости проблемы нижних оценок сложности (разумеется, в рамках модели) имеет сложность универсальных схем. При этом эффективным доказательствам сопоставляются схемы, которые являются универсальными для множества схем "малой" сложности. Далее, высокие нижние оценки сложности для схем в монотонном базисе доказываются труднее, поскольку универсальные монотонные схемы имеют малую сложность. С другой стороны, они все же доказываются, так как монотонные схемы являются частным случаем схем без нулевых цепей, а для последних универсальные схемы имеют экспоненциальную сложность. Наконец, для прогнозирования возможностей доказательства высоких нижних оценок сложности для новых моделей вычислений следует изучить сложность универсальных схем для этих моделей. Значение этой сложности (а оно в случае универсальных схем оценивается без труда) и дает представление о том, какой величины нижние оценки сложности можно получить для данной модели вычислений.

Предложенная модель доказательств нижних оценок сложности позволяет объяснить еще одно загадочное явление из теории сложности. Оно сформулировано в следующем вопросе: почему для тех моделей вычислений, где высокие нижние оценки не получаются, они (эти оценки) оказываются совсем уж низкими (а именно, линейными для СФЭ и не выше $n^{5/2}$ для булевых формул)? Объяснение кроется в том, что для СФЭ и булевых формул все известные доказательства нижних оценок сложности не выходят за пределы нашей модели, а величины нижних оценок сложности в этой модели определяются сложностью универсальных схем. Поскольку универсальные схемы допускают очень экономную реализацию, то и величины нижних оценок сложности оказываются весьма скромными.

Автор еще раз хотел бы подчеркнуть, что изложенные ответы на поставленные выше три вопроса следует рассматривать как относительные: они имеют силу только для тех доказательств нижних оценок сложности, которые описываются универсальными доказательствами, и потому не исключают возможности положительного решения проблемы нижних оценок сложности.

Опишем структуру книги. Она состоит из введения, четырех глав, списка литературы и приложения.

В главе I дается краткий очерк развития проблемы нижних оценок сложности и обсуждаются различные подходы к уточнению понятия "эффективное доказательство нижних оценок сложности". Вводятся основные понятия, используемые на протяжении всей работы. Основное назначение главы - это обоснование и формулировка тех вопросов, которым посвящена работа. Из них три основных вопроса были отмечены выше.

Глава 2 посвящена анализу доказательств нижних оценок сложности. Автор стремился представить эти доказательства возможно более широко как в смысле разнообразия моделей вычислений, так и в смысле методов доказательства. В частности, анализируются доказательства из работ [I2, I5, 23, 29, 37, 39, 45, 46, 48, 49, 55, 64, 63, 76, 85, 92, 94], а они, в свою очередь, являются представителями значительно более широкого круга доказательств нижних оценок сложности. В главе 2 рассматриваются нижние оценки сложности для следую -

щих моделей вычислений: схемы из функциональных элементов, синхронные схемы, булевы формулы, схемы в неполных базисах, монотонные схемы для вычисления полиномов, схемы без нулевых цепей и схемы ограниченной глубины.

Результатом анализа доказательств нижних оценок сложности является единая трактовка. Отметим основные положения. Во-первых, каждому доказательству нижней оценки сложности можно сопоставить некоторое множество $\mathcal{F}$ частичных булевых функций (определение см. в п.I.3), которое в большей степени характеризует это доказательство. Во-вторых, можно выделить два этапа, из которых определяющим является первый. На этом этапе производится эффективная оценка снизу ширины функции (см. п.2.I). Поскольку первый является определяющим, это означает, что доказательство нижней оценки сложности фактически сводится к нижней оценке ширины функции*.

Этот вывод является главным результатом главы 2. На его основе в следующей за ней главе строятся математические модели доказательств нижних оценок сложности. Глава 2 позволяет попытаться ответить на сформулированный выше первый вопрос. А именно, доказательство нижней оценки сложности можно считать эффективным, если множество $\mathcal{F}$ состоит лишь из функций "малой" сложности (например, сложности $O(n)$).

Глава 3 посвящена построению математических моделей доказательств нижних оценок сложности. Предлагаются две такие модели, которые называются соответственно "универсальная функция" и "универсальное доказательство". Доказательства нижних оценок сложности моделируются в них доказательствами нижних оценок сложности соответственно для универсальных функций и универсальных схем.

Первая модель является более точной, но имеет ограниченную применимость. Главное внимание мы уделяем второй модели. Она менее точна, поскольку моделирует только первый этап доказательства нижних оценок сложности, но применима к огромному большинству известных доказательств нижних оценок сложности.

В главе 3 на большом числе примеров показывается, что известные доказательства нижних оценок сложности действительно можно моделировать нашей моделью универсальных доказательств. При этом выясняется, что универсальные схемы для ряда моделей вычислений с ограничениями (схемы в некотором неполном базисе для функций трехзначной логики, схемы без нулевых цепей, схемы ограниченной глубины) имеют экспоненциально большую сложность. Мы рассматриваем это как ответ на второй вопрос, сформулированный выше. А именно, для названных моделей вычислений с ограничениями проблема нижних оценок сложности решается положительно, поскольку для этих моделей универсальные схемы имеют экспоненциально большую сложность.

* В ряде доказательств первый этап явным образом не присутствует, поскольку авторы удовлетворяются тривиальной нижней оценкой ширины.

Глава 4 посвящена конструированию универсальных схем. Такие схемы строятся для тех моделей вычислений (схемы из функциональных элементов, синхронные схемы и булевы формулы), для которых в главе 3 не были получены высокие нижние оценки сложности. Выясняется, что универсальные функции для этих моделей вычислений имеют "малую" сложность.

Результаты и конструкции главы 4 позволяют ответить на третий из сформулированных выше вопросов. А именно, для прогнозирования возможностей доказательства высоких нижних оценок сложности для новых моделей вычислений следует изучить сложность универсальной схемы. Значение этой сложности на качественном уровне позволяет судить о возможной величине нижних оценок сложности. Математическим выражением этого утверждения является

Теорема 4.8. Для произвольного множества $\mathcal{S}$ схем с полюсами из множества X ($|X| = n$) в классе схем из функциональных элементов универсальным доказательством $\mathcal{S}$ не выводимы нижние оценки сложности, превосходящие по порядку $s^2(s+n)$, если $L(\mathcal{S}) \leq s(n)$.

Похожую теорему (с несколько более высокими оценками) можно доказать и для синхронных схем. Для булевых формул найдена экономная реализация универсальных функций, но не универсальных схем. Поэтому выводы о трудностях доказательства высоких нижних оценок сложности в случае булевых формул надо делать с большей осторожностью.

Укажем работы, которые оказали идейное влияние на автора. Прежде всего следует отметить стимулирующую роль работ С.В.Яблонского [54, 96] и О.Б.Лупанова [I9, 20], в которых подчеркивалась важность и трудность проблемы нижних оценок сложности. В плане методологическое большое воздействие на автора оказали работы С.В.Яблонского [52] и Ю.И.Журавлева [8, I0], в которых построены математические модели эффективных алгоритмов для объяснения трудностей решения некоторых центральных задач теории управляющих систем. Понятие универсального доказательства нижних оценок сложности возникло под влиянием известной работы Э.И.Нечипорука [23], а также работы В.Пауля [76].

ГЛАВА I. ПРОБЛЕМА НИЖНИХ ОЦЕНОК СЛОЖНОСТИ

Краткий обзор содержания главы.

В п.I.I дается краткий обзор по проблеме нижних оценок сложности. Обзор не претендует на полноту. Это скорее исторический очерк проблемы. Его основное назначение – подвести читателя к тем задачам, которые составляют предмет исследования в данной книге. Подробное обсуждение методов доказательства нижних оценок сложности проводится в главе 2. Там же предлагается единая трактовка этих доказательств.

В п.I.2 обсуждаются различные подходы к уточнению понятия "эффективное доказательство нижней оценки сложности" и обосновывается предлагаемый подход.

В п.I.3 даются основные определения и обозначения, используемые в работе.

В п.I.4 приводятся определения универсальных функций и универсальных схем. Эти понятия в дальнейшем играют важную роль в данной работе.

I.I. Развитие проблемы нижних оценок сложности

Проблема нижних оценок сложности (сокращенно НОСЛ) имеет примерно полувековую историю. Она возникает совершенно естественно как только начинается изучение сложности. В самом деле, когда определено понятие сложности некоторого объекта, появляется естественное желание найти значение этой сложности или хотя бы хорошо оценить эту сложность сверху и снизу.

Задачи оценки сложности сверху и снизу существенно различаются по трудности. Действительно, чтобы оценить сверху сложность вычисления некоторой функции, достаточно предъявить *некоторое* ее вычисление (например, программу на некотором языке, машину Тьюринга, схему из функциональных элементов и т.п.) и оценить сверху сложность этого вычисления. Простота задачи оценки сложности сверху

объясняется тем, что любое конкретное вычисление функции дает верхнюю оценку сложности.

Дело коренным образом меняется, когда мы переходим к нижней оценке сложности. Для получения нижней оценки надо убедиться, что *все* вычисления данной функции имеют большую сложность. Перебор всех вычислений функции связан с неимоверным объемом работы (см., например, [52]), который немыслимо выполнить. Если же речь идет о вычислении не одной функции с фиксированным числом аргументов, а целой последовательности функций, то такой перебор становится принципиально невозможным из-за бесконечности множества вычислений.

Эти принципиальные трудности заставили отказаться от попыток дать хорошие нетривиальные* нижние оценки сложности произвольной функции. Проблема НОСЛ звучит теперь несколько иначе: доказать хорошую нижнюю оценку сложности не для произвольной функции, а для какой-нибудь функции.

I.I.I. Неэффективные нижние оценки сложности

В модифицированной постановке проблема НОСЛ вскоре нашла решение. В работе Дж.Риордана и К.Шеннона [8I] был предложен метод, получивший впоследствии название мощностного метода Шеннона, который позволяет доказать, что почти все функции (алгебры логики, зависящие от n переменных) имеют очень большую сложность. Этот результат получается в итоге сравнения числа функций от n переменных с числом схем, вычисляющих эти функции и имеющих сложность не более заданной величины $K(n)$.

В тех случаях, когда вычислительная схема допускает на входе слова произвольной длины (как, скажем, машина Тьюринга или нормальный алгорифм), то существование функций большой сложности доказывает диагональный метод, основанный на идее Кантора.

Казалось бы, проблема НОСЛ решена. Но решение, предлагаемое мощностным методом Шеннона или диагонализацией, оставляет чувство неудовлетворенности. Оно происходит оттого, что эти методы доказывают лишь существование сложных функций, но не применимы ни к каким конкретным (индивидуальным) функциям. К тому же, при описании этих

* Тривиальной НОСЛ мы называем такую, которая вытекает из необходимости просмотреть всю существенную входную информацию. Для естественных моделей вычислений эта оценка не превышает длины входной информации.

функций используются сложностные термины, в результате чего функция оказывается сложной, поскольку она сложна по определению. Такая тавтология, конечно, ни в коей мере не может нас удовлетворить.

Поэтому проблема НОСЛ вновь претерпела изменение формулировки. Теперь уже требовалось доказать высокие НОСЛ для функций, определение которых не использует сложностных категорий. Предполагалось, что такая формулировка проблемы поставит надежный заслон на пути неудовлетворительных решений. Действительно, те решения, которые доставляются мощностным методом Шеннона или диагонализацией, перестали подходить.

Решения проблемы НОСЛ в новой постановке были предложены рядом авторов [57, 73, 67, 87, 51]. Функции, рассматриваемые в этих работах, действительно не используют сложностных терминов при своем определении. Без этих терминов удается обойтись благодаря другим сильным выразительным средствам. Общим для всех этих работ является полиномиальное сведение вычисления сложных функций, построенных мощностным методом Шеннона или диагонализацией, к вычислению этих индивидуальных функций. Другими словами, эти работы не могут избежать применения мощностного метода Шеннона или диагонализации. Именно по этой причине упомянутые решения проблемы НОСЛ тоже трудно признать удовлетворительными.

Итак, проблема НОСЛ вновь нуждается в уточнении формулировки. Нетрудно понять, что сведения, о которых говорилось в предыдущем абзаце, возможны лишь к очень сложным функциям. Поэтому один из способов исключить из рассмотрения доказательства, подобные названным , состоит в том, чтобы решать проблему НОСЛ для не слишком сложных функций, например, для функций из класса NP или даже P. Тогда сведения существенно затрудняются, но полностью не исключаются. На таких путях доказывает нижние оценки сложности Н.К.Косовский [14] и некоторые другие.

Все нижние оценки сложности, о которых говорилось выше, являются в какой-то мере неудовлетворительными. Их принято называть неэффективными НОСЛ. Хотя точного определения понятия неэффективной НОСЛ не существует, можно отметить характерную черту этих НОСЛ – все они так или иначе опираются на мощностной метод Шеннона или диагонализацию.

I.I.2. Эффективные нижние оценки сложности

Начиная с 50-х годов, стали разрабатываться методы доказательства эффективных нижних оценок сложности. Эти методы основываются на весьма тщательном анализе структур вычислительных схем. Поэтому каждый такой метод привязан к вполне определенной вычислительной схеме, то есть к модели вычислений. Скажем, метод следов, разработанный Я.М.Бардзинем [2] и Ф.Хенни [65], применим только к одноленточным машинам Тьюринга, а методы В.М.Храпченко [49] и Э.И.Нечипорука [23] только к булевым формулам, причем первый из них – к формулам в конкретном базисе $\{\wedge, \vee, -\}$.

Поэтому, говоря об эффективных НОСЛ, надо уточнить прежде всего, с какими моделями вычислений мы работаем. Как известно (см., например, [82]), различные модели вычислений: машины Тьюринга в различных модификациях, РАМ-машины, нормальные алгорифмы и т.п., полиномиально эквивалентны между собой. Точнее, это означает следующее: любая функция, вычислимая на одной модели со сложностью L, вычислима на каждой из других моделей со сложностью не более L^c, где c – константа, зависящая от моделей. Поэтому неполиномиальная (например, экспоненциальная) НОСЛ, доказанная для одной модели вычислений, остается неполиномиальной и для другой модели. Если же НОСЛ полиномиальная, то при переходе к другой модели эта НОСЛ может превратиться в тривиальную НОСЛ. По этой причине невысокие НОСЛ (а эффективные НОСЛ именно таковы) имеют силу только для определенной модели.

Среди различных моделей вычислений особое место занимают схемы из функциональных элементов (СФЭ). Эти схемы в некотором естественном смысле полиномиально эквивалентны машинам Тьюринга (см., например, [62, 26]), а следовательно, и всем другим признанным моделям вычислений. В то же время СФЭ обладают большей простотой, поскольку имеют фиксированное число входов в отличие от машин Тьюринга и подобных им моделей. Это делает СФЭ более предпочтительными при доказательствах НОСЛ. В то же время все основные трудности, связанные с решением проблемы НОСЛ, не только сохраняют для них силу, но и выступают наиболее выпукло. Это объясняется тем, что в пределах полиномиальной эквивалентности СФЭ являются одной из наиболее мощных моделей.

Поскольку СФЭ вычисляют булевы функции, то мы будем интересоваться сложностью именно булевых функций. Это нисколько не ограничивает общность результатов, поскольку при вычислении булевых функций все трудности, связанные с получением НОСЛ, не только сохраняют силу, но и проявляются наиболее ярко.

В чем же заключаются эти трудности? В том, что несмотря на значительные усилия, не удается доказать высокие эффективные НОСЛ. В частности, для СФЭ получены только линейные (от числа переменных функции) НОСЛ [5, I2, 39, 40, 43, 55, 6I, 62, 76, 83, 84, 88]. Вопрос "Можно ли доказать нелинейные НОСЛ в классе СФЭ?" давно стоит в теории сложности. Разумеется, неэффективные НОСЛ мы при этом исключаем из рассмотрения. На протяжении уже нескольких десятилетий нет сколько-нибудь заметного прогресса на пути положительного решения этого вопроса.

Другой интересной моделью вычисления булевых функций являются булевы формулы. Их можно рассматривать как частный случай СФЭ. Этот частный случай характеризуется тем, что выход элемента может подаваться на вход лишь одного элемента. Про булевы формулы не доказано что они полиномиально эквивалентны СФЭ и, следовательно, другим признанным моделям вычислений. Поэтому следует ожидать, что в классе булевых формул можно доказать более высокие НОСЛ.

Это ожидание нашло частичное подтверждение в работе Б.А.Субботовской [44], которая получила нелинейные НОСЛ (вида $n^{3/2}$ по порядку) для формул в базисе $\{\wedge, \vee, \neg\}$. Следующее продвижение в этом направлении сделано в работах Э.И.Нечипорука [23] и В.М.Храпченко [48, 49]: в [23] НОСЛ в произвольном конечном базисе поднята до почти квадратичной ($n^2/\log n$ по порядку), а в [48, 49] до квадратичной (в конкретном базисе $\{\wedge, \vee, \neg\}$). Были разработаны и другие методы доказательств НОСЛ в классе булевых формул [66, 22, 58, 80]. Эти методы расширили границы применимости методов, но не смогли поднять величину НОСЛ выше, чем в [23, 48, 49]. Последнее продвижение было сделано А.Е.Андреевым, который на основе обобщения метода Б.А.Субботовской [44] и с использованием идеи универсальной функции Э.И.Нечипорука [23] получил более чем квадратичную НОСЛ для формул в базисе $\{\wedge, \vee, \neg\}$ (вида $n^{5/2}/((\log n)^{3/2} \log\log n)$ по порядку) (см. Андреев А.Е. Об одном методе получения более чем квадратичных эффективных нижних оценок сложности $\mathfrak{R}$ -схем // Вестн. МГУ. Мат., мех. - I987. - № I. - С.70 - 73).

I.I.3. Нижние оценки для моделей с ограничениями

Трудности решения проблемы НОСЛ вынудили искать успех на флангах. Стали рассматривать модели вычислений более слабые, чем СФЭ. Их называют моделями с ограничениями. Примерами таких моделей являются дизъюнктивные нормальные формы (ДНФ), схемы в неполных базисах, ограниченной глубины, без нулевых цепей (определения см. в п.2.6 - 2.I0) и т.п. Ни для одной из этих моделей не доказана их полиномиальная эквивалентность СФЭ. Это повышает шансы на решение проблемы НОСЛ для этих моделей, но, как мы уже видели на примере булевых формул, не дает гарантии успеха.

В случае ДНФ проблема НОСЛ решается положительно, причем без больших усилий (см. для справок [4]). Это объясняется тем, что задача построения экономной ДНФ является задачей на покрытие, а для последней нижние оценки сложности строятся без труда. В случае ДНФ задачу НОСЛ можно ставить даже для произвольной функции, причем для многих индивидуальных функций удается получить нетривиальные НОСЛ. Серьезные трудности здесь возникают лишь в тех случаях, когда функция имеет много больших интервалов, как, например, в случае отрицания кодовых функций [4I].

В случае других моделей с ограничениями задача НОСЛ не является непосредственно задачей на покрытие. Поэтому в этих случаях задача НОСЛ решается намного труднее. Однако, как показано в главе 2, в большом числе доказательств НОСЛ в случае всех моделей, в том числе и без ограничений, задачу НОСЛ удается свести к задаче на покрытие. На этом пути получаются нижние оценки сложности.

Первое существенное продвижение в решении проблемы НОСЛ для схем с ограничениями было получено в работе К.Шнорра [85] для монотонных схем, вычисляющих полиномы. Хотя полиномы и отличны от булевых функций, тем не менее идеи этой работы оказали заметное влияние на развитие проблемы НОСЛ вообще и оценки сложности булевых функций в частности. Работа [85] послужила как бы сигналом к штурму проблемы НОСЛ на моделях с ограничениями.

В последующие годы были получены экспоненциальные или близкие к ним НОСЛ для целого ряда моделей с ограничениями. Для схем, вычисляющих функции k -значной логики при $k \geqslant 3$ в неполных базисах, это сделал Г.А.Ткачев [45]. Для схем ограниченной глубины почти экспоненциальные НОСЛ установили Г.А. Ткачев [46], Л. Вэлиант [9I],

36527

М. Клэйв, В. Пауль, Н. Пиппенджер и М. Янакакис [69], А. Яо [97] и др.

Интересная и очень естественная модель (контактные схемы без нулевых цепей) была предложена А.К.Пулатовым [37]. Для частного случая этой модели (параллельно-последовательные схемы без нулевых цепей) он установил экспоненциальные НОСЛ. С.Е.Кузнецов [16] сумел распространить его оценки на случай произвольных контактных схем без нулевых цепей. Он же [15] перенес понятие схем без нулевых цепей на СФЭ и получил экспоненциальные НОСЛ для этой модели.

Долгое время остро стоял вопрос, можно ли получить высокие НОСЛ для неполного базиса в булевском случае. Из таких базисов наиболее интересен монотонный базис $\{\wedge,\vee\}$. Хотя с давних пор [24] в этом базисе получались более высокие НОСЛ, нежели в полном базисе, однако перейти порог оценки n^2, к которому подошел И.Вегенер [92, 94] и которого достигла Е.А.Окольнишникова [35], не удавалось. Решающий сдвиг произошел в 1985 г., когда А.Е.Андреев [1] и А.А.Разборов [38] опубликовали неполиномиальные (вида 2^{n^c} в [1] и $n^{c\log n}$ в [38]) НОСЛ в монотонном базисе.

I.I.4. Итоги развития проблемы НОСЛ

Подводя итоги, можно констатировать, что для целого ряда моделей с ограничениями проблема НОСЛ успешно решена. В то же время для наиболее интересных моделей, а именно, СФЭ и формул в полных базисах, проблема стоит незыблемо уже десятилетиями.

Мы вынуждены также признать, что проблема нижней оценки сложности не имеет отточенной формулировки. Главным препятствием на пути к достижению такой формулировки является неформализованность понятия "эффективное доказательство нижней оценки сложности". Пока такой отточенной формулировки не существует, мы можем представить проблему НОСЛ лишь совокупностью вопросов. Назовем важнейшие из этих вопросов.

Вопрос первый. Как провести четкую границу между эффективными и неэффективными доказательствами НОСЛ?

Вопрос второй. Почему для одних моделей с ограничениями высокие НОСЛ получаются легче, для других (например, схемы в монотонном базисе) значительно труднее, а для третьих вообще не получаются?

Вопрос третий. Можно ли прогнозировать возможности доказательства высоких НОСЛ для новых, еще не исследованных моделей вычислений?

Полувековая история проблемы НОСЛ продемонстрировала сложность этих вопросов. Поэтому трудно рассчитывать на то, что в близком будущем мы получим однозначные ответы на эти вопросы. В то же время для прогресса в решении проблемы НОСЛ важно искать ответы на поставленные вопросы. В такой ситуации нам представляется разумным искать компромиссные варианты. В данной книге развивается один из таких вариантов. Он заключается в построении математической модели доказательств НОСЛ. Эта модель призвана достаточно адекватно отразить текущее состояние проблемы НОСЛ и пролить свет на поставленные вопросы. Это должно способствовать лучшему пониманию проблемы НОСЛ и ориентировать при поисках путей решения этой проблемы.

Проблеме НОСЛ посвящены обзоры О.Б.Лупанова [20], автора [25], А.П.Бельтюкова [3], Д.Ю.Григорьева [7] и В.М.Храпченко [50]. Значительное место проблеме НОСЛ отведено в монографиях Дж.Савиджа [82] и автора [26] и в обзоре А.О.Слисенко [42].

I.2. Эффективные и неэффективные нижние оценки сложности

Мы видели в предыдущем параграфе, что длительные попытки решения проблемы НОСЛ не имели успеха в наиболее интересном случае, когда базис полон. Это позволяет предположить существование принципиальных трудностей, препятствующих решению проблемы НОСЛ. В частности, может оказаться, что при определенных условиях проблема НОСЛ вообще не разрешима, то есть высокие НОСЛ получить невозможно. Тогда нужно строить формальную теорию проблемы НОСЛ, в которой можно было бы доказать невыводимость высоких НОСЛ.

Однако этот замысел сталкивается с серьезной трудностью. Дело в том, что, строго говоря, высокие НОСЛ доказать можно, например, мощностным методом Шеннона. Другое дело, что такие доказательства нас не устраивают. Но тогда нужно уметь строго формально отделять эффективные НОСЛ от неэффективных. При попытках положительного решения проблемы НОСЛ необходимости в этом не возникает, поскольку на интуитивном уровне до сих пор не возникало затруднений при определении, эффективна НОСЛ или нет. Если же пытаться установить невыводимость высоких НОСЛ, нужно прежде всего провести формальную границу между эффективными и неэффективными доказательствами.

Уточнять понятие эффективности НОСЛ можно на разных путях. Один из естественных подходов состоит в том, чтобы измерять степень эффективности доказательства сложностью функции, для которой устанавливается НОСЛ: чем проще функция, тем эффективнее НОСЛ. Такой подход уже упоминался в предыдущем параграфе. Он действительно позволяет считать неэффективными шенноновское доказательство, а также доказательства из [5I, 57, 67, 73, 87], поскольку, скажем, для функций из класса NP эти доказательства уже не годятся. Однако при таком подходе проблема НОСЛ мало чем отличается от проблемы $P \stackrel{?}{=} NP$, то есть утрачиваются специфические черты проблемы НОСЛ. Как следствие этой утраты, не появляются никакие новые соображения о невозможности доказательств высоких НОСЛ.

В данной работе развивается другой подход к уточнению понятия эффективности НОСЛ. Он связывает понятие эффективности не со сложностью функции, подлежащей оценке снизу, а со средствами, используемыми при доказательстве. Основанием для такого подхода служит то обстоятельство, что целый ряд эффективных в интуитивном смысле доказательств НОСЛ (например, методы Нечипорука [23], Храпченко [49], Харпера–Сэвиджа [64], Малышева [22], см. также п.2.3 – 2.5) применимы почти ко всем булевым функциям, причем дают для них нетривиальные и притом невысокие НОСЛ. Эти оценки являются предметом серьезного рассмотрения, хотя несравненно уступают по величине оценкам, установленным для почти всех функций мощностным методом Шеннона. Отсюда следует, что понятие эффективности в этих примерах не связано с видом функций, для которых они устанавливаются, а является характеристикой доказательства.

Предложенный подход к уточнению понятия эффективности будет описан в п.2.II. Суть его состоит в том, что доказательствам НОСЛ сопоставляют задачи на покрытие. При этом в роли покрываемых объектов выступают частичные булевы функции (определение см. в п.I.3) функции f, подлежащей оценке, или подсхемы схемы для функции f. Мы ставим эффективность доказательства в зависимость от двух факторов.

Первым фактором является сложность "элементарных" частичных булевых функций или подсхем, о которых говорилось выше. Пусть s есть максимальная сложность этих элементарных функций или схем. Чем ниже эта сложность s, тем эффективнее доказательство. В частности, во всех доказательствах НОСЛ, рассматриваемых в главе 2, $s(n) = O(n)$. Это напоминает известный подход, который связывает

эффективность доказательства со сложностью функции, но отличается от него тем, что мы говорим о сложности только частичных булевых функций, а не всей функции. Второй фактор – это отношение λ величины нижней оценки сложности к сложности $s(n)$. Очевидно, $\lambda \geq 1$. Чем больше величина λ, тем эффективнее доказательство. Для неэффективных в интуитивном смысле доказательств $\lambda = 1$.

I.3. Основные понятия и обозначения

Множество двоичных наборов (векторов) длины n обозначим B^n. Оно является областью определения булевых функций n переменных. Множество B^n называют еще (n-мерным) кубом.

Мы используем стандартные обозначения для элементарных булевых функций: $\wedge$, $\vee$, $^-$, $\oplus$, $\sim$ обозначают соответственно конъюнкцию, дизъюнкцию, отрицание, сложение по модулю 2 и эквивалентность. Иногда мы пишем x^α вместо $x \sim \alpha$. Множество всех булевых функций обозначается P_2.

Символом X будем обозначать множество переменных булевой функции. Как правило, это множество $\{x_1, \ldots, x_n\}$. Множество булевых функций, зависящих от переменных $x_1, \ldots, x_n$, обозначается P_2^n или $P_2^n(X)$. Наряду с переменными X мы будем рассматривать дополнительные булевы переменные $Y (Y \cap X = \emptyset)$. Булеву функцию f с переменными X, Y обозначаем $f(X,Y)$ или $f(\tilde{x}, \tilde{y})$.

Пусть $A \subseteq X$. Подстановкой констант (на места переменных A) называется отображение $c : A \to \{0,1\}$. П о д ф у н к ц и е й булевой функции f, соответствующей подстановке c, называется функция $f_c : B^n \to \{0,1\}$, определяемая соотношением

$$f_c(x_1, \ldots, x_n) = f(u_1, \ldots, u_n),$$

где

$$u_i = \begin{cases} c(x_i), & \text{если } x_i \in A, \\ x_i & \text{в противном случае.} \end{cases}$$

Очевидно, функция f_c от переменных из A уже не зависит.

Если g есть подфункция функции f, то f называется н а д ф у н к ц и е й функции g.

Ч а с т и ч н а я булева функция (ч.б.ф.) – это функция, определенная на некотором подмножестве $D \subseteq B^n$ и принимающая значения 0 и I. Булева функция f называется д о о п р е д е л е –

нием ч.б.ф. g, если $f=g$ на всем множестве D. Функция g называется в этом случае частичной функцией функции f. Схема S реализует по определению ч.б.ф. g, если она реализует некоторое ее доопределение.

Переменная $x_i \in X$ называется существенной для булевой функции $f(X)$, если функция f содержит хотя бы одну из подфункций $x_i, \bar{x}_i$. Булевы функции f и g называются равными, если после отбрасывания всех несущественных переменных совпадают их множества переменных и отображения, ими осуществляемые.

Элементарная конъюнкция K – это выражение вида $x_{i_1}^{a_1} \dots x_{i_s}^{a_s}$, где все $a_j \in \{0,1\}$, а переменные $x_{i_1}, \dots, x_{i_s}$ все различны. Дизъюнктивная нормальная форма (ДНФ) – это дизъюнкция элементарных конъюнкций K. Конъюнкция K в этом случае называется еще д и з ъ ю н к т о м ДНФ.

С каждой ДНФ D естественным образом связывается булева функция, про которую говорят, что она реализуется ДНФ D. Две ДНФ называются эквивалентными, если они реализуют одну и ту же функцию.

Пусть ДНФ D реализует булеву функцию f. Дизъюнкт K ДНФ D называется п р о с т ы м и м п л и к а н т о м функции f, если при опускании любого вхождения переменной в конъюнкцию K полученная ДНФ не эквивалентна ДНФ D.

Элементы множества B^n называют иногда точками n-мерного куба. Множество точек $\tilde{a} \in B^n$, на которых булева функция $f \in P_2^n$ равна I, принято обозначать N_f.

На единичном кубе B_2^n определена метрика Хэмминга ρ. Для точек $\tilde{a} = (a_1, \dots, a_n)$, $\tilde{b} = (b_1, \dots, b_n)$ согласно определению $\rho(\tilde{a}, \tilde{b}) = \sum_{i=1}^{n} |a_i - b_i|$.

Перейдем к определению схем из функциональных элементов (СФЭ), которые для краткости будем называть просто схемами. Чтобы избежать громоздкости и неоправданного формализма, определим схемы для случая конкретного базиса $B_1 = \{\wedge, \vee, -\}$. Из определения будет ясно, как распространить его на другие базисы.

Пусть G – конечный ориентированный граф без контуров, в каждую вершину которого заходят не более двух дуг. Вершины, в которые не заходят дуги, называются в х о д а м и или п о л ю с а м и схемы. Остальные вершины называются в н у т р е н н и м и. Некоторые вершины графа G пометим как выходные. Не теряя общности, можно предполагать, что из каждой невыходной вершины ведет ориентированный путь хотя бы в одну выходную вершину.

Припишем теперь каждому полюсу букву алфавита $\{x_1, \dots, x_n\}$, каждой внутренней вершине с одной входящей дугой символ $-$, а вершине с двумя входящими дугами один из символов $\wedge$ или $\vee$. Внутренняя вершина вместе с приписанным ей символом называется (функциональным) э л е м е н т о м, а полученный граф называется с х е м о й и з ф у н к ц и о н а л ь н ы х э л е м е н т о в.

Графически элемент принято изображать треугольником с одним или двумя входами (по числу заходящих дуг). Символ булевой операции, приписанный вершине v, обозначают Оп (v). Если Оп (v) равен $\wedge$ или $\vee$, то вершину v называют соответственно $\wedge$-вершиной или $\vee$-вершиной.

Если схема содержит дугу (v, w), то вершина w называется с ы н о м вершины v, а вершина v – р о д и т е л е м вершины w. Транзитивное замыкание отношения быть родителем (сыном) называется отношением быть п р е д к о м (п о т о м к о м).

Каждая вершина v схемы S вместе со всеми своими предками определяет подсхему схемы S, которую будем обозначать $S(v)$. Выход схемы, как правило, обозначается символом t. Путь в схеме, начинающийся в вершине a и заканчивающийся в вершине w, обозначим ($a \Rightarrow w$). Мы ограничимся рассмотрением таких схем, в которых каждая вершина соединена путем с некоторым выходом.

Синтаксическое описание схем закончено. Перейдем к описанию семантики. Схемы служат для вычисления булевых функций.

Припишем булевы функции вершинам схемы S следующим образом. Каждому полюсу x_i приписывается функция x_i. Пусть некоторой вершине c предшествуют вершины a и b, которым уже приписаны функции $f_a(x_1, \dots, x_n)$ и $f_b(x_1, \dots, x_n)$. Если вершина c помечена символом $\wedge(\vee)$, то ей приписывается функция $f_a \wedge f_b$ ($f_a \vee f_b$). Если в вершину c заходит только одна дуга (а именно, из вершины a), то вершине c приписывается функция f_a. Про эту функцию будем говорить, что она в ы ч и с л я е т с я (р е а л и з у е т с я) с х е м о й S в в е р ш и н е c, и обозначим ее Функ (c). Таким образом можно найти Функ (d) для любой вершины d схемы S. Это понятие полезно в задачах анализа схем, например, при доказательстве нижних оценок сложности. Когда исследуют макроповедение схемы (то есть рассматривают ее как черный ящик со входами и выходами), интересуются только функциями, вычисляемыми схемой в выходных точ-

ках. Пусть выходные точки схемы некоторым образом упорядочены: v_1, v_2, ..., v_m. По определению схема S реализует булевы функции $f_1, \ldots, f_m$ (или говорят, булев (n, m)-оператор $(f_1, \ldots, f_m)$) если Функ $(v_i) = f_i(x_1, \ldots, x_n)$, $i = 1, \ldots, m$.

Две схемы называются эквивалентными, если они реализуют один и тот же булев оператор.

Приведенное определение схемы из функциональных элементов и реализуемого ею оператора очевидным образом можно распространить на случай произвольного базиса. В дальнейшем мы будем полагать, что это уже проделано, и иметь дело со схемами в произвольном конечном базисе. Более того, в качестве элементов базиса можно брать не только булевы функции, но, например, функции k-значной логики или операции некоторой алгебры (например, кольца).

С л о ж н о с т ь ю схемы S (обозначение $L(S)$) называется число внутренних вершин (то есть элементов) схемы S. Сложность булевой функции f – это минимальная сложность схемы, вычисляющей функцию f. Обозначается она $L(f)$. Схема S, вычисляющая функцию f, называется м и н и м а л ь н о й, если $L(S) = L(f)$.

Опишем теперь другую модель вычислений – б у л е в ы ф о р м у л ы. Их можно рассматривать как частный случай схем. Этот частный случай характеризуется тем, что каждая вершина может подаваться на вход лишь одной вершины, то есть иметь лишь одного сына. В силу такого определения формула может иметь много одноименных полюсов. Граф такой схемы является, очевидно, деревом, полюсы являются листьями этого дерева.

В случае формул под сложностью понимают число листьев, а не число внутренних вершин. В силу соотношения $\bar{\bar{u}} = u$ можно исключить из рассмотрения формулы, в которых встречаются последовательные одновходовые вершины. Тогда число листьев и число внутренних вершин по порядку равны (в случае конечного базиса). Сложность булевой функции f в классе формул обозначается $L_\Phi(f)$.

Введем теперь понятие параллельно-последовательной контактной схемы (П-схемы). П-схемы изоморфны булевым формулам в базисе $\{\wedge, \vee, {}^-\}$ в которых отрицания разрешается использовать лишь над знаками переменных. Иногда язык П-схем бывает удобнее. Поэтому дадим независимое определение. Контактом называется ребро графа вместе с приписанной ему буквой из алфавита $\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$.

Индуктивное определение П- с х е м ы выглядит так:

(I) один контакт (a, b) есть П-схема с полюсами a и b.

(2) если $S_1(a_1, b_1)$ и $S_2(a_2, b_2)$ суть П-схемы с полюсами соответственно a_1, b_1 и a_2, b_2, то

– результат отождествления $a_1 = a_2$, $b_1 = b_2$ есть П-схема с полюсами a_1, b_1 (п а р а л л е л ь н о е с о е д и н е н и е П-схем S_1 и S_2);

– результат отождествления $a_2 = b_1$ есть П-схема с полюсами a_1, b_2 (п о с л е д о в а т е л ь н о е с о е д и н е н и е П-схем S_1 и S_2).

Индуктивно определим булеву функцию, вычисляемую П-схемой. Если П-схема состоит из одного контакта x_i^d, то она вычисляет по определению функцию x_i^d. Если П-схемы S_1 и S_2 вычисляют соответственно функции f_1 и f_2, то их последовательное соединение вычисляет по определению функцию $f_1 \wedge f_2$, а параллельное соединение – $f_1 \vee f_2$.

Поскольку П-схемы изоморфны формулам в базисе $\{\wedge, \vee, {}^-\}$, то они могут рассматриваться как частный случай схем из функциональных элементов, в которых выходные степени всех вершин не превышают I. Однако мера сложности у них своя: $L_\Pi(S)$ – это число контактов П-схемы S. Эта мера может слегка отличаться от схемной сложности.

Введем, наконец, ряд обозначений. Мощность множества A обозначается $|A|$. В выражениях вида $\log a$ имеется в виду двоичный логарифм. $[a]$ и $]a[$ обозначают результат округления числа a до целого соответственно с недостатком и с избытком.

$a(n) \lesssim b(n)$, $a(n) = O(b(n))$ и $b(n) = \Omega(a(n))$ суть различные способы записи отношения $a(n) \leq c\, b(n)$, где $n \to \infty$, а c – некоторая константа.

I.4. Универсальные функции и универсальные схемы

В последующих главах широко используется понятие универсальности. Введем необходимые определения.

Пусть $\mathcal{F}(X)$ есть произвольное множество булевых функций с переменными из множества X, а Y есть дополнительное множество булевых переменных ($Y \cap X = \emptyset$). Булева функция $UF(X, Y)$ называется у н и в е р с а л ь н о й для множества $\mathcal{F}$, если для каждой функции $f \in \mathcal{F}$ существует подстановка констант $\tilde{c}$ на места переменных Y, при которой $UF_{\tilde{c}} = f$. Универсальную функцию множества $\mathcal{F}$ будем обозначать также $UF(\mathcal{F})$. Переменные из

Y называют еще свободными переменными. Их число должно быть не меньше $]\log|\mathcal{F}|[$. Существование универсальных функций очевидно.

Введем теперь понятие у н и в е р с а л ь н о й с х е м ы. Пусть $\mathcal{S}(X)$ есть некоторое множество схем, полюсам которых приписаны переменные из X (не обязательно все). Рассмотрим схему $UC(X,Y)$, у которой наряду с полюсами $x_1,\dots,x_n$ есть еще свободные входы $y_1,y_2,\dots(X\cap Y)=\emptyset$. Схема $UC(X,Y)$(пошагово) моделирует по определению схемы из множества $\mathcal{S}(X)$, если для каждой схемы $S\in\mathcal{S}(X)$существуют взаимно-однозначное отображение U множества вершин схемы S в множество вершин схемы $UC(X,Y)$ и подстановка констант $\hat{C}$ на места переменных Y , обладающие следующими свойствами:

(а) $U(x_i)=x_i$, $i=1,\dots,n$;

(б) $On(U(v))=On(v)$;

(в) каждое ребро (v,w) схемы S отображается в некоторый путь из $U(v)$ в $U(w)$, причем различные такие пути не имеют общих вершин за исключением разве лишь концевых вершин путей;

(г) $Функ_{\hat{C}}(U(v))$ = $Функ(v)$.

Схему $UC(X,Y)$ в таком случае называют также универсальной для множества схем $\mathcal{S}(X)$ и обозначают $UC(\mathcal{S})$.

Универсальные схемы можно строить тривиально - достаточно взять "объединение" схем из множества $\mathcal{S}$. Но такие схемы далеко не оптимальны по сложности. Символом $L(UC(\mathcal{S}))$будем обозначать минимальную сложность универсальной схемы множества схем $\mathcal{S}$. В заключение сформулируем очевидное

<u>Утверждение I.I</u>. Если $\mathcal{T}$ и $\mathcal{S}$ суть два множества схем и $\mathcal{T}\subset\mathcal{S}$, то универсальная схема $UC(\mathcal{S})$ является также универсальной для множества $\mathcal{T}$.

ГЛАВА 2. НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ И НИЖНИЕ ОЦЕНКИ ШИРИНЫ

В этой главе проводится анализ эффективных доказательств нижних оценок сложности (НОСЛ) для различных моделей вычислений, как с ограничениями, так и без них. В результате этого анализа рассмотренным доказательствам при всем их разнообразии удается дать единую трактовку, которая связывает с каждым доказательством НОСЛ некоторую задачу на покрытие. При этом в качестве покрываемых объектов выступают частичные функции исходной функции (то есть функции, подлежащей оценке снизу). Выясняется, что важным этапом доказательства является оценка снизу ширины схемы. Оценка, полученная на этом этапе, является в некотором смысле определяющей для величины НОСЛ. На втором этапе проводится усиление этой оценки. Величина усиления зависит от сложности частичных функций, которые фигурируют в задаче на покрытие. При эффективных доказательствах НОСЛ сложность этих частичных функций всегда небольшая (как правило, $O(n)$).

Рассматриваемые в этой главе доказательства НОСЛ почерпнуты из работ [39,I2,76,55,64,23,49,45,92, 94, 85, 29, 37, 46] различных авторов. При отборе доказательств автор руководствовался стремлением представить НОСЛ возможно более широко как в смысле разнообразия моделей вычислений, для которых эти оценки устанавливаются, так и в смысле методов доказательства. Этим объясняется обширность данной главы. Автор сознательно пошел на это, поскольку только на большом числе примеров можно убедить читателя в универсальности предлагаемой трактовки. Главное в этой трактовке - наличие тесной связи между задачей НОСЛ и задачей нижней оценки ширины функции. Предложенную трактовку можно рассматривать как первый этап построения математических моделей доказательств НОСЛ. Окончательное построение моделей будет проведено в следующей главе.

Ввиду обширности этой главы приведем краткий обзор ее содержания:

В п.2.I вводятся понятия ширины схемы и ширины функции и устанавливается связь этих понятий с понятием сложности. Понятие ширины играет важную роль в последующих параграфах этой главы.

В п.2.2 – 2.I0 анализируются представительные доказательства НОСЛ для различных моделей вычислений. Эти модели следующие: схемы из функциональных элементов в базисах $\{\wedge, \vee, ^-\}$ и B_2 (множество всех булевых функций двух переменных), синхронные схемы, булевы формулы в произвольном конечном базисе и в базисе $\{\wedge, \vee, ^-\}$, схемы в неполных базисах для функций трехзначной логики и булевых функций монотонные схемы для вычисления полиномов, схемы без нулевых цепей и схемы ограниченной глубины. С каждым из этих доказательств мы связываем некоторую задачу на покрытие. При этом покрываются частичные функции той функции, сложность которой оценивается. В качестве покрывающих объектов выступают подсхемы. Далее, в каждом доказательстве НОСЛ мы различаем два этапа, из которых первый – это оценка снизу ширины функции. Выявленные в п.2.2 – 2.I0 характерные черты доказательств НОСЛ будут положены в основу при построении математических моделей НОСЛ (это делается уже в следующей главе).

В п.2.II на основе анализа доказательств НОСЛ из п.2.2 – 2.I0 производится уточнение понятия эффективности при доказательстве НОСЛ. Оно связывается со сложностью частичных функций, о которых говорилось в п.2.2 – 2.I0.

В п.2.I2 устанавливается, что во всех рассмотренных доказательствах НОСЛ задачу нижней оценки сложности без большой погрешности можно заменить другой задачей, а именно, задачей нижней оценки ширины функции, поскольку полученная при этом оценка мало отличается по величине от нижней оценки сложности.

Материалы этой главы опубликованы в [25, 26, 29, 3I, 34, 74].

2.I. Ширина схемы и ширина функции

В этом параграфе мы вводим понятие ширины функции. В дальнейшем (п.2.I2) мы увидим, что задача оценки снизу ширины функции тесно связана с задачей НОСЛ.

Две различные вершины схемы из функциональных элементов называются несравнимыми, если не существует ориентированного пути в схеме, соединяющего одну из этих вершин с другой. Множество N вершин схемы S называется **независимым**, если каждая пара различных вершин из N несравнима. Максимальное число вершин

в независимом множестве схемы S называется шириной **схемы** и обозначается $W(S)$. Величина $\max W(S)$, где максимум берется по всем минимальным схемам S, реализующим функцию f, называется **шириной функции** f и обозначается $W(f)$.

Близким к понятию ширины схемы является понятие ширины сечения схемы. Множество T вершин схемы называется **сечением**, если любой путь, соединяющий некоторый вход схемы с выходом, содержит вершину из T. Сечение T называется тупиковым, если оно перестает быть сечением при удалении из T произвольной вершины. Примерами тупиковых сечений являются множество входных вершин и множество выходных вершин схемы. Максимальное число вершин в тупиковом сечении схемы S называется **шириной сечения** схемы S и обозначается $W_c(S)$. Величина $\max W_c(S)$, где максимум берется по всем минимальным схемам S, реализующим функцию f, называется шириной сечения функции f и обозначается $W_c(f)$.

Во многих доказательствах НОСЛ этой главы тупиковые сечения являются одновременно и независимыми множествами.

Введем также понятие реберной ширины. Две различные дуги называются независимыми, если они не принадлежат одновременно никакому ориентированному пути схемы S. В качестве примера можно указать дуги, выходящие из одной вершины схемы, или дуги, выходящие из входных полюсов. Множество дуг схемы называется независимым, если в нем каждая пара различных дуг независима. Максимальное число дуг в независимом множестве схемы S называется **реберной шириной** схемы и обозначается $W_e(S)$. Максимум величины $W_e(S)$ по всем минимальным схемам, реализующим функцию f, называется реберной шириной функции f и обозначается $W_e(f)$.

Определим теперь ширину П-схем. Множество T контактов П-схемы называется независимым, если никакие два контакта из T не принадлежат одной цепи. Аналогично случаю схем из функциональных элементов определяются ширина П-схемы $W_n(S)$ и ширина функции $W_n(f)$.

Установим связь между независимыми множествами контактов и тупиковыми сечениями. **Сечением** П-схемы называется такое множество ее контактов, которое содержит хотя бы по одному контакту из каждой цепи П-схемы. Сечение T называется **тупиковым**, если оно перестает быть сечением после удаления из T произвольного контакта.

Лемма 2.I. Тупиковое сечение П-схемы образует независимое множество.

Доказательство индукцией по числу m контактов в П-схеме. При $m=1$ утверждение очевидно.

Действуя по индукции, рассмотрим произвольную П-схему с m контактами. Она является либо параллельным, либо последовательным соединением двух П-схем S_1 и S_2. В случае последовательного соединения все тупиковое сечение T лежит в одной из схем S_1 и S_2 и в силу предположения индукции образует в ней независимое множество. Тогда оно независимо и в S. Легко рассматривается и случай параллельного соединения. □

2.2. Линейные нижние оценки сложности для схем из функциональных элементов

В этом параграфе рассматриваются доказательства НОСЛ в классе схем из функциональных элементов в базисах $B_1=\{\wedge,\vee,^-\}$ и $B_2=P_2^2$ (множество всех двуместных булевых функций). Доказательства упорядочены в соответствии с техническими приемами, используемыми при доказательстве. Как уже говорилось, при этом преследуется цель выявить множество $\mathcal{F}$ ч.б.ф., которое покрывается в этом доказательстве. Мы модифицировали некоторые доказательства по сравнению с оригиналом, чтобы облегчить отыскание множества $\mathcal{F}$.

Функции базиса B_2 разбиваются на 3 класса: функции типа $\wedge$ – это 8 функций вида $(x^a\wedge y^b)^c$, где $a,b,c\in\{0,1\}$, функции типа $\oplus$ – это функции $x\oplus y$ и $x\sim y$ и 6 функций от одной или нуля переменных. Очевиден следующий факт:

Утверждение 2.I. Если минимальная схема в базисе B_2 реализует функцию, зависящую существенно от двух или более переменных, то она содержит только элементы типов $\wedge$ и $\oplus$ *.

2.2.I. Техника доказательств: подстановка констант

Одним из наиболее распространенных приемов при доказательстве НОСЛ является подстановка констант (как правило, на места переменных). Особенно широко этот прием используется в базисе $B_1=\{\wedge,\vee,^-\}$. Его применение основано на следующем свойстве схем:

* Здесь считается, что элемент имеет тот тип, каков тип функции, приписанной этому элементу. Элемент "отрицание" называется еще инвертором.

Утверждение 2.2. Если на вход некоторого двухвходового элемента схемы в базисе B_1 подается константа 0 или I, то этот элемент можно удалить из схемы, сохранив функцию схемы.

Доказательство очевидно ввиду соотношений $x\vee 0=x$, $x\vee 1=1$, $x\wedge 0=0$, $x\wedge 1=x$.

Очевидно, для каждой из функций $\wedge$ и $\vee$ существует константа, при подаче которой на место одной переменной функция обращается в константу, то есть не зависит от второй переменной. Эта константа (0 для $\wedge$ и I для $\vee$) называется забивающим значением переменной, а операция подачи этой константы называется забиванием второй переменной.

Замечание. Операция забивания применима не только к $\wedge$ и $\vee$, но и к произвольной функции типа $\wedge$, то есть к функции вида $(u^a\wedge v^b)^c$. Это свойство будет использовано в последующих п.п.

Продемонстрируем прием забивания на примере линейной функции $l_n=x_1\oplus\ldots\oplus x_n$. Обозначим $\bar{l}_n=l_n\oplus 1$.

Лемма 2.2. [39]. Пусть S_n^{min} – произвольная минимальная схема, реализующая одну из функций l_n или $\bar{l}_n$ $(n\geq 3)$. Если в схеме есть полюсы 0 и I, то найдутся 4 или более элементов, после удаления которых получится схема S_{n-1}, реализующая l_{n-1} или $\bar{l}_{n-1}$.

Доказательство основано на тщательном переборе возможных структур схемы. Упорядочение перебора ведется по таким признакам, как:

– есть ли переменная, которая подается на вход инвертора,

– если нет, то существует ли переменная, которая подается на входы ровно одного или не менее трех элементов схемы.

Мы не будем разбирать все возможные случаи, поскольку их слишком много. Проиллюстрируем прием забивания на одном из случаев. Этот случай изображен на рис.2.I и характеризуется следующим:

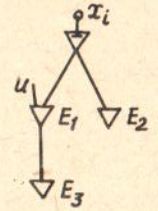

Рис.2.I. Фрагмент схемы для линейной функции

некоторая переменная подается на вход инвертора, выход которого "ветвится". Элементы E_1 и E_2 отличны от инверторов в силу минимальности схемы. Далее, они не могут быть выходными (иначе переменная x_i забила бы все остальные переменные, что противоречит линейности функций ℓ_n и $\bar{\ell}_n$). Элементы E_1 и E_2 не могут одновременно подаваться на входы друг друга, поскольку это привело бы к образованию ориентированного цикла в схеме. Поэтому в ней существует элемент E_3 (см. рис.2.I). Выберем такое значение переменной x_i, которое забивает u . Тогда с учетом утверждения 2.2 можно удалить все 4 элемента на рис.2.I. Полученная схема реализует ℓ_{n-1} или $\bar{\ell}_{n-1}$.

Из леммы 2.2 легко вытекает нижняя оценка сложности линейной функции в базисе B_1 :

$$L(\ell_n) \geq 4n-4 .$$

Проведем теперь краткий анализ доказательства леммы 2.2. Для этого определим сначала некоторые ч.б.ф. Пусть e есть произвольное ребро куба B^n, то есть пара точек $\tilde{a}, \tilde{b} \in B^n$ таких, что $\rho(\tilde{a}, \tilde{b}) = 1$. Определим частичную булеву функцию $\varphi_e(\tilde{x})$ следующим образом:

$$\varphi_e(\tilde{x}) = \begin{cases} 1, \text{ если } \tilde{x} = \tilde{a} , \\ 0, \text{ если } \tilde{x} = \tilde{b} , \\ \Delta \text{ в остальных случаях} \end{cases}$$

(здесь $\Delta \in \{0,1\}$). Положив $\bar{\Delta} = \Delta$, можно считать определенной функцию $\bar{\varphi}_e(\tilde{x})$.

Как мы доказали существование в схеме элемента E_3 (остальные элементы на рис.2.I существуют по условию)? Этот элемент необходим для того, чтобы на выходе схемы была реализована функция, доопределяющая ч.б.ф. вида $\varphi_e(\tilde{x})$.

Отберем теперь для каждого ребра e по одной функции из пары (φ_e , $\bar{\varphi}_e$) так, чтобы каждая из отобранных ч.б.ф. являлась частичной функцией функции схемы. Полученное множество ч.б.ф. $\mathcal{F}$ характеризует доказательство леммы 2.2 в том смысле, что существование тех или иных элементов обосновывается необходимостью доопределить на выходе функции из $\mathcal{F}$.

Ширина схемы оценивается здесь тривиально - числом входных полюсов.

Прием подстановки констант работает и в базисе B_2 , поскольку для этого базиса с небольшой модификацией сохраняет силу утверждение 2.2. Эта модификация состоит в том, что при удалении элемента может понадобиться и замена операции, приписанной последующему элементу. К примеру, пусть элемент $\varphi(x,y)$ подается на первый вход вершины с операцией $\psi(u,v)$. Пусть далее, к примеру, $\varphi(x,0) = \bar{x}$. Тогда при подаче 0 на второй вход элемента $\varphi(x,y)$ можно удалить этот элемент, заменив операцию $\psi(u,v)$ на $\chi(u,v) = \psi(\bar{u},v)$.

2.2.2. Техника доказательств: взаимное размещение элементов

Одна из первых нетривиальных нижних оценок сложности в базисе B_2 , состоящем из всех булевых функций двух переменных, была установлена в работе Б.М.Клосса и В.А.Малышева [I2]. При доказательстве нижней оценки в этой работе было учтено взаимное расположение элементов в минимальной схеме. В этом п. описывается этот прием. Символ $L(\ )$ обозначает в этом п. сложность в базисе B_2 .

Схема называется приведенной, если из каждой ее вершины, кроме выходной, выходит хотя бы одна дуга. Очевидно, для каждой схемы существует эквивалентная ей приведенная схема не большей сложности.

Утверждение 2.3. Пусть приведенная одновыходная схема S сложности L содержит ρ_i полюсов с выходной степенью i и v_i элементов с выходной степенью i ($i = 1, \ldots, L$). Тогда

$$L(S) \geq \rho_1 + 2\rho_2 + \ldots + L\rho_L + v_2 + 2v_3 + \ldots + (L-1)v_L - 1 .$$

Справедливость утверждения следует из того, что входящих дуг в схеме не более $2L$, а выходящих $\rho_1 + 2\rho_2 + \ldots + L\rho_L + L - 1 + v_2 + \ldots + (L-1)v_L$. Пояснение к слагаемому $L-1$: все элементы, кроме выходного, имеют хотя бы по одной выходящей дуге.

Функция f называется п а р н о - р а з д е л и м о й , если для любой пары различных аргументов x_i, x_j из $\mathcal{X}$ и любых двух пар $(a_i, a_j), (b_i, b_j)$ значений этих аргументов таких, что $a_i + a_j \neq b_i + b_j$ (сложение обычное, а не по модулю 2 !) существует подфункция $\varphi(x_i, x_j)$ функции f , р а з д е л я ю щ а я эти две пары (a_i, a_j) и (b_i, b_j) (функция $\varphi(x_i, x_j)$ разделяет по определению пары (a_i, a_j) и (b_i, b_j), если $\varphi(a_i, a_j) \neq \varphi(b_i, b_j)$).

В качестве примера парно-разделимой функции можно рассмотреть универсальную функцию множества

$$\mathcal{F} = \{ x_i \wedge x_j , \; x_i \oplus x_j \mid 1 \leq i < j \leq n \} \qquad (2.1)$$

или множества

$$\mathcal{F}=\{x_i \wedge x_j\ ,\ x_i \vee x_j \mid 1 \le i<j \le n\}\ . \qquad (2.2)$$

Существуют парно-разделимые функции, не имеющие дополнительных переменных, например, функция

$$f_n=((\sum_{i=1}^{n} x_i)\ mod\ 3)\ mod\ 2\ ,\quad n\ge 3\ .$$

Отметим характеристические свойства функций типов $\wedge$ и $\oplus$ применительно к парной разделимости.

Утверждение 2.4. Функция типа $\oplus$ не разделяет пары (0,0) и (1,1), а функция типа $\wedge$ не разделяет одну из пар (0,1), (1,0) с одной из пар (0,0), (1,1).

Нижеследующая теорема 2.1 является небольшой модификацией теоремы из [I2]. Модификация состоит в том, что функции f разрешается иметь дополнительные переменные y.

Теорема 2.1. Если функция $f(x,y)$ парно-разделима, то

$$L(f) \ge (10n-5)/9\ .$$

Доказательство. Мы повторим доказательство из [I2] с небольшими упрощениями, чтобы убедиться, что оно сохраняет силу при введении дополнительных переменных, и выявить множество покрываемых ч.б.ф.

Пусть S есть произвольная минимальная схема, реализующая функцию $f(x,y)$. В силу утверждения 2.1 схема содержит только элементы типов $\wedge$ и $\oplus$.

Функция f в силу парной разделимости зависит существенно от всех переменных из x. Поэтому в схеме S есть полюсы x_1 $\dots, x_n$, причем $n \ge 2$. Пусть ρ_1 из них имеют выходную степень 1. Назовем эти полюсы о т м е ч е н н ы м и.

Предположим, что в схеме S есть вершина a, на оба входа которой подаются отмеченные полюсы x_i и x_j. Они должны быть различными в силу минимальности схемы. На выходе вершины a вычисляется функция одного из типов $\wedge$ и $\oplus$. Поэтому на выходе этой вершины (а следовательно, и всей схемы) не может вычисляться парно-разделимая функция в силу утверждения 2.4.

Комментарий 1. Отнесем к искомому множеству $\mathcal{F}$ покрываемых ч.б.ф. две или более функции переменных x_i, x_j, которые в совокупности обеспечивают разделимость переменных x_i и x_j. На основании необходимости покрыть эти ч.б.ф. мы заключили, что вершины a описанного вида в схеме S быть не может.

Следовательно, схема S содержит ρ_1 различных вершин, на входы которых подаются отмеченные полюсы. Если такая вершина имеет выходную степень 1, будем называть ее о т м е ч е н н о й (она по определению отлична от полюса).

Обозначим символом ℓ число отмеченных вершин. Тогда $\rho_1-\ell$ вершин, на входы которых подаются отмеченные полюсы, имеют выходную степень не менее 2.

Из утверждения 2.3 следует

$$L \ge \rho_1 + 2(n-\rho_1)+\rho_1-\ell-1 = 2n-\ell-1\ . \qquad (2.3)$$

Докажем теперь, что $L \ge 1.25\ell$. Для этого рассмотрим взаимное расположение вершин.

Лемма 2.3. Пусть a и b – отмеченные вершины минимальной схемы S, причем a непосредственно предшествует b. Тогда вершина a типа $\wedge$, а вершина b типа $\oplus$.

Доказательство. Пусть на входы вершин a и b подаются соответственно отмеченные полюсы x_i и x_j. Если вершина b имеет тип $\wedge$, то обозначим символом d забивающее значение переменной x_j на входе элемента b. Тогда на выходе этого элемента не разделяются пары $(0,d)$ и $(1,d)$ значений переменных x_i, x_j. Ввиду отмеченности вершин a и b не разделяются они и на выходе схемы. Поэтому вершина b имеет тип $\oplus$ в силу минимальности схемы и утверждения 2.1. Если бы и вершина a имела тип $\oplus$, то на выходе вершины b вычислялась бы функция вида $x_i \oplus x_j \oplus h(x \setminus \{x_i, x_j\})$, которая не может разделить пары (0,0) и (1,1) значений переменных x_i, x_j. □

Комментарий 2. При доказательстве леммы вновь использованы ч.ф., отмеченные в комментарии 1. Типы вершин мы установили, исходя из необходимости покрыть ч.ф. из множества $\mathcal{F}$.

Следствие. Вершина b из условия леммы 2.3 не может подаваться на вход отмеченной вершины схемы S.

Отсюда вытекает, что выходы по крайней мере половины отмеченных вершин подаются на входы неотмеченных. Поэтому число последних не менее $\ell/4$. Следовательно,

$$L \ge \ell + \ell/4 = 5\ell/4\ ,\ \text{то есть}\ 4L \ge 5\ell\ . \qquad (2.4)$$

Переписав (2.3) в виде $5L \ge 10n-5\ell-5$ и сложив его с (2.4), получим утверждение теоремы. □

Если свойство парной разделимости выполняется и для подфункций функции f, можно получить для f и более высокую нижнюю оценку. Функция $f(X)$ называется m раз парно-разделимой, если при подстановке вместо любых $m-1$ переменных произвольных констант получившаяся функция снова парно-разделима.

Пример. Функция $C_n(x_1,\dots,x_n)=\sum\limits_{1\le i<j\le n} x_i x_j$ $n-2$ раза парно-разделима.

Теорема 2.2.[12]. $L(C_n(x_1,\dots,x_n))\ge 2(n-1)$ при $n\ge 3$.

Доказательство индукцией по n. При $n=3$ перебором убеждаемся, что $L(C_3)\ge 4$. Выберем теперь в схеме полюс x_i с выходной степенью не менее двух (он существует в силу парной разделимости) и положим $x_i=0$. Тогда полученная схема реализует функцию C_{n-1} и содержит по крайней мере на 2 элемента меньше (в силу аналога утверждения 2.2).

Комментарий 3. В теоремах 2.1 и 2.2 ширина схемы оценивается снизу числом n полюсов $x_1,\dots,x_n$. Существование вершин, число которых и определяет величину нижней оценки, обосновывается необходимостью покрытия функций из множества $\mathcal{F}$ (см. комментарий 1 к теореме 2.1). В частности, множество $\mathcal{F}$ может быть таким, как в (2.1) или (2.2).

2.2.3. Техника доказательств: учет расщеплений

Под расщеплением понимается вершина схемы, имеющая выходную степень не менее 2. Как видно из утверждения 2.3, наличие таких вершин повышает сложность схемы. Поскольку реально не удается доказать существование в схеме вершин с выходной степенью более 2, то мы сформулируем частный случай утверждения 2.3:

Утверждение 2.5. Если схема S имеет n полюсов, ρ расщеплений и одну выходную вершину, то

$$L(S)\ge n+\rho-1 . \qquad (2.5)$$

Частично учет расщеплений проводился уже в теореме 2.1. В нижеследующей теореме 2.3 мы используем этот прием в полной мере. Он был разработан В.Паулем в [76].

Нетрудно заметить, что при оценке сложности парно-разделимых функций в п.2.2.2 условия леммы 2.3 были выполнены с трудом. Поэтому, если потребовать от парно-разделимой функции "немного" дополнительных свойств, условия леммы 2.3 перестанут выполняться, и в схеме появится много новых расщеплений. Мы потребуем от парно-разделимой функции, чтобы она была надфункцией множества функций $\mathcal{F}$ из (2.1).

Следующее утверждение является переформулировкой леммы из [76].

Лемма 2.4. В минимальной схеме для универсальной функции множества $\mathcal{F}$ из (2.1) каждой паре полюсов $x_i, x_j\in X$ соответствуют такие пути $(x_i\Rightarrow t)$ и $(x_j\Rightarrow t)$, что до их первого пересечения хотя бы один из них разветвляется.

Доказательство от противного. Пусть пути $(x_i\Rightarrow t)$ и $(x_j\Rightarrow t)$ впервые встречаются в вершине a и до этого они не разветвляются. Тогда при произвольной подстановке констант на места переменных, отличных от x_i и x_j, тип функции $\varphi(x_i,x_j)$, вычисляемой в вершине a, совпадает с типом вершины a либо функция $\varphi(x_i,x_j)$ не зависит хотя бы от одной из переменных x_i, x_j. Поэтому такая схема не может вычислять нашу функцию.

Комментарий. Универсальные функции множеств $\mathcal{F}$ из (2.1) и (2.2) в равной мере парно-разделимы. Поэтому для них обеих имеет силу оценка теоремы 2.1. В случае леммы 2.4 множество $\mathcal{F}$ из (2.2) уже не годится. Здесь требуется, чтобы для каждой пары i,j $(i\ne j)$ множество $\mathcal{F}$ содержало функции обоих типов (и $\wedge$ и $\oplus$).

Сформулируем теперь теорему из [76] в удобных для нас терминах:

Теорема 2.3. Для универсальной функции UF множества функций $\mathcal{F}$ из (2.1)

$$L(UF)\ge 2n-2$$

в базисе B_2.

Доказательство. В произвольной минимальной схеме для функции UF имеется $n-1$ таких полюсов $x_i\in X$, что путь $(x_i\Rightarrow t)$ разветвляется. В противном случае для некоторых $x_{i_0}, x_{j_0}\in X$ существовало бы только по одному пути $(x_{i_0}\Rightarrow t)$ и $(x_{j_0}\Rightarrow t)$, что противоречит лемме 2.4.

Возьмем в каждом из $n-1$ путей $(x_i\Rightarrow t)$ первую вершину с выходной степенью не менее 2. Эти вершины попарно различны в силу леммы 2.4. Применение утверждения 2.5 дает оценку $2n-2$. □

2.2.4. Техника доказательств: присваивание функций

Мы рассматривали в п.2.2.1 прием, который заключается в присваивании некоторой переменной некоторой булевой константы. В данном параграфе этот прием обобщается до присваивания произвольной

булевой функции некоторой переменной. Этот прием был предложен В.Паулем [76]. Мы продемонстрируем его на примере оценки сложности универсальной функции множества

$$\mathcal{F} = \{x_1, \ldots, x_n\}. \tag{2.6}$$

Теорема 2.4. Для универсальной функции UF множества $\mathcal{F} = \{x_1, \ldots, x_n\}$ в базисе B_2 справедлива нижняя оценка

$$L(UF(\mathcal{F})) \geq 2n-2. \tag{2.7}$$

Доказательство почти дословно повторяет доказательство из [76]. При $n=1$ утверждение очевидно. Пусть теперь $n \geq 2$. Возможны три случая.

Случай 1. Существует $x_i \in \mathcal{F}$ такое, что выходная степень полюса x_i не меньше 2.

Случай 2. Существует $x_i \in \mathcal{F}$ такое, что выходная степень полюса x_i равна 1 и единственное ребро, выходящее из x_i, идет в вершину типа $\wedge$.

Случай 3. Существует $x_i \in \mathcal{F}$ такое, что выходная степень полюса x_i равна 1 и единственное ребро, выходящее из x_i, идет в вершину типа $\oplus$. Обозначим эту вершину v.

Рассмотрим только третий случай, поскольку в первых двух применяется уже встречавшаяся в п.2.2.1 – 2.2.3 техника. В случае 3 вершина v не может быть выходной. Действительно, выберем значения дополнительных переменных так, чтобы $UF = x_j$ $(j \neq i)$. При этом функция, вычисляемая в вершине v, зависит от x_i вопреки определению нашей универсальной функции. Поэтому вершина v не выходная.

Пусть на второй вход вершины v подается некоторая функция y. Подадим ее и на место x_i, то есть положим $x_i := y$ (в этом и состоит новый прием). Тогда в вершине v реализуется константа, и из схемы можно удалить элемент v и следующий за ним элемент. Подстановка $x_i := y$ может сильно изменить реализуемую на выходе функцию, но универсальная функция множества $\mathcal{F}$ из (2.6) устойчива к таким подстановкам, поскольку при подходящих значениях дополнительных переменных она равна x_j независимо от значений остальных переменных из $\mathcal{X} \setminus \{x_j\}$. Поэтому после замены $x_i := y$ полученная схема реализует универсальную функцию $UF(\mathcal{F} \setminus \{x_i\})$. Остается воспользоваться предположением индукции. □

В каждом из рассмотренных в п.2.2.1 – 2.2.3 доказательств НОСЛ как правило, использовался лишь один из описанных приемов (не считая подстановок констант). Комбинирование различных приемов (и особенно, учет взаимного расположения вершин) позволяет доказать следующее утверждение:

Теорема 2.5. Для универсальной функции множества

$$\mathcal{F} = \{x_i \wedge x_j,\ x_i \oplus x_j \mid 1 \leq i \leq j \leq n\}$$

имеет место следующая нижняя оценка в базисе B_2:

$$L(UF(\mathcal{F})) \geq 3n-3.$$

Доказательство следует доказательствам работ [76, 55]. Здесь оно не приводится, поскольку требует нескольких страниц текста, а необходимая техника уже описана выше.

Комментарий. Множества частичных функций $\mathcal{F}$ в теоремах 2.4 и 2.5 явным образом указаны. Можно заметить, что в теореме 2.5 оно отличается от (2.1) лишь функциями вида $x_i \wedge x_i$, то есть x_i. Это позволяет доказывать теорему 2.5 комбинированием приемов доказательств теорем 2.3 и 2.4.

2.3. Нижняя оценка в классе синхронных схем

В этом параграфе рассматривается нижняя оценка в классе синхронных СФЭ (определение см. ниже) из работы Л.Харпера и Дж.Сэвиджа [64]. Показывается, что это доказательство сводится к нижней оценке ширины функции. При этом характерно то обстоятельство, что удается оценить снизу большое количество (по порядку $\log n$) непересекающихся независимых множеств, что приводит к нижней оценке $cn \log n$ (c – некоторая константа). Последнее удается благодаря синхронности схем.

Сложность реализации "почти всех" булевых функций в классе синхронных схем исследована в работе О.Б.Лупанова [18].

СФЭ называется синхронной, если каждая ее вершина удовлетворяет следующему условию: все (ориентированные) пути, ведущие из полюсов в эту вершину, имеют одинаковую длину. При физической интерпретации это означает, что входные сигналы достигают данной вершины одновременно. В этом параграфе под схемами понимаются синхронные СФЭ. Максимальное число переменных у базисных функций в этом параграфе обозначается через r.

Вершины синхронной схемы естественным образом делятся на ярусы. t-й ярус образуют вершины, в которые ведут пути длины t (из полюсов). Наибольший номер яруса называется глубиной схемы S

и обозначается $D(S)$. Глубиной функции f (обозначение $D(f)$) называется минимальная глубина схемы, реализующей функцию f.

Мы будем рассматривать лишь такие схемы, в которых каждая вершина соединена путем с некоторым выходом. Очевидно, для каждой функции существует минимальная схема такого вида.

Каждый ярус синхронной СФЭ образует очевидно независимое множество вершин схемы. Нижняя оценка работы [64] основана на оценке мощности этих множеств. Обозначим вершины t -го яруса синхронной СФЭ S, вычисляющей некоторую функцию F, символами $a_1, \dots, a_p$. Функции, вычисляемые схемой S в этих вершинах, обозначим соответственно $h_1, \dots, h_p$.

Пусть A есть произвольное подмножество множества переменных X. Обозначим символом F_A множество различных булевых функций которые получаются из функции $F(X,Y)$ при всевозможных подстановках констант на места всех переменных, кроме переменных множества A. Поскольку вершины $a_1, \dots, a_p$ образуют сечение схемы S, то

$$|F_A| \le \prod_{j=1}^{p} |(h_j)_A| . \qquad (2.7)$$

Из этого неравенства можно извлечь нижнюю оценку для p, если иметь нижнюю оценку для $|F_A|$ и верхнюю оценку для $|(h_j)_A|$. Покажем, как это можно сделать.

Среднее значение произвольной величины q по всем m -элементным подмножествам $A \subseteq X$ обозначим $M(q, m, X)$. Следующая лемма является небольшим обобщением утверждения из [64]. Обобщение состоит в том, что у оператора разрешаются дополнительные переменные Y.

Лемма 2.5. Пусть существенные переменные оператора $g(X,Y)$ принадлежат множеству $B \subseteq X \cup Y$, $|B| = b$. Тогда при условии $0 < mb/(n-m-b) < 1$

$$M(\log_r |g_A|, m, X) \le 1/(1-R), \qquad (2.8)$$

где $R = mb/(n-m-b)$ (напоминаем, что r – это максимальное число переменных у базисных функций).

Доказательство. Выберем произвольное m -элементное подмножество A множества X. Пусть $|A \cap B| = k$. Разнообразие операторов в множестве g_A достигается за счет подстановок констант на места переменных из $B \setminus A$. Поэтому $|g_A| < r^{b-k}$ и $\log_r |g_A| \le b-k$. Число способов выбора подмножества A из X, при которых $|A \cap B| = k$, равно $C_{b'}^{k} C_{n-b'}^{m-k}$, где $b' = |B \cap X|$. Поэтому

$$M(\log_r |g_A|, m, X) \le \frac{1}{C_n^m} \sum_{k=0}^{u} C_{b'}^{k} C_{n-b'}^{m-k} (b-k) \qquad (2.9)$$

где $u = \min(m, b')$.

Для оценки суммы в правой части неравенства (2.9) выясним, который из членов суммы больше. Для этого, обозначив k -й член суммы символом d_k, оценим отношение двух соседних членов.

$$\frac{d_{k+1}}{d_k} = \frac{C_{b'}^{k+1} C_{n-b'}^{m-k-1} (b-k-1)}{C_{b'}^{k} C_{n-b'}^{m-k} (b-k)} < \frac{(b'-k)(m-k)}{(k+1)(n-b'-m+k+1)} \le \frac{mb}{n-b-m}.$$

Обозначив последнее отношение R и учитывая, что по условию $0 < R < 1$, можем заключить, что в сумме (2.9) член d_0 максимальный. Поэтому

$$M(\log_r |g_A|, m, X) \le \frac{1}{C_n^m} \sum_{k=0}^{u} d_k \le \frac{d_0}{C_n^m} \sum_{k=0}^{\infty} R^k = \frac{C_{n-b'}^{m}}{C_n^m} \sum_{k=0}^{\infty} R^k \le \frac{1}{1-R}.$$

Лемма доказана. □

Применим эту лемму к функциям h_j, реализуемым схемой S на t -м ярусе. Для этого надо убедиться, что выполнено условие $0 < R < 1$. Для каких номеров ярусов оно выполняется? Ответ на этот вопрос дает

Следствие. Если номер t яруса удовлетворяет неравенству

$$r^t \le \frac{\delta(n-m)}{m+\delta} \qquad (2.10)$$

при некотором $\delta (0 < \delta < 1)$, $m < n$ и $m \ge 1$, то

$$M(\log_r |(h_j)_A|, m, X) \le \frac{1}{1-\delta}$$

(r обозначает максимальное число переменных у базисных функций).

Доказательство. Вершине t -го яруса предшествуют не более r^t полюсов. Поэтому

$$b \le r^t . \qquad (2.11)$$

Убедимся сначала, что в условиях следствия $R = mb/(n-m-b) > 0$. Поскольку $mb > 0$, достаточно проверить, что $n-m-b > 0$, или ввиду (2.10), (2.11) более сильное неравенство $n-m-\frac{\delta(n-m)}{m+\delta} > 0$. Ввиду $m > 0$ последнее неравенство очевидно.

Поскольку R есть растущая функция b, то ввиду (2.10) и (2

$$R = \frac{mb}{n-m-b} \le \frac{mr^t}{n-m-r^t} \le \delta < 1 \ .$$

Итак, для функции h_j выполнены условия леммы 2.5, причем $0 < R \le \delta$. Подставив эту оценку в (2.8), получим утверждение следствия.

Имея верхнюю оценку для величин $|(h_j)_A|$, точнее, оценку сре днего значения логарифма этих величин, можно перейти к оценке сни ширины ρ сечения на основе неравенства (2.7).

Следующую лемму можно извлечь из работы [64].

Лемма 2.6. Если номер t яруса удовлетворяет условиям следс вия леммы 2.5, то число ρ вершин t-го яруса произвольной синх ронной схемы, реализующей функцию $F(X,Y)(|X|=n)$, удовлетворяе неравенству

$$\rho \ge (1-\delta) M(\log_r |F_A|, m, x) . \qquad (2.12)$$

Доказательство. Прологарифмируем неравенство (2.7), затем усредним обе части неравенства по всем $A \subseteq X, |A| = m$ поменяем в правой части порядок суммирования по A и по j и пр именим следствие леммы 2.5:

$$M(\log_r |F_A|, m, x) \le \sum_{j=1}^{\rho} M(\log_r |(h_j)_A|, m, x) \le \rho/(1-\delta) .$$

Лемма доказана.

Неравенство (2.12) дает нижнюю оценку ширины схемы. Чтобы уст новить более высокую НОСЛ схемы S для функции F, остается зам тить, что неравенство (2.12) справедливо для целого ряда ярусов сх мы S. Поэтому оценку (2.12) удается увеличить по порядку в $\log$ раз, где n – число существенных переменных функции F в множест X.

Комментарий. В качестве множества $\mathcal{F}$ покрываемых ч.б.ф. в оп санном доказательстве выступает множество функций вида $(h_j)_A$. Ши рина схемы S оценивается снизу числом ρ вершин одного яруса. Очевидно, эти вершины образуют независимое множество.

2.4. Метод Нечипорука

Метод, предложенный Э.И.Нечипоруком в [23], является одним из более известных и популярных методов доказательства НОСЛ. Он по воляет доказывать НОСЛ в классе булевых формул в произвольном ко нечном базисе. Метод применялся и в ряде других работ [13, 60, 76]. описан в монографиях [82] и [26]. Для успешного применения мето необходимо, чтобы оцениваемая функция имела много подфункций.

Опишем метод Нечипорука под интересующим нас углом зрения.

Теорема 2.6 [23]. Пусть множество переменных X функции $F(X,Y)$ бито на ρ подмножеств $X_1, \ldots, X_\rho$, а F_i есть число различ ных подфункций, получающихся из F при всевозможных подстановках нстант на места всех переменных, не принадлежащих X_i. Тогда в извольном конечном базисе

$$L_\Phi(F) \ge c \sum_{i=1}^{\rho} \log F_i \ . \qquad (2.13)$$

Замечание 1. Приведенная здесь формулировка по фо значительно отличается от оригинальной, поскольку в [23] она ормулирована для конкретной функции.

Замечание 2. Значение константы c зависит от ба са. Из доказательства можно понять, каким его следует выбрать.

Доказательство. Пусть $\mathcal{F}_i$ $(i = 1, \ldots, \rho)$ есть ожество подфункций, получающихся из $F(X,Y)$ при всевозможных под становках констант на места переменных, не входящих в X_i. Очевид , функции из $\mathcal{F}_i$ зависят только от переменных из X_i. Обозначим $= \mathcal{F}_1 \cup \ldots \cup \mathcal{F}_\rho$.

Пусть Φ есть произвольная формула, реализующая функцию F, D есть дерево этой формулы. Тем же символом D обозначим мно ество вершин дерева D.

Множество листьев дерева D, которым приписаны переменные из X_i, обозначим L_i. Пусть D_i есть множество тех вершин дерева D, у которых есть предки в множестве L_i. Вершины множества D_i образуют дерево, которое обозначим тем же символом D_i (см. ис.2.2, на котором ребра дерева D_i выделены жирными линиями).

Рассмотрим подмножество T тех вершин множества $D \setminus D_i$, ко рые подаются на входы вершин из D_i. Поскольку разнообразие ункций на выходе дерева D_i обеспечивается только за счет подмно ества T, то $|T| \ge \log F_i$.

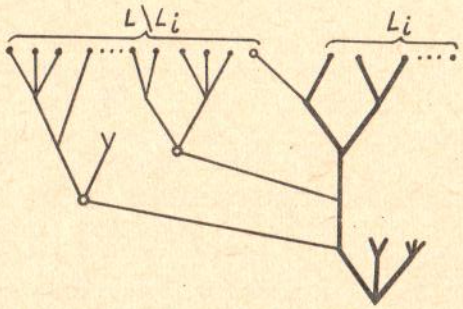

Рис.2.2. Фрагменты деревьев D и D_i

Комментарий. Очевидно, множество вершин T независимо. Тем мым мы оценили снизу ширину схемы. Эта оценка получена из необход мости покрыть подфункции из $\mathcal{F}_i$.

На втором этапе доказательства удается "умножить" оценку $\log$ на величину ρ, точнее, получить НОСЛ вида $c\sum_{i=1}^{\rho}\log F_i$. Это де лается следующим образом. Поскольку в поддерево D_i заходят не ме нее $\log F_i$ дуг из T и базис конечен, то поддерево D_i содержит не менее $c'\log F_i$ вершин. Отсюда можно вывести, что $|L_i| \geq c\log F_i$ что и приводит к требуемой оценке.

2.5. Метод Храпченко

В.М.Храпченко [48, 49] предложил метод доказательства НОСЛ в классе булевых формул в базисе $\{\wedge, \vee, {}^-\}$. В силу изоморфизма этих формул с П-схемами метод применим равным образом к П-схемам. Мето Храпченко позволяет установить НОСЛ величиной вплоть до n^2. Нар ду с методом Нечипорука метод Храпченко является одним из наиболе известных методов доказательств НОСЛ (см., например, [82, 26]).

Опишем метод Храпченко. Для произвольной булевой функции $f(x_1,\dots,x_n)$ обозначим $N_1=\{\tilde\sigma \mid f(\tilde\sigma)=1\}$, $N_0=\{\tilde\sigma \mid f(\tilde\sigma)=0\}$. Далее, пусть $R_f=\{(\tilde\sigma,\tilde\delta) \mid \tilde\sigma\in N_1, \tilde\delta\in N_0, \rho(\tilde\sigma,\tilde\delta)=1\}$.

Пару точек $(\tilde\sigma,\tilde\delta)$ будем называть ребром (j-го направле ния), если наборы $\tilde\sigma,\tilde\delta$ различаются только в одной координате (а именно, j-й).

Пусть S есть произвольная П-схема, реализующая функцию f. Обозначим $L = L(S)$. Перенумеруем контакты схемы S числами от до L.

Каждому набору $\tilde\sigma\in N_1$ сопоставим одну цепь $C(\tilde\sigma)$ в S, все ко нтакты которой замкнуты на наборе $\tilde\sigma$. Очевидно, эта цепь может со ржать лишь контакты $x_1^{\sigma_1},\dots,x_n^{\sigma_n}$. Каждому набору $\tilde\delta\in N_0$ сопос авим тупиковое сечение (опр. см. в п.2.I) $T(\tilde\delta)$, все контакты кото ого разомкнуты на наборе $\tilde\delta$. Это сечение может содержать лишь нтакты $x_1^{\delta_1},\dots,x_n^{\delta_n}$.

Комментарий. Если набор $\tilde\sigma$ инцидентен ρ ребрам из R_f, то ечение $T(\tilde\sigma)$ содержит не менее ρ контактов. Из леммы 2.I ясно, о множество контактов T независимо. Поэтому $W_\Pi(f)\geq\rho$. качестве множества $\mathcal{F}$ мы рассмотрим множество ч.б.ф., каждая из оторых совпадает с f на концах одного ребра из R_f, а в остальном произвольна.

Вторая часть доказательства состоит в том, чтобы "умножить"ши ину схемы S на длину цепи. Покажем, как это можно сделать.

Сопоставим ребру $(\tilde\sigma,\tilde\delta)\in R_f$ один контакт, который лежит на ересечении цепи $C(\tilde\sigma)$ и сечения $T(\tilde\delta)$. Если ребро $(\tilde\sigma,\tilde\delta)$ имеет j-е направление, то очевидно, это контакт x_j или $\bar x_j$. Обозначим имволом R_i множество ребер из R_f, которым сопоставлен контакт номером i $(1\leq i\leq L)$.

Утверждение 2.5. Все ребра множества R_i имеют одно направле ие, а именно, j-е, если i-й контакт есть контакт переменной x_j.

Обозначим символом r_i число ребер в R_i. Очевидно

$$\sum_{i=1}^{L} r_i = |R_f| \quad . \tag{2.I4}$$

Возведя (2.I4) в квадрат и применив неравенство Коши-Буняков кого, получим

$$|R_f|^2=(\Sigma r_i)^2=(\Sigma r_i\cdot 1)^2\leq \Sigma r_i^2\cdot\Sigma 1^2 = L\sum_{i=1}^{L} r_i^2 \tag{2.I5}$$

Оценим теперь сумму Σr_i^2. Для этого построим двудольный раф инциденций контакты - пары из $N_1\times N_0$. Одну долю вершин это о графа G составляют контакты схемы S. Их L штук. Другую до ю образует множество $N_1\times N_0$. i-й контакт соединим ребром с арой $(\tilde\sigma,\tilde\delta)\in N_1\times N_0$ тогда и только тогда, когда каждая из вер ин $\tilde\sigma,\tilde\delta$ инцидентна ребру из R_i.

Очевидно, i -й контакт соединен в графе G с r_i^2 вершинам второй доли. Поэтому граф G содержит $\sum_{i=1}^{L} r_i^2$ ребер.

С другой стороны, вершина $\tilde{\sigma}$ (соответственно, $\tilde{\delta}$) инцидентна ребру из R_i лишь в том случае, если цепь $C(\tilde{\sigma})$ (сечение $T(\tilde{\delta})$ содержит i -й контакт. Воспользуемся теперь следующим утверждением.

Лемма 2.7 [48]. В произвольной П-схеме каждая цепь с каждым тупиковым сечением имеет ровно один общий контакт.

Из нее следует, что каждая вершина из $N_1 \times N_0$ соединена в графе G не более, чем с одним контактом. Поэтому

$$\sum_{i=1}^{L} r_i^2 \le |N_0| \cdot |N_1| .$$

В соединении с (2.I5) это дает необходимую нижнюю оценку. Тем самым доказана

Теорема 2.7 [49]. Если $N_1 = \{\tilde{\sigma} \mid f(\tilde{\sigma}) = 1\}$, $N_0 = \{\tilde{\delta} \mid f(\tilde{\delta}) = 0\}$, $R_f = \{(\tilde{\sigma}, \tilde{\delta}) \mid \tilde{\sigma} \in N_1, \tilde{\delta} \in N_0, \rho(\tilde{\sigma}, \tilde{\delta}) = 1\}$, то

$$L_{\Pi}(f) \ge \frac{|R_f|^2}{|N_1| \cdot |N_0|} .$$

Метод Храпченко основан на применении этой теоремы.

2.6. Нижняя оценка в неполном базисе для функций из P_3

В этом параграфе рассматривается доказательство экспоненциальной НОСЛ не для булевой функции, а для некоторой функции трехзначной логики в подходящем неполном базисе. Эта оценка была установлена Г.А.Ткачевым [45].

Введем ряд дополнительных определений и обозначений. Пусть $E_k = \{0, 1, \dots, k-1\}$. Функции, определенные на декартовой степени E_k^n $(n = 1, 2, \dots)$ множества E_k и принимающие значения из E_k, называются функциями k -значной логики. Множество таких функций обозначается P_k.

Значение $a \in E_k$ называется форсирующим для функции $g \in P_k$, если функция g принимает значение a, как только хотя бы один из аргумент равен a.

Для функций $K(\ ,\ )$ и $D(\ ,\ )$, представленных таблицей 2.I, значение 2 является форсирующим.

Таблица 2.I

Функции $K(x,y)$ (слева) и $D(x,y)$ (справа)

	0	I	2
0	0	0	2
I	0	I	2
2	2	2	2

	0	I	2
0	0	2	2
I	2	2	2
2	2	2	2

Очевидно следующее

Утверждение 2.6. Если значение a является форсирующим для всех функций базиса B, то оно является форсирующим для произвольной функции, представимой в базисе B.

Функции $K(x,y)$ и $D(x,y)$, заданные таблицей 2.I, имеют некоторую аналогию соответственно с конъюнкцией и дизъюнкцией. Поэтому иногда мы будем их так называть.

Отметим простейшие свойства функций $K(x,y)$ и $D(x,y)$.

Утверждение 2.7. Функции $K(x,y)$ и $D(x,y)$ коммутативны и ассоциативны.

Свойство ассоциативности позволяет писать $H(x_1, \dots, x_n)$ вместо $H(\dots H(H(x_1, x_2), x_3), \dots, x_n)$. Поэтому будем считать определенными выражения $K(x_1, \dots, x_n)$ и $D(x_1, \dots, x_n)$.

В зависимости от приписанной операции внутренние вершины схемы в базисе $B = \{K, D\}$ делятся на K -вершины и D -вершины.

В силу утверждения 2.6 функции, представимые в базисе $B = \{K(x,y), D(x,y)\}$, достаточно определить на множестве $E_2^n = \{(\sigma_1, \dots, \sigma_n) \mid \sigma_i \in \{0, 1\}, \ i = 1, \dots, n\}$. Определим функцию $f(x_1, \dots, x_n)$ следующим образом:

$$f(x_1, \dots, x_n) = \begin{cases} 0, \text{ если } (x_1, \dots, x_n) \in E_2^n \text{ и } w(x_1, \dots, x_n) < \rho, \\ 2 \text{ в остальных случаях} \end{cases} \qquad (2.I6)$$

здесь ρ - некоторый параметр, $1 \le \rho \le n$, а $w(x_1, \dots, x_n) = x_1 + \dots + x_n$ - вес набора $(x_1, \dots, x_n)$).

Очевидно, функция f представима в виде

$$f(x_1, \dots, x_n) = D(K(x_1, \dots, x_\rho), \dots, K(x_{i_1}, \dots, x_{i_\rho}), \dots, K(x_{n-\rho+1}, \dots, x_n)) \qquad (2.I7)$$

(дизъюнкция всех конъюнкций ρ переменных).

Лемма 2.8 [45]. В произвольной схеме S в базисе $B = \{K, D\}$, реализующей функцию f (см. (2.I6)), для любого набора $\tilde{\sigma} \in E_2^n$ веса

ρ существует пара вершин u, v такая, что $v \in$ Сын (u) Функ$(u,\tilde{\sigma})$=I, Функ$(v,\tilde{\sigma})$=2 и вершина v является D-вершиной

Доказательство. Пусть v есть такая вершина схемы S, для которой Функ $(v,\tilde{\sigma})$ = 2, а предки вершины v этим свойством не обладают. Поскольку $f(\tilde{\sigma})$ = 2, такая вершина существует, а поскольку $\tilde{\sigma} \in E_2^n$, вершина v отлична от полюса. силу определения вершины v для всех ее предков u Функ $(u,\tilde{\sigma}) \in \{0,1\}$. Тогда из определения функций K и D следует, что ршина v может быть только D-вершиной. Отсюда же следует, по крайней мере для одного из родителей u вершины v Функ $(u,\tilde{\sigma})$ = I.

Вершину u, существование которой доказано в лемме 2.8, ставим в соответствие набору $\tilde{\sigma} \in E_2^n$ веса ρ.

Две различные вершины схемы называются несравнимыми, если одна из них не предшествует другой.

Лемма 2.9 [45]. Разным наборам $\tilde{\sigma}, \tilde{\delta} \in E_2^n$ веса ρ соответст несравнимые вершины схемы, реализующей функцию f.

Доказательство. Пусть вершина u схемы S ответствует набору $\tilde{\sigma} \in E_2^n$ веса ρ. Обозначим символом $I(u)$ мн ство индексов переменных, приписанных полюсам-предкам вершины u.

Для любого $i \in I(u)$ очевидно $\sigma_i = 1$. В противном случае Функ $(u,\tilde{\sigma})$ не может равняться I, как следует из определения функ K и D.

Далее, для любого $j \in I(u)$ $\sigma_j = 0$. В противном случае есть при σ_j = I), заменив σ_j на 0, мы получили бы набор $\tilde{\delta} \in E_2^n$ веса $\rho - 1$, на котором по определению $f(\tilde{\delta}) = 0$. В то же время, скольку вершина u не связана путем с x_j, то по-прежне Функ $(u,\tilde{\delta})$ = I и, следовательно, Функ $(v,\tilde{\delta})$ = 2. В таком случае силу утверждения 2.6 на выходе схемы тоже будет 2. Противореч

Итак, вершина u однозначно определяет набор $\tilde{\sigma}$. Следовательно, разным наборам $\tilde{\alpha}$ и $\tilde{\beta}$ из E_2^n веса ρ соответствуют разные вершины a и b. Предположим теперь, что вершина a предшествует вершине b. Если им предшествуют одни и те же полюсы, по доказанному $\tilde{\alpha} = \tilde{\beta}$. Поэтому множество $I(a)$ строго содержится в множестве $I(b)$. Но тогда $\tilde{\alpha} < \tilde{\beta}$, что противоречит тому, что $w(\tilde{\alpha}) = w(\tilde{\beta}) = \rho$.

Следствие. Ширина произвольной схемы в базисе $B = \{K, D\}$ для функции f из (2.I6) не менее C_n^ρ.

Теорема 2.8 [45]. Для функции $f(x_1, \ldots, x_n)$, определяемой монотоном (2.I6), справедлива нижняя оценка (в базисе $B = \{K, D\}$)

$$L(f) \geq 2C_n^\rho - 1 .$$

Доказательство. Чтобы соединить C_n^ρ несравмых вершин с выходом схемы, требуется не менее $C_n^\rho - 1$ вершин.

Комментарий. В качестве множества $\mathcal{F}$ ч.ф., покрываемых в ом доказательстве, здесь можно взять множество функций $\varphi_{\tilde{\sigma}}$ вида

$$\varphi_{\tilde{\sigma}}(\tilde{x}) = \begin{cases} 2, \text{ если } \tilde{x} = \tilde{\sigma}, \\ 0, \text{ если } w(x_1, \ldots, x_n) < \rho, \\ \text{не определена в остальных случаях,} \end{cases}$$

е $\tilde{\sigma}$ пробегает все точки из E_2^n веса ρ. Ширина схемы оценивается в следствии леммы 2.9.

2.7. Нижние оценки в монотонном базисе

Рассмотрим теперь нижние оценки сложности в условиях неполноты базиса в булевском случае, то есть при $k = 2$. Среди таких базисов наибольший интерес представляет монотонный базис $\{\wedge, \vee\}$. Значительные усилия были направлены на доказательство НОСЛ в этом базисе. десь следует отметить работы Э.И.Нечипорука [24], В.Пратта [79], Патерсона [75], К.Мельхорна и Ц.Галила [72], Э.Ламаньи и Дж.Сэ джа [70], К.Мельхорна [7I], Н.Пипенджера [78], В.Пауля [77], Ю.Григорьева [6], И.Вегенера [92-94] и Е.А.Окольнишниковой [35]. жняя оценка во всех этих работах получена не для отдельной булевой функции (в этом случае не удавалось получать сколько-нибудь сокие НОСЛ), а для систем булевых функций. Из числа перечисленных работ в [35] получена самая высокая нижняя оценка (величины n^2). Этот порог n^2 казался уже непреодолимым, когда к неожиданности для многих специалистов А.Е.Андреев [I] и А.А.Разборов [38] оказали существенно более высокие НОСЛ (почти экспоненциальная в] и $n^{c \log n}$ в [38]). В [I, 38] развиты принципиально новые методы, которые еще подлежат осмыслению. Мы не будем их здесь затрагивать. Из остальных работ, по-видимому, наибольшую известность олучили оценки И.Вегенера [92, 94], одну из которых мы и рассмотрим в качестве представителя большой группы доказательств.

В [92] получена почти квадратичная нижняя оценка. Она устанавливается для системы f_{MN}^m булевых функций $y_{h_1 \ldots h_m}$ ($1 \leq h_1, \ldots, h_m \leq M$), содержащей M^m функций. Аргументами этих

функций служат булевы переменные $x^i_{h_i \ell}$, где $1 \le i \le m$, $1 \le \ell \le N$. Эти переменные удобно интерпретировать как элементы m матриц, имеющих по M строк (h_i обозначает номер строки, $1 \le h_i \le M$) и N столбцов. Итого, получается mMN входных переменных. Каждая выходная переменная определяется следующим образом:

$$y_{h_1 \dots h_m} = \bigvee_{1 \le \ell \le N} x^1_{h_1 \ell} x^2_{h_2 \ell} \dots x^m_{h_m \ell} .$$

Это можно интерпретировать следующим образом: из каждой из m матриц выбирается по одной строке (h_1-я из первой, ..., h_m-я из m-й) и проверяется, имеют ли все выбранные строки общую единичную компоненту. Если это так, то выходная переменная $y_{h_1 \dots h_m}$ полагается равной I, в противном случае равной 0. При $m = 2$ получается обычное булево произведение матрицы $(x^1_{h_1 \ell})$ и матрицы, транспортированной к матрице $(x^2_{h_2 \ell})$.

Отметим некоторые технические приемы, использованные при доказательстве. Во-первых, рассматривается новая мера сложности $L^\wedge$, при которой в схеме подсчитываются лишь элементы конъюнкции. Очевидно, $L \ge L^\wedge$. Во-вторых, на входы схемы разрешается подавать не только переменные, но и конъюнкции переменных, если они содержат менее m переменных. Сложность таких схем обозначается L^*. Очевидно $L \ge L^\wedge \ge L^{*\wedge}$. В работе оценивается величина $L^{*\wedge}$.

Для каждого набора $(h_1 \dots h_m) \in \{1, \dots, M\}^m$ обозначим символом $Q_{h_1 \dots h_m}$ множество всех монотонных функций, имеющих конъюнкцию $x^1_{h_1 N} \dots x^m_{h_m N}$ своим простым импликантом. В схеме S, реализующей систему f^m_{MN}, каждому простому импликанту $I(h_1, \dots, h_m) = x^1_{h_1 N} \dots x^m_{h_m N}$ сопоставляется вершина G схемы S, в которой "впервые" вычисляется этот простой импликант. Точнее, это означает следующее: конъюнкция $I(h_1, \dots, h_m)$ является простым импликантом функции, вычисляемой схемой S в вершине G, а родители вершины G этим свойством не обладают. Поскольку функции входных вершин схемы S принадлежат множеству $Q_{h_1 \dots h_m}$, а выходные функции $y_{h_1 \dots h_m}$ принадлежат множеству $Q_{h_1 \dots h_m}$, то вершина G существует, причем является $\wedge$-вершиной. Основная лемма работы [92] утверждает существование минимальной в смысле меры $L^{*\wedge}$ схемы S, реализующей систему f^m_{MN}, в которой вершины G, соответствующие разным простым импликантам $I(h_1 \dots h_m)$ и $I(h'_1 \dots h'_m)$, различны. При этом

существенно используется то обстоятельство, что в схеме M^m выходов, то есть имеется тупиковое сечение из M^m вершин.

На следующем шаге доказательства переменные $x^i_{h_i N}$ заменяются константами так, что выполняются следующие два условия:

(а) $2M^m/m$ элементов G, выявленных на предыдущем шаге, исключаются из схемы, поскольку хотя бы на один вход каждого из них поступает константа;

(б) полученная схема реализует систему $f^m_{M,N-1}$, то есть по-прежнему ширина сечения функции не менее M^m.

Это позволяет доказать следующее утверждение:

Теорема 2.9 [92]. Для любого натурального $m \ge 2$ имеет место следующая нижняя оценка в базисе $\{\wedge, \vee\}$

$$L(f^m_{MN}) \ge N] 2M^m/m [.$$

При подходящих значениях параметров ($m = [\log n]$, $M = 2$, $N = [n/(2 \log n)]$) это дает по порядку нижнюю оценку $n^2/\log^2 n$, где через n обозначено число входных переменных.

З а м е ч а н и е . При подстановках констант на последнем шаге доказательства удалось удалить из схемы лишь $2M^m/m$ элементов из числа выявленных M^m. Создается впечатление, что на этом шаге доказательство "не дожимает" оценку. Работа И.Вегенера [94] подтвердила это. В ней он развил новую технику доказательства, которая позволила поднять НОСЛ системы f^m_{MN} до $n^2/\log n$ (по порядку).

Комментарий. Оценка ширины схемы в этом доказательстве тривиальная – по числу входов, а оценка ширины сечения – по числу выходов. В качестве множества $\mathcal{F}$ покрываемых функций выступает множество функций $y_{h_1 \dots h_m}$. Каждая из этих функций имеет сложность не более N в смысле меры $L^{*\wedge}$.

2.8. Нижние оценки сложности монотонного вычисления полиномов

Монотонная схема для вычисления полиномов строится в базисе $[\times, +]$. Такая схема является более общим объектом, нежели булева схема, поскольку использует не обязательно булевы операции, а операции из произвольного кольца. Задача доказательства НОСЛ для таких схем имеет много общего с булевским случаем. Исторически имен-

но для задачи монотонного вычисления полиномов была раньше другим установлена экспоненциальная НОСЛ. Это сделано в работе К.Шнорра [85].

Для подтверждения гипотезы о том, что с доказательством НОСЛ можно связать задачу на покрытие и на оценку ширины, следует рассмотреть и доказательство из [85]. Тому есть по крайней мере две причины. Во-первых, работа К.Шнорра получила широкую известность, вызвала к жизни ряд других работ [90, 68]. Во-вторых, доказательство НОСЛ, представленное в [85], по форме сильно отличается от доказательств НОСЛ в задаче на покрытие. Поэтому для подтверждения справедливости нашей трактовки доказательств НОСЛ следует переделать доказательство из [85], представив его как доказательство в некоторой задаче на покрытие. Это и проделывается в данном параграфе.

2.8.1. Монотонные схемы для вычисления полиномов

Мы будем рассматривать полиномы с вещественными коэффициентами над переменными $X=\{x_1,\dots,x_n\}$, хотя результаты работы сохраняют силу и для полиномов с коэффициентами из произвольного кольца без делителей нуля. Каждый м о н о м полинома – это терм вида $x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$, где все i_j суть неотрицательные целые числа (переменные предполагаются коммутирующими). Множество мономов полинома p будем обозначать $mon(p)$. Тогда п о л и н о м p можно представить как

$$p=\sum_{m_j\in mon(p)}\alpha_j m_j,$$

где $\alpha_j\in R$ (R – кольцо вещественных чисел).

Полиномы p_1 и p_2 называются э к в и в а л е н т н ы м и (обозначение $p_1\sim p_2$), если равны их множества мономов. В этой работе мы не различаем эквивалентные полиномы. Поэтому полином вполне определяется множеством своих мономов. Полином p_1 называется п о д полиномом полинома p, если $mon(p_1)\subseteq mon(p)$.

Множество положительных вещественных чисел обозначим R^+.

Мы будем вычислять полином с помощью схем в монотонном базисе $\{+,\times\}$. Полюсам схемы приписаны либо переменные, либо константы из R^+. Очевидно, такими схемами (они называются м о н о т о н н ы м и) можно вычислять лишь полиномы с положительными коэффициентами.

Мы будем рассматривать лишь такие схемы, в которых каждая вершина соединена некоторым путем с выходной вершиной t.

В соответствии с приписанной операцией различают $+$ -вершины и $\times$-вершины. Число $+$ -вершин в схеме S обозначается $L_+(S)$.

Каждой вершине a схемы естественным образом приписывается полином $pol(a)$, про который говорят, что он вычисляется в этой вершине. Для входных вершин этот полином совпадает с переменной или константой, помечающей вершину. Если вершина c является сыном вершин a и b, то по определению полином $pol(c)$ вершины c эквивалентен полиному, полученному из $pol(a)\circ pol(b)$, где $\circ$ обозначает операцию, приписанную вершине c. Полином, вычисляемый в выходной вершине, называется п о л и н о м о м с х е м ы.

Сложностью вычисления полинома p (обозначение $L(p)$) называется минимальная сложность схемы, вычисляющей полином p. $L_+(p)$ обозначает минимальное число $+$ -вершин в схеме, вычисляющей полином p.

В заключение этого параграфа сформулируем два простых свойства монотонных схем.

Утверждение 2.8. Пусть v – произвольная вершина монотонной схемы. Тогда полином этой схемы представим в виде $pol(v)\times P+Q$, где P и Q – некоторые полиномы, из которых Q может быть пустым.

Это очевидное свойство монотонных схем служит основой для получения нижних оценок сложности.

Утверждение 2.9. В минимальной монотонной схеме полиномы, вычисляемые в разных вершинах, не эквивалентны.

Д о к а з а т е л ь с т в о. Предположим, что для разных вершин u и v $pol(u)\sim pol(v)$. "Перекинув" начала дуг, выходящих из вершины v, в вершину u и удалив вершину v, получим в силу утверждения 2.8 эквивалентную схему, что противоречит минимальности исходной схемы. □

Схема называется п р и в е д е н н о й, если полином, вычисляемый в $+$ -вершине, содержит не менее двух различных мономов. Очевидно, для каждой схемы существует эквивалентная приведенная схема не большей сложности. В силу утверждения 2.9 минимальная схема является приведенной.

2.8.2. Порождающая подсхема монома

Понятие порождающей подсхемы позволяет проследить историю ф мирования монома. Близкое понятие введено в [68].

Пусть схема (S,t) вычисляет в выходной вершине t полином Сопоставим каждому моному $m \in mon(P)$ некоторую схему, которую б дем называть п о р о ж д а ю щ е й п о д с х е м о й моном m в схеме (S,t). Для построения порождающей подсхемы применим рекурсивную процедуру.

Если схема S не содержит + -вершин, то порождающая подсх монома m в схеме S совпадает по определению со схемой S .

Пусть теперь (S,t) есть произвольная схема, включающая + -ве шины. Обозначим символами u и v родителей выходной вершины t Можно считать, что в схемах (S,u) и (S,v) мономам уже сопоставлен порождающие подсхемы. При необходимости (в частности, при $u=v$ продублируем вершины схемы S так, чтобы схемы (S,u) и (S,v) не имели общих вершин. Каждая вершина схем (S,u) и (S,v) отображает естественным образом в одноименную вершину схемы S . Это отобр жение индуцирует отображение вершин порождающей подсхемы в множе во вершин схемы S , что и дает основание применять термин "под схема".

Если t есть + -вершина, то очевидно моном m принадлеж полиному по крайней мере одной из вершин u и v . Обозначим э вершину w . Если на роль вершины w годится каждая из вершин u,v , то положим для определенности $w=u$. Присоединив к п рождающей подсхеме монома m в схеме (S,w) дугу (w,t) , получи порождающую подсхему монома m в схеме (S,t).

Если t есть X-вершина, то очевидно, полиномы $pol(u)$ и $pol(v)$ содержат некоторые мономы m_u и m_v такие, что $m = m_u m_v$. Соединив порождающие подсхемы мономов m_u и m_v д гами (u,t) и (v,t) с вершиной t , получим порождающую подсхему монома m в схеме (S,t).

З а м е ч а н и е I . Поскольку представление $m = m_u m$ вообще говоря, не однозначно, то и порождающая подсхема монома с ится, вообще говоря, не однозначно. Другим источником неоднознач сти является то, что один и тот же моном может входить в оба пол нома $pol(u)$ и $pol(v)$.

З а м е ч а н и е 2 . Порождающая подсхема является схе

бычном смысле, если в ней операцию + рассматривать как одно - тную операцию сложения с нулем.

Отметим некоторые очевидные свойства порождающих подсхем.

Утверждение 2.10. В порождающей подсхеме в любую X-вершину ходят две дуги, а в + -вершину одна дуга.

Утверждение 2.11. Порождающая подсхема монома m вычисляет омономный полином, эквивалентный m .

Лемма 2.10. Порождающая подсхема монома m в приведенной схе- S совпадает со схемой S в том и только в том случае, когда ема S вычисляет одномономный полином.

Д о к а з а т е л ь с т в о . В силу приведенности такая схе- S не содержит + -вершин и поэтому порождающая подсхема моно- m совпадает по определению с S . Если схема S содержит -вершины, то порождающая подсхема отлична от схемы S в силу тверждения 2.10. □

Вершина приведенной схемы S называется о б р а з у ю - й , если в ней вычисляется одномономный полином, а хотя бы ин из ее сыновей не обладает этим свойством. Очевидно, образующая ршина является либо полюсом, либо X-вершиной. Далее, хотя бы ин из ее сыновей либо является + -вершиной, либо имеет среди редков + -вершину. Прообраз образующей вершины в порождающей одсхеме тоже будем называть образующей вершиной. Если из образую - й вершины ведет дуга в некоторую + -вершину, назовем такую дугу а л ь т е р н а т и в н о й .

Лемма 2.11. Если полином P приведенной схемы S содержит олее одного монома, то порождающая подсхема каждого монома $m \in mon(P)$ в схеме S содержит некоторую альтернативную дугу.

Д о к а з а т е л ь с т в о . Если бы порождающая подсхема S' монома m схемы S содержала только X-вершины, то она овпадала бы со схемой S . В силу леммы 2.10 схема S вычисляла бы в этом случае одномономный полином, что противоречит условию. По- тому в порождающей подсхеме S' есть + -вершины. Отыщем в ней акую + -вершину w , среди предков которой в подсхеме S' нет + -вершины. Очевидно, один из родителей вершины w принадлежит одсхеме S' и является образующей вершиной. □

2.8.3. Вычисление одномерных полиномов

Рассмотрим выражение вида

$$(m_{11}+\ldots+m_{1\rho_1})(m_{21}+\ldots+m_{2\rho_2})\ldots(m_{r1}+\ldots+m_{r\rho_r})m_{r+1}\ , \quad (2.18$$

где m_{r+1} и m_{ij} суть мономы $(1\le i\le r,\ 1\le j\le\rho_i)$, $\rho_i\ge 2$ для всех i и все мономы в пределах одной скобки различны. Множество всевозможных мономов, которые получаются при раскрытии всех скобок в (2.18), называется r – м е р н ы м и н т е р в а л о м. Это понятие введено в [15]. Будем говорить, что полином содержит r –мерный интервал, если некоторое подмножество мономов этого полинома образует r –мерный интервал. Очевидно, что при $r\ge 2$ он содержит в этом случае и $(r-1)$ –мерные интервалы. В силу утверждения 2.8 очевидно

Утверждение 2.12. Если полином некоторой вершины схемы содержит r –мерный интервал, то тем же свойством обладают все потомки этой вершины.

Полином называется о д н о м е р н ы м , если он не содержит двумерных интервалов. Идея использовать отсутствие двумерных интервалов для доказательства нижних оценок сложности восходит к работе [24] Э.И.Нечипорука.

Схемы, вычисляющие одномерные полиномы, обладают рядом специфических свойств, что устанавливается ниже в леммах 2.12 – 2.15.

Лемма 2.12. В приведенной схеме, вычисляющей одномерный полином, не существует двух различных путей, соединяющих + –вершину с X –вершиной.

Д о к а з а т е л ь с т в о . В силу приведенности схемы утверждения 2.12 такая схема вычисляла бы неодномерный полином. □

Лемма 2.13. Если приведенная схема вычисляет одномерный полином ρ , то порождающая подсхема каждого монома полинома ρ содержит не более одной альтернативной дуги.

Д о к а з а т е л ь с т в о . В силу утверждения 2.10 пути, начинающиеся с двух разных альтернативных дуг, могут встретиться лишь в X –вершине, но это противоречит лемме 2.12. □

Разобьем вершины схемы на ярусы, отнеся к h –му ярусу все те вершины a , для которых длина самого длинного пути, ведущего из a в выходную вершину, равна h .

Сформулируем еще одно специфическое свойство схем, вычисляющих одномерные полиномы.

Лемма 2.14. В минимальной схеме, вычисляющей одномерный полином, никакая + –вершина не может соединяться с выходом двумя различными путями.

Д о к а з а т е л ь с т в о индукцией по номерам ярусов + –вершин. В силу утверждения 2.9 и леммы 2.12 для + –вершин 0 яруса лемма верна.

Продолжая по индукции, рассмотрим произвольную + –вершину h – яруса. Предположим, что она соединяется с выходом двумя различными путями. Пусть эти пути впервые "расходятся" в вершине a и после этого впервые "встречаются" в вершине d . Обозначим отрезки этих путей между вершинами a и d (исключая вершину d) соответственно C_1 и C_2 . Заметим, что в силу приведенности схемы полином вершины a содержит не менее двух мономов. Далее, в силу леммы 2.12 вершина d может быть только + –вершиной.

Обозначим символами d_1 и d_2 соответственно последние вершины путей C_1 и C_2 , то есть вершины, непосредственно предшествующие вершине d . $d_1\ne d_2$, так как в противном случае обе они совпали бы с вершиной a , и мы имели бы $pol(a)\sim pol(d)$, что противоречит минимальности схемы. Полиномы, вычисляемые в вершинах d_1 и d_2 , можно представить в виде

$$pol(d_1)\sim pol(a)\cdot m_1+\rho_1\ ,\quad pol(d_2)\sim pol(a)\cdot m_2+\rho_2\ , \quad (2.19)$$

где m_1 и m_2 – некоторые мономы (возможно, пустые), а ρ_1 и ρ_2 – некоторые полиномы (тоже, возможно, пустые).

Мономы m_1 и m_2 в (2.19) не могут быть различными, так как в противном случае подполином $(m_1+m_2)pol(a)$, вычисляемый в вершине d , был бы двумерным, что ввиду утверждения 2.12 противоречит условию леммы.

Итак, $m_1=m_2$. Если при этом пути C_1 и C_2 не содержат + –вершин, отличных от a , то в (2.19) $\rho_1=\rho_2=\emptyset$ и, следовательно, $pol(d_1)\sim pol(d_2)$, что ввиду утверждения 2.9 противоречит минимальности схемы S .

Пусть теперь $m_1=m_2=m$ и хотя бы один из путей C_1 и C_2 (для определенности, C_1) содержит + –вершины, отличные от a . Пусть b есть первая такая вершина на пути C_1 . По предположению индукции + –вершина b соединена с выходом единственным путем (который пролегает через вершину d). Пусть дуги (v,b) и (b,w) принадлежат пути C_1 , а u – второй родитель вершины b . Тогда полиномы вершин d_1 и d представимы в виде

$pol(d_1) \sim (m' pol(a) + pol(u))\, m'' + R$,

где $m' \cdot m'' = m$, а R некоторый полином (возможно, пустой),

$pol(d) \sim pol(d_1) + pol(a) \cdot m + P_2 \sim pol(u) \cdot m'' + R + pol(a) \cdot m +$

Произведем эквивалентное преобразование схемы S : уберем ги (v,b) и (u,b) и добавим дугу (u,w). Тогда

$pol(d) \sim pol(u) \cdot m'' + R + pol(a) \cdot m + P_2$,

то есть эквивалентен исходному. Поскольку по предположению индук вершины пути $(b \Rightarrow d)$ соединены с выходом только через вершину a то полученная схема эквивалентна исходной. В то же время она сод жит меньше вершин, что противоречит минимальности схемы S .

Сформулируем, наконец, заключительное свойство схем, вычисл щих одномерные полиномы.

Лемма 2.I5. В минимальной схеме, вычисляющей одномерный пол ном, каждая альтернативная дуга может принадлежать порождающей п схеме лишь одного монома.

Доказательство. Предположим, что порождающи подсхемы S_1 и S_2 мономов соответственно m_1 и m_2 содержат щую альтернативную дугу (a,b). В силу леммы 2.I4 эта дуга прина лежит только одному пути, ведущему в выходную вершину. Следовате но, этот путь принадлежит обеим подсхемам S_1 и S_2 . В силу лем 2.I3 и индуктивного построения порождающих подсхем $S_1 = S_2$ и, сл довательно, $m_1 = m_2$ (в силу утверждения 2.II).

Теперь мы можем доказать в терминах покрытий теорему, очень близкую к теореме Шнорра [85].

Теорема 2.I0. Для произвольного одномерного полинома

$$L_+(P) \geq |mon(P)| - 1 \quad .$$

Доказательство. Рассмотрим минимальную (по слу сложений) схему S , вычисляющую полином P . При $|mon(P)| =$ теорема очевидна. Поэтому в дальнейшем $|mon(P)| \geq 2$. Каждому моно из P сопоставим некоторую альтернативную дугу (лемма 2.II). В лу леммы 2.I5 эти дуги для разных мономов различны. Поэтому в сх S не менее $|mon(P)|$ альтернативных дуг.

Если путь C , начинающийся с альтернативной дуги, впервы встречается с некоторым другим путем схемы S в некоторой $\times$ шине v , то этот второй путь удалим, в том числе "снимем" верш v с пути C . В силу одномерности полинома схемы эта операци не удаляет альтернативные дуги. Проделав достаточное число раз т

преобразование, придем к схеме S' , в которой X-вершины мо- лишь предшествовать + -вершинам. Чтобы собрать $|mon(P)|$ путей й схемы, начинающихся с альтернативных дуг, требуется не менее $|mon(P)|$ -I операций сложения. □

Комментарий. Из определения образующей вершины следует, что тернативные дуги образуют реберно независимое множество. Поэтому лу лемм 2.II и 2.I5 реберная ширина одномерного полинома P менее $|mon(P)|$. Роль покрываемых подфункций здесь играют мономы.

2.9. Нижние оценки для схем без нулевых цепей

Понятие контактных схем без нулевых цепей введено А.К.Пулато - [37] и распространено на схемы из функциональных элементов .Кузнецовым [I5]. Для частного случая контактных схем, а именно раллельно-последовательных схем (П-схем) без нулевых цепей в [37] тановлены экспоненциальные или близкие к ним НОСЛ. Для контактных м и схем из функциональных элементов без нулевых цепей аналогич- оценки получены в [I5, I6]. В качестве представителя этой груп- доказательств мы рассмотрим доказательство из [37] и покажем, что по существу сводится к оценке ширины схемы.

Понятия П-схемы, цепи и тупикового сечения были описаны в п.I.3 .I.

Цепь П-схемы называется нулевой, если она имеет тождественно левую проводимость, то есть содержит одновременно контакты вида x и $\bar{x}$. П-схема без нулевых цепей согласно определению не со- ржит нулевых цепей. Сложность функции f в классе П-схем без ну- вых цепей обозначается $L^*_{\Pi}(f)$. Очевидно, каждая булева функция, оме константы 0, может быть реализована П-схемой без нулевых це - й. Ее можно построить, например, в соответствии с ДНФ функции f.

Лемма 2.I6 [37]. Пусть f - произвольная булева функция такая, о из $\tilde{\alpha}, \tilde{\beta} \in N_f$ следует, что $\rho(\tilde{\alpha}, \tilde{\beta}) \geq 2$. Тогда каждая цепь мини- льной П-схемы S без нулевых цепей, реализующей функцию f , со- ржит ровно по одному контакту каждой переменной.

Доказательство. Очевидно, множество контактов T любой переменной x схемы S образует сечение (иначе функ - f обращалась бы в единицу на паре соседних наборов). Пусть $T' \subseteq T$ есть тупиковое сечение схемы S . Если некоторый контакт $c \in T \setminus T'$, то любая цепь схемы S , проходящая через этот контакт,

содержит другой контакт этой же переменной $x^{\delta} \in T'$. Поскольку
схеме нет нулевых цепей, то $\delta = \bar{\delta}$. Поэтому "закоротив" контак
x^{δ} (то есть стянув его концы в одну точку), получим эквивалент
ную схему меньшей сложности, что противоречит минимальности схем
S. Следовательно, сечение T тупиковое. В силу леммы 2.7 ка
дая цепь схемы S содержит ровно один контакт из множества T

Пусть a_0 и b_0 – две произвольные вершины, лежащие на одн
цепи П-схемы S. П-схема S_0 с полюсами a_0 и b_0 называетс
подсхемой схемы S, если каждая ее цепь является подцепью нек
торой цепи S.

Следствие. Пусть множество переменных подсхемы
схемы из леммы 2.I6 есть Y. Тогда каждая цепь подсхемы S_0 с
держит ровно по одному контакту из Y.

Определим теперь функцию, для которой будет установлена ни
няя оценка сложности. Подмножество $C_d \subseteq B^n (2 \le d \le n)$ называе
(n, d)-кодом, если для любой пары точек $\tilde{\alpha}, \tilde{\beta} \in C_d$
$\rho(\tilde{\alpha}, \tilde{\beta}) \ge d$. Характеристической функцией множества $A \subseteq B^n$
зывается функция $f \in P_2^n$ такая, что $N_f = A$. Характеристическую
функцию (n, d)-кода обозначим $C_d(x_1, \ldots, x_n)$.

Циклом контактной схемы будем называть цикл без самопересече
ний графа этой схемы.

Лемма 2.I7 [37]. Минимальная П-схема S без нулевых цепей,
реализующая функцию $C_d(x_1, \ldots, x_n)$, не содержит циклов длины, ме
ньшей $2d$.

Доказательство. Предположим обратное. Пусть
минимальный цикл B схемы S имеет длину менее $2d$. Обозначи
S_B минимальную подсхему схемы S, содержащую цикл B. В с
минимальности подсхемы S_B ее полюсы принадлежат циклу B. Пу
подсхема S_B содержит контакты k переменных. Тогда в силу следс
вия леммы 2.I6 длина цикла равна $2k$, что по предположению мень
$2d$. Итак, $k < d$.

Рассмотрим две произвольные различные цепи схемы S, прох
дящие через S_B и совпадающие вне S_B. Поскольку расстояние меж
различными точками из C_d не менее d и $k < d$, то эти две цеп
состоят из одних и тех же контактов. Поэтому подсхему S_B можно
заменить одной из ее цепей, сохранив функцию схемы. Но это проти
речит минимальности схемы S. □

Будем говорить, что множество циклов П-схемы образует цепочку циклов, если все полюсы минимальных подсхем, со-

держащих эти циклы, лежат последовательно на одной цепи схемы S.
Число этих циклов называется длиной цепочки циклов. Очевидно, циклы одной цепочки не имеют общих контактов.

Следствие. Для схемы S из леммы 2.I7 максимальная длина цепочки циклов не превышает $[n/d]$.

Оценим теперь сверху число цепей схемы S. Для этого рассмотрим сначала преобразование φ схем, не меняющее числа цепей и длин цепочек циклов. Оно применяется к схемам с двумя и более контактами и состоит в следующем: если все цепи схемы S, проходящие через оба конца контакта, проходят через контакт (то есть если к контакту не присоединена параллельно подсхема), то концы этого контакта стягиваются в одну точку. При этом, если один из концов был полюсом схемы, то новая вершина становится полюсом.

Схема S' называется неприводимой, если к ней неприменимо преобразование φ.

Лемма 2.I8 [37]. В неприводимой схеме S' с двумя и более контактами все контакты самой длинной цепи принадлежат циклам длины 2.

Доказательство. Пусть C – произвольная самая длинная цепь неприводимой схемы S'. Если некоторый контакт этой цепи не принадлежит никакому циклу, то к нему применимо преобразование φ, что противоречит неприводимости S'. Пусть теперь контакт x цепи C принадлежит циклу длины более 2. Если все остальные контакты этого цикла не принадлежат цепи C, то это противоречит максимальности цепи C. В противном случае к контакту x применимо преобразование φ. □

Следствие. Если S' неприводимая схема, полученная из схемы S леммы 2.I7, то длины цепей в S' не превышают $[n/d]$.

Его справедливость немедленно следует из определения преобразования φ, леммы 2.I8 и следствия леммы 2.I7.

Граф П-схемы называется П-сетью.

Подразбиение ребра заключается в добавлении новой вершины на середину ребра. Два графа называются гомеоморфными, если их можно получить из одного графа последовательными подразбиениями ребер.

Лемма 2.I9. Для каждой П-сети S с максимальной длиной цепи h существует гомеоморфная П-сеть, у которой все цепи имеют длину h

Доказательство индукцией по числу m ребер П-сети S. При $m=1$ утверждение очевидно. При произвольном m П-сеть S является в соответствии с индуктивным определением либо параллельным, либо последовательным соединением двух П-сетей S_1 и S_2. В силу предположения индукции S_1 и S_2 удовлетворяют утверждению леммы. Поэтому их последовательное соединение тоже удовлетворяет утверждению леммы. В случае параллельного соединения, если одна из сетей S_1, S_2 (для определенности S_1) имеет максимальную длину цепи $q < h$, то применим $h-q$ раз операцию подразбиения ребра ко всем ребрам, инцидентным одному из полюсов сети S_1. □

Преобразуем теперь неприводимую схему S' из следствия лем мы 2.18 в гомеоморфную П-сеть S'', у которой все цепи имеют длин $h=[n/d]$. Доказательство леммы 2.19 показывает, как это мож но сделать.

Разобьем теперь ребра П-сети S'' на ярусы. Пусть полюсами се ти S'' являются вершины a и b. Первый ярус образует ребра, ин цидентные вершине a. i-й ярус составляют ребра, смежные с реб рами $(i-1)$-го яруса и не принадлежащие ярусам с номерами меньше Очевидно, получится h ярусов. Ясно также, что ребра одного яруса образуют тупиковое сечение П-сети S''. Пусть M есть максимальное число ребер в одном ярусе П-сети S''. Ясно, что M является нижне оценкой ширины П-сети S''.

Каждая цепь сети S'' содержит ровно по одному ребру из каждо го яруса. Поэтому число $C(S'')$ цепей сети S'' удовлетворяет неравен ству

$$C(S'') \le M^h . \qquad (2.20)$$

Пусть теперь f есть характеристическая функция произвольно (n,d)-кода, а $W_n(f)$ есть ширина функции f в классе П-схем. Пусть S есть минимальная П-схема, реализующая функцию f. Сог ласно определению ширины $W_n(f) \ge W_n(S)$.

Из определения сетей S' и S'' легко видеть, что

$$W_n(S'') = W_n(S') = W_n(S), \quad C(S'') = C(S') = C(S). \qquad (2.21)$$

Лемма 2.20. Ширина характеристической функции f произволь ного (n,d)-кода удовлетворяет неравенству

$$W_n(f) \ge |N_f|^{d/n} .$$

Доказательство. Каждая цепь П-схемы S замк нута ровно на одном наборе из N_f. Поэтому $C(S) \ge |N_f|$. Оста этой воспользоваться соотношениями (2.20) и (2.21) и условием $h = [n/d]$. □

Теорема 2.II [37]. Для характеристической функции f произ вольного (n,d)-кода

$$L_n^*(f) \ge d\,|N_f|^{d/n} .$$

Доказательство вытекает из леммы 2.20, если учесть, что каждый контакт схемы S' получен стягиванием не менее d контактов схемы S.

Комментарий. Мы видим, что доказательство НОСЛ для функции f свелось в основном к оценке ее ширины. Роль покрываемых ч.б.ф. иг рают функции, каждая из которых равна I в одной точке множества N_f и равна 0 там, где функция f равна 0.

2.I0. Нижние оценки при ограничении на глубину

В этом параграфе мы рассматриваем схемы с ограничением на глу бину. Они впервые изучались О.Б.Лупановым [I7, 2I], который устано вил, что при глубине не менее 3 это ограничение асимптотически не влияет на сложность реализации "почти всех" булевых функций. С дру гой стороны, для схем с ограничением на глубину не доказана их по линомиальная эквивалентность обычным схемам, что дает шансы на до казательство высоких НОСЛ для этих схем. Такие оценки действительно установлены. Впервые это сделал Г.А.Ткачев [46], который доказал почти экспоненциальные НОСЛ для схем глубины 3. Затем аналогичные результаты установили Л.Вэлиант [9I], М.Клэйв, В.Пауль, Н.Пиппенджер и М.Янакакис [69], А.Яо [97] и другие. Эти результаты говорят о том, что схемы с ограничением на глубину действительно не полиномиально эквивалентны обычным схемам.

В упомянутых работах схемы с ограничением на глубину определя ются с небольшими различиями, но по существу эти определения экви валентны. Мы используем здесь простейший вариант определения. Сог ласно этому определению рассматриваются схемы в базисе $\{\wedge, \vee\}$, по люсам которых могут быть приписаны переменные и их отрицания. Ясно, что такими схемами можно реализовать произвольную булеву функцию.

Разобьем теперь внутренние вершины схемы на слои. Пусть для определенности выходная вершина t схемы есть $\vee$-вершина. Тогда

I-й слой схемы по определению состоит из вершины t и всех $\vee$-вершин v схемы, удовлетворяющих следующему условию: любой путь ($v \Rightarrow t$) не содержит $\wedge$-вершин (то есть содержит только $\vee$-вершины). Пусть определены слои I-й, ..., (i-I)-й и пусть для определенности слой i-I состоит из $\vee$-вершин, то есть является $\vee$-слоем. Тогда i-й слой состоит из всех тех $\wedge$-вершин w, которые удовлетворяют следующему условию: любой потомок вершины w либо является $\wedge$-вершиной, либо принадлежит слою с номером, меньшим i. Если (i-I)-й слой является $\wedge$-слоем, то i-й слой определяется двойственным образом.

Число получившихся слоев в схеме называется ее г л у б и н о й *. В частности, ДНФ можно рассматривать как схемы глубины 2. В схемах ограниченной глубины разрешается иметь только константное число слоев. Наиболее изучены (если не считать ДНФ и КНФ) схемы глубины 3. Среди них различают $\vee\wedge\vee$-схемы (где выход есть $\vee$-вершина) и $\wedge\vee\wedge$-схемы (выход является $\wedge$-вершиной).

Вершина схемы называется г р а н и ч н о й $\vee\wedge$-вершиной, если она является $\vee$-вершиной, а хотя бы один из ее сыновей есть $\wedge$-вершина. Двойственным образом определяется граничная $\wedge\vee$-вершина. Граничные $\vee\wedge$ и $\wedge\vee$-вершины образуют множество граничных вершин.

Нетрудно видеть, что в случае константной глубины формулы полиномиально эквивалентны СФЭ.

Хотя доказательства в [46, 69, 91, 97] проводятся для разных функций и используют разную технику доказательств, в идейном плане они схожи. Поэтому для определенности в дальнейшем будем обсуждать доказательство из [46]. В этой работе доказательство НОСЛ проводится для некоторой монотонной функции $f_N(x_1,\dots,x_N)$, все простые импликанты которой имеют одинаковую длину m. Множество этих импликантов обозначим $PI(f)$.

Положим

$$NM_f = \{\tilde{x} \mid f(\tilde{x}) = 1 \quad \text{и} \quad \tilde{y} < \tilde{x} \Rightarrow f(\tilde{y}) = 0\}$$

(множество нижних единиц функции f). Обозначим далее символом $P_t(f)$ множество всех монотонных булевых функций, которые принимают значение I в t точках множества NM_f и равны нулю на множестве $B^n \setminus N_f$.

* Следует отличать эту глубину от глубины как длины самого длинного пути в схеме (см. п.2.3). В литературе утвердилось одно то же название "глубина" для двух разных понятий.

Рассмотрим две задачи на покрытие. В первой задаче функции из множества $P_t(f)$ реализуются в классе КНФ. Нас интересует при этом минимальная сложность реализации функций из множества $P_t(f)$ (под сложностью здесь понимается число дизъюнкций (то есть число скобок), из которых состоит КНФ). Вторая задача заключается в покрытии множества N_f множествами N_g, где $g \in P_t(f)$, $t \le k$. Такое покрытие содержит очевидно не менее $|PI(f)|/k$ множеств.

Каждому покрытию в первой задаче можно сопоставить граничные $\vee\wedge$-вершины. Это вершины, в которых реализуются дизъюнкты КНФ. Каждому покрытию во второй задаче сопоставляются граничные $\wedge\vee$-вершины. Это вершины, в которых реализуются функции из множеств $P_t(f)$, "покрывающие" функцию f.

Тем самым, можно сказать, что доказательство НОСЛ для функции $f_N(x_1,\dots,x_N)$ сводится к оценкам ширины двух сечений: одно сечение образуют $\vee\wedge$-вершины, второе $\wedge\vee$-вершины. При надлежащем выборе параметра k получается нижняя оценка сложности, близкая к экспоненциальной. Она складывается из оценок сложности двух указанных сечений.

2.II. Характеристика эффективных нижних оценок сложности

В главе I говорилось о том, что для решения проблемы НОСЛ важно отделить эффективные НОСЛ от неэффективных. Материал этой главы позволяет описать некоторые характерные черты эффективных доказательств НОСЛ.

Наша характеризация основана на рассмотрении множества $\mathcal{F}$ ч.б.ф., покрываемых при доказательстве НОСЛ. Такие множества $\mathcal{F}$ были выявлены во всех доказательствах НОСЛ этой главы. Очевидно, такое множество можно указать и в случае неэффективных доказательств: достаточно взять его состоящим из одной функции, а именно, той функции, для которой проводится доказательство НОСЛ. Тогда характерное отличие эффективных доказательств состоит в том, что для них множество $\mathcal{F}$ состоит из большого числа простых функций. В частности, для всех рассмотренных в этой главе доказательств НОСЛ множество $\mathcal{F}$ состоит из ч.б.ф. сложности $O(n)$.

Описанная характеризация позволяет говорить и о степени эффективности доказательства: чем меньше сложность ч.б.ф. из множества $\mathcal{F}$, тем эффективнее доказательство. Наименее эффективными (по

нашей прежней терминологии, неэффективными) являются доказательства, основанные на применении мощностного метода Шеннона.

2.I2. От оценки сложности к оценке ширины

В п.2.2 – 2.I0 были рассмотрены представительные доказательства НОСЛ для различных моделей вычислений. Подведем теперь итоги этого рассмотрения. Разобранные примеры говорят о том, что доказательства НОСЛ разбиваются, как правило, на несколько этапов.

На первом этапе оценивается снизу ширина схемы функции, подлежащей оценке снизу. Этот этап представлен наиболее выпукло для схем с ограничениями. Уточним теперь, чем оценивается снизу ширина схемы. Для этого заметим, что с каждым из рассмотренных доказательств можно ассоциировать некоторую задачу на покрытие. Что при этом покрывается? Покрывается множество $\mathcal{F}$ ч.б.ф., указанных при разборе каждого доказательства. В качестве покрывающего множества выступает некоторое множество $\mathcal{S}$ подсхем схемы. Схема $S \in \mathcal{S}$ покрывает по определению ч.б.ф. $g \in \mathcal{F}$ тогда и только тогда, когда схема S реализует (вычисляет) функцию g. Множество $\mathcal{S}$ наиболее выпукло представлено в п.2.8 – это множество порождающих подсхем мономов. Рассмотрим произвольную универсальную схему $UC(\mathcal{S})$ множества $\mathcal{S}$. Тогда первый этап доказательства НОСЛ во всех рассмотренных доказательствах можно считать этапом оценки ширины схемы $UC(\mathcal{S})$.

При описании второго этапа доказательств НОСЛ полезно вспомнить название "метод длины-ширины", использованное О.Б.Лупановым [20] применительно к некоторым доказательствам НОСЛ. Мы утверждаем сейчас, что такую трактовку можно применить к каждому из доказательств этой главы. Трактовка станет более понятной, если слегка изменить название на "метод ширины-глубины". Уточним сначала понятие глубины.

Глубиной схемы называется длина самого длинного ориентированного пути в схеме.

Произвольную схему можно трактовать как двумерный объект, имеющий ширину и глубину, и снабдить каждую вершину схемы парой координат. Это можно сделать, например, следующим образом. Назовем j-слоем схемы S множество ее вершин v, удовлетворяющих следующему условию: длина самого длинного пути, соединяющего вершину v с одним из выходов, равна j. Очевидно, j может меняться от 0 до $d(S)$, где $d(S)$ – глубина схемы S. Перенумеровав вершины j-го слоя числами I,2, ..., снабдим каждую вершину v схемы парой координат (j, i), где j – номер слоя, которому принадлежит вершина v, а i – ее номер в этом слое.

Какое максимальное значение может принимать координата i? Поскольку множество вершин одного слоя образует независимое множество, то $i \le W(S)$ (напомним, что $W(S)$ обозначает ширину схемы S). Следовательно, число внутренних вершин схемы S, то есть ее сложность $L(S)$, не превышает произведения $W(S) \cdot d(S)$, то есть произведения ширины схемы на ее глубину.

Представление $L(S) \le W(S) \cdot d(S)$ дает конечно, не нижнюю, а верхнюю оценку сложности. Но если в подходящей минимальной схеме для функции f удастся найти "много" непересекающихся или слабо пересекающихся независимых множеств, то это дает нетривиальную нижнюю оценку вида $L(f) \ge w \cdot \ell$, где w оценивает снизу ширину функции f. Такое представление нижней оценки можно обнаружить во всех рассмотренных доказательствах. Особенно наглядно оно для схем из нулевых цепей (п.2.9) и синхронных схем (п.2.3).

Представление $L(f) \ge w \cdot \ell$ возможно для любой нижней оценки сложности: достаточно взять $w = 1$. Однако нас интересуют лишь такие доказательства НОСЛ, которые "сводятся" к нижней оценке ширины функции в том смысле, что в представлении $w \cdot \ell$ сомножитель w является "главным". Именно таковы все рассмотренные доказательства.

Для подтверждения изучим внимательнее сомножитель ℓ. Какие значения он может принимать? Здесь полезно вернуться к первому этапу доказательств НОСЛ и рассмотреть множество $\mathcal{F}$ ч.б.ф., мажорирующее доказательство. Во всех рассмотренных доказательствах множество $\mathcal{F}$ состоит лишь из простых функций, а именно, ч.б.ф. из $\mathcal{F}$ имеют сложность $O(n)$. По этой причине во всех рассмотренных доказательствах $\ell = O(n)$.

Изложенные выше соображения говорят о наличии тесной связи между задачей нижней оценки сложности $L(f)$ и задачей нижней оценки ширины функции $W(f)$. Мы привели доводы в пользу того, что первая из этих задач в значительной мере сводится ко второй. Это повышает интерес к задаче нижней оценки ширины схемы. Она будет рассматриваться в следующей главе.

ЗАКЛЮЧЕНИЕ

Мы рассмотрели в этой главе большое число представительных доказательств НОСЛ. При всем разнообразии этих доказательств в них можно отметить общие характерные черты.

Все рассматриваемые доказательства НОСЛ включают в качестве первого этапа нижнюю оценку ширины функции. Поскольку ширина функции не превышает сложности (по порядку), то первый этап уже дает нижнюю оценку сложности.

На втором этапе усиливается НОСЛ, полученная на первом этапе. Для всех рассматриваемых доказательств величина этого усиления весьма небольшая (а именно, $O(n)$). Точнее, она не превышает величины $\ell(n)$, которая характеризует степень эффективности доказательств. В частности, во всех известных эффективных доказательствах НОСЛ $\ell(n) = O(n)$.

Следовательно, для эффективных доказательств величина НОСЛ с точностью до множителя $\ell(n)$ равна нижней оценке ширины функции, полученной на первом этапе. Это заключение следует считать главным выводом данной главы.

ГЛАВА 3. МОДЕЛИ ДОКАЗАТЕЛЬСТВ НИЖНИХ ОЦЕНОК СЛОЖНОСТИ

В предыдущей главе была установлена тесная связь между доказательствами нижних оценок сложности и нижних оценок ширины. Это позволяет при моделировании доказательств НОСЛ ограничиться моделированием доказательств нижних оценок ширины.

В п.3.2 – 3.6 строятся конкретные модели доказательств нижних оценок сложности для различных моделей вычислений. В п.3.7 описываются два класса моделей доказательств НОСЛ. Изучение этих моделей позволяет дать ответ на второй вопрос проблемы НОСЛ, сформулированный в п.I.I.4.

3.I. Нижние оценки ширины схемы

Различные понятия ширины схемы были введены в п.2.I. Результаты главы 2 говорят о наличии тесной связи между задачами нижней оценки сложности и нижней оценки ширины. Интуитивно чувствуется, что эти две задачи очень близки. В этом параграфе мы дадим новые доводы в пользу этого предположения. А именно, мы покажем, что почти все булевы функции n переменных имеют экспоненциально большую ширину. В наших доказательства применяется мощностной метод Шеннона. Для простоты в качестве модели вычислений рассмотрим синхронные схемы (см. п.2.3 главы 2).

Пусть максимальная ширина яруса схемы S не превышает p. Занумеруем вершины каждого яруса (в том числе ярус, состоящий из полюсов) числами I,2, ... При этом полюс x_i снабдим номером i. Каждой внутренней вершине v_t i-го яруса сопоставим код

$$\varphi j_1 \dots j_r \lambda \,, \qquad (3.I)$$

где φ – это булева операция, приписанная вершине v_t, символы $j_1, \dots, j_r$ суть номера вершин (i-I)-го яруса, подаваемые на вход вершины v_t, а $\lambda \in \{0,1\}$. Признак λ говорит о том, является вершина v_t последней вершиной яруса или нет. Если операция φ

имеет менее r аргументов, то поставим на места оставшихся аргументов число I.

i -му ярусу схемы сопоставим код, который является конкатенацией кодов вершин $v_1, v_2, \ldots$ этого яруса, а всей схеме – конкатенацию кодов ярусов, начиная с первого. Очевидно, что по полученному коду синхронную схему S можно восстановить с точностью до изоморфизма.

Оценим сверху длину кода схемы. Пусть базис B содержит b различных операций. Тогда на первом месте в коде (3.I) может стоять один из b символов, а на следующих r местах символы алфавита $\{1, \ldots, \rho\}$. Таким образом, код схемы S сложности L при $L \geq 1$ состоит из L символов алфавита $B \times \{1, \ldots, \rho\}^r \times \{0,1\}$. Поэтому число различных таких кодов не превышает величины

$$(2b\rho^r)^L .$$

Лемма 3.I. Число $N(n, L, \rho)$ приведенных синхронных схем, реализующих функции n переменных, имеющих сложность не более L и ширину не более ρ, не превышает величины $(2b\rho^r)^{L+1} \cdot n$.

Доказательство. Приведенная схема нулевой сложности состоит из одного полюса. Поэтому число таких схем не превышает n. Число оставшихся схем не превышает $\sum_{i=1}^{L} a^i$, где $a = 2b\rho^r$. Поскольку $a \geq 2$, последняя сумма не превышает a^{L+1}.

Теорема 3.I. Для почти всех булевых функций f от n переменных ширина функции f в классе синхронных схем больше $2^{(1-\varepsilon)n/r}$ (ε – произвольная положительная константа, r – максимальное число переменных у базисных функций).

Доказательство. Из работы О.Б.Лупанова [I8] известно, что произвольную булеву функцию n переменных можно реализовать синхронной схемой сложности не более $(1+\alpha_n)2^n/n$, где $\alpha_n \to 0$ при $n \to \infty$. Оценим число $N(n, L, \rho)$ при $L = (1+\alpha_n)2^n/n$ и $\rho = 2^{(1-\varepsilon)n/r}$, где ε – произвольная положительная константа. В силу леммы 3.I

$$N(n, L, \rho) \leq (2b \cdot 2^{(1-\varepsilon)n})^{(1+\beta_n)2^n/n} \cdot n,$$

где $\beta_n \to 0$ при $n \to \infty$. Поэтому $N(n, L, \rho) \leq 2^{(1-\lambda)2^n}$, где λ – некоторая положительная константа. Следовательно,

$$N(n, L, \rho) = o(2^{2^n}) . \qquad (3.2)$$

Поскольку сложности $(1+\alpha_n)2^n/n$ достаточно для реализации произвольной булевой функции n переменных, то в силу мощностной леммы Шеннона из соотношения (3.2) следует, что для почти всех булевых функций n переменных максимальная ширина яруса в минимальной схеме превышает величину $2^{(1-\varepsilon)n/r}$.

Аналогичным образом можно было бы оценить ширину почти всех функций и в случае произвольных схем из функциональных элементов. Мы не стали этого делать, поскольку цель наша состоит в другом: показать, что имеется много общего между задачами нижней оценки сложности и нижней оценки ширины. Эта общность проявляется в том, что в обоих задачах доказуемы экспоненциальные нижние оценки и в обоих случаях это достигается применением неэффективных доказательств. Попытки эффективного доказательства высоких нижних оценок в обеих задачах сталкиваются примерно с одинаковыми трудностями.

3.2. Нижние оценки сложности универсальных функций

В главе 2 было показано, что целый ряд доказательств нижних оценок сложности (см. теоремы 2.I, 2.3, 2.5, 2.6 и леммы 2.5, 2.6) допускает перенос на подходящие универсальные функции. В этом параграфе устанавливаются некоторые "явные" нижние оценки сложности универсальных функций. Их вывод опирается на лемму 2.6 и теорему 2.6 главы 2.

3.2.I. Случай синхронных схем

Нижняя оценка сложности синхронных схем, установленная в П.2.3 главы 2, применяется здесь к конкретной универсальной функции. При этом получается максимальная по порядку НОСЛ, доказуемая для синхронных схем.

Пусть $\mathcal{F}$ есть множество всех булевых функций с переменными из множества X, причем эти функции имеют не более m существенных переменных. Для задания одной функции из $\mathcal{F}$ достаточно выбрать m-ку переменных (C_n^m способов) и далее фиксировать одну функцию этих переменных (2^{2^m} способов). Поэтому для задания универсальной функции $UF(\mathcal{F})$ достаточно иметь $2^m + \lceil \log C_r^m \rceil \leq 2^m + m \log n + 1$ дополнительных переменных.

Для любой m-ки переменных A из X универсальная функция $UF(\mathcal{F})$ содержит 2^{2^m} различных функций этих переменных. Поэтому (см. обозначения в п.2.3)

$$M(\log|UF(\mathcal{F})_A|, m, X) = 2^m \qquad (3.3)$$

и применение леммы 2.6 к $UF(\mathcal{F})$ дает $\rho \geq (1-\delta)2^m$

Положим $m =]\log n[$ и зафиксируем δ так, чтобы $0<\delta<1$. Тогда условия леммы 2.5 выполнены для $\log n$ ярусов (по порядку). Тем самым доказана

Теорема 3.2. Для универсальной функции $UF(\mathcal{F})$ в классе синхронных схем справедлива нижняя оценка $L(UF(\mathcal{F})) \succcurlyeq n\log n$.

З а м е ч а н и е. На первый взгляд может показаться, что, выбирая бо́льшие значения m, можно на основе (3.3) получать более высокие нижние оценки сложности. Однако не надо забывать, что $|Y| \geq 2^m$ и увеличение m увеличивает общее число переменных универсальной функции $UF(\mathcal{F})$, а нижние оценки надо получать в терминах общего числа переменных. Выбирая $m =]\log n[$, мы не увеличиваем по порядку общее число переменных.

3.2.2. Метод Нечипорука для универсальной функции

Применим метод Нечипорука к универсальной функции. Как видно из доказательства теоремы 2.6, оно сохраняет силу для произвольной функции, которая содержит функции из $\mathcal{F}_1 \cup \ldots \cup \mathcal{F}_\rho$ (см. п.2.4) в качестве своих подфункций. В частности, теорема применима к универсальной функции множества $\mathcal{F} = \mathcal{F}_1 \cup \ldots \cup \mathcal{F}_\rho$.

Чтобы получить оценку в терминах числа переменных, возьмем n вида 2^m, m вида 2^q, $\rho = n/m$ и разобьем множество X на ρ равномощных множеств $X_1, \ldots, X_\rho$, то есть $|X_1| = \ldots = |X_\rho| = m$. В качестве множества $\mathcal{F}_i$ возьмем множество $P_2^m(X_i)$ всех булевых функций, зависящих от переменных X_i. Положим $\mathcal{F} = \mathcal{F}_1 \cup \ldots \cup \mathcal{F}_\rho$. Универсальная функция $UF(\mathcal{F})$ множества $\mathcal{F}$ фактически совпадает с функцией, описанной в работе В.Пауля [76]. Оценка ее сложности вытекает из теоремы 2.6:

$$L_\varphi(UF(\mathcal{F})) \succcurlyeq n^2/\log n.$$

Действительно, $F_i = 2^{2^m} = 2^n$ для всех $i = 1, \ldots, \rho$. □

3.3. Сложность универсальных схем в неполном базисе $\{K, D\}$

В п.2.6 была доказана экспоненциальная нижняя оценка ширины схемы в базисе $B = \{K(x,y), D(x,y)\}$, где функции K и D задаются таблицей 2.I. Поскольку функции $K(x,y)$ и $D(x,y)$ имеют общее форсирующее значение (а именно, 2), то базис B, очевидно, не полон. В этом базисе не реализуемы универсальные функции, как это будет показано в главе 4 (п.4.3). В то же время универсальные схемы существуют всегда. В этом параграфе доказательство нижней оценки ширины функции (см. лемму 2.9 из п.2.6) моделируется доказательством нижней оценки подходящей универсальной схемы.

Введем несколько понятий, дополняющих понятие универсальной схемы (см. п.I.4). При определении универсальной схемы $UC(\mathcal{S})$ вершины каждой схемы $S \in \mathcal{S}$ отображались в вершины универсальной схемы $UC(\mathcal{S})$. Это отображение обозначалось символом U. Если при этом t есть выходная вершина схемы S, то говорят, что схема S реализуется в вершине $U(t)$ универсальной схемы.

Две схемы из $\mathcal{S}$ называются н е с о в м е с т и м ы м и, если они не могут быть реализованы в одной и той же вершине никакой универсальной схемы множества $\mathcal{S}$. Схема, состоящая только из полюса x_i, очевидно, несовместима ни с какой другой схемой. Далее, несовместимы две схемы, выходным вершинам которых приписаны разные операции. В остальном универсальные схемы имеют очень большие возможности для совмещения схем. В то же время при ограничениях на модели вычислений, что мы и имеем в данном случае, возможности совмещения резко уменьшаются.

Подмножество $\mathcal{S}' \subseteq \mathcal{S}$ называется несовместимым, если все схемы из $\mathcal{S}'$ попарно несовместимы. Наибольшее число схем в несовместимом подмножестве множества $\mathcal{S}$ обозначается $\alpha(\mathcal{S})$. Мы оценим в этом параграфе снизу величину $\alpha(\mathcal{S})$ для подходящего множества $\mathcal{S}$, что позволит оценить снизу сложность универсальной схемы.

Определим сначала множество $\mathcal{S}$ схем. Пусть $\tilde{\sigma}$ есть произвольный набор из E_2^n веса ρ, а $i_1, \ldots, i_\rho$ суть единичные разряды набора $\tilde{\sigma}$. Рассмотрим схему $S(\tilde{\sigma})$, построенную в соответствии с формулой $K(x_{i_1}, \ldots, x_{i_\rho})$. Эта схема реализует функцию, которая является доопределением ч.б.ф., равной I при $x_{i_1} = \ldots = x_{i_\rho} = 1$ и равной 0 на наборах $\tilde{\sigma} \in E_2^n$ веса $\rho - 1$. Положим

$$\mathcal{S}=\{S(\tilde{\sigma})\mid \tilde{\sigma}\in E_2^n,\ w(\tilde{\sigma})=p\}. \qquad (3.4)$$

Покажем, что множество $\mathcal{S}$ несовместимо.

Лемма 3.2. Множество $\mathcal{S}$, заданное соотношением (3.4), несовместимо.

Доказательство. Предположим, что схемы $S(\tilde{\sigma})$ и $S(\tilde{\delta})$ ($\tilde{\sigma}$ и $\tilde{\delta}$ – наборы из E_2^n веса p) реализуются в одной и той же вершине u некоторой универсальной схемы $UC(\mathcal{S})$ множества $\mathcal{S}$ из (3.4). Пусть схема $S(\tilde{\sigma})$ реализуется при $Y=\tilde{\alpha}$, а схема $S(\tilde{\delta})$ при $Y=\tilde{\beta}$. Обозначим символом Y_1 множество тех дополнительных полюсов из Y, которые предшествуют вершине u. Из определения функций K и D следует, что оба набора $\tilde{\alpha}$ и $\tilde{\beta}$ состоят из единиц в тех разрядах, которые принадлежат множеству Y_1. Повторяя далее доказательство леммы 2.9 главы 2, получим, что $\tilde{\sigma}=\tilde{\delta}$. Это означает, что при $\tilde{\sigma}\neq\tilde{\delta}$ схемы $S(\tilde{\sigma})$ и $S(\tilde{\delta})$ реализуются в разных вершинах. Следовательно, множество $\mathcal{S}$, заданное соотношением (3.4), несовместимо.

Следствие. Для множества $\mathcal{S}$ схем, определенных соотношением (3.4), в базисе $\{K(x,y),D(x,y)\}$ (см. таблицу 2.1 в главе 2) имеет место нижняя оценка $L(UC(\mathcal{S}))\geq C_n^p$.

3.4. Сложность монотонных универсальных схем для вычисления полиномов

Промоделируем теперь доказательство нижней оценки реберной ширины для одномерных полиномов (см. п.2.8) в случае монотонных схем доказательством НОСЛ для подходящего универсального полинома. Напомним, что монотонность схемы в данном случае означает, что базис содержит только монотонные функции $+$, $\times$ и на входы схемы разрешается подавать только (строго) положительные константы (но не 0!). Предполагается также, что кольцо не содержит делителей нуля. Напомним, что множество положительных констант в п.2.8 обозначалось R^+.

Уточним сначала понятие универсального полинома. При этом будем ориентироваться на понятие универсальной схемы.

Рассмотрим полиномы $P(X,Y)$, которые наряду с переменными X могут содержать новые переменные Y ($Y\cap X=\emptyset$). Переменные Y будем называть дополнительными, подстановкой констант на места дополнительных переменных – замены всех переменных из Y некоторыми константами из R^+. В результате подстановки констант на места дополнительных переменных получается некоторый полином над множеством переменных X.

Монотонная схема $UC(X,Y)$, полюсам которой приписаны переменные из $X\cup Y$, называется универсальной для множества полиномов $\mathcal{P}$, если для каждого полинома $P\in\mathcal{P}$ существуют вершина $v(P)$ схемы $UC(X,Y)$ и подстановка констант из R^+ на места дополнительных переменных Y такие, что после этой подстановки констант в вершине $v(P)$ вычисляется полином, эквивалентный полиному P. Универсальную монотонную схему для множества полиномов $\mathcal{P}$ будем обозначать $UC(\mathcal{P})$. Про вершину $v(P)$ будем говорить, что в ней реализуется полином P.

Замечание. В отличие от случая универсальных функций наличие дополнительных переменных в универсальной схеме не обязательно. Действительно, поскольку разные полиномы могут по определению вычисляться в разных вершинах, то универсальная схема может быть образована из отдельных схем для разных полиномов. Мы увидим ниже, что именно так (или близко к этому) обстоит дело с произвольной универсальной схемой при вычислении полиномов. При этом, конечно, существенно, что мы ограничиваемся монотонными схемами.

Минимальную сложность монотонной универсальной схемы для множества полиномов $\mathcal{P}$ обозначим $L(UC(\mathcal{P}))$.

По аналогии со случаем булевских схем два монотонных полинома из $\mathcal{P}$ называются несовместимыми, если они не могут быть реализованы в одной и той же вершине никакой монотонной универсальной схемы множества $\mathcal{P}$. Множество $\mathcal{P}$ монотонных полиномов называется несовместимым, если каждая пара различных полиномов из $\mathcal{P}$ несовместима.

Теорема 3.3. Произвольное множество $\mathcal{P}$ неэквивалентных монотонных полиномов несовместимо.

Доказательство. Рассмотрим произвольную монотонную универсальную схему $UC(\mathcal{P})$ для множества полиномов $\mathcal{P}$. В силу монотонности при любых подстановках констант из R^+ на места дополнительных переменных получаются эквивалентные полиномы. Поэтому два полинома из $\mathcal{P}$ не могут быть реализованы в одной вершине схемы $UC(\mathcal{P})$.

Свойство несовместимости позволяет легко моделировать доказательство теоремы 2.10. Для этого достаточно в качестве множества $\mathcal{P}$

взять множество одномономных полиномов, вычисляемых в образующих вершинах схемы, реализующей одномерный полином.

З а м е ч а н и е . Сложность универсальной схемы экспоненциально уменьшается, если разрешить заменять дополнительные переменные не только положительными константами, но и нулем. Действительно, схема, построенная в соответствии с формулой

$$\prod_{i=1}^{n} (x_i \times y_i + 1 \times z_i) \qquad (3.5)$$

(y_i и z_i - дополнительные переменные), имеет линейную сложность и универсальна для множества $M(x_1,\dots,x_n)$ мономов вида $x_1^{\sigma_1}\dots x_n^{\sigma_n}$ ($\sigma_i \in \{0,1\}$, $1 \le i \le n$). В то же время, как показывает теорема 3.3, в случае монотонных схем универсальная схема $UC(M(x_1,\dots,x_n))$ имеет экспоненциальную сложность. Поскольку для схемы, построенной в соответствии с (3.5), требуются лишь константы 0 и I, этот пример можно истолковывать как экспоненциальную силу добавления константы 0.

Покажем теперь, что не только доказательство теоремы 2.I0, но и многие другие доказательства НОСЛ монотонного вычисления полиномов можно моделировать доказательством НОСЛ универсальной схемы.

Если $\mathcal{P}$ есть множество полиномов сложности не более $S(n)$, то монотонную универсальную схему этого множества обозначим $UC(n,S)$.

Доказательство нижней оценки сложности для полинома P называется и н в а р и а н т н ы м , если оно сохраняет силу для любого полинома, эквивалентного P . В частности, доказательство теоремы 2.I0 инвариантно.

Доказательство нижней оценки сложности для полинома $P(x_1,\dots,x_n)$ принадлежит по определению классу (t,S) , если оно доказывает существование в некоторой минимальной схеме, вычисляющей полином P, $t(n)$ различных вершин, в которых вычисляются полиномы сложности не более $S(n)$. Такое доказательство называют еще (t,S)-доказательством. Инвариантные (t,S)-доказательства образуют естественный класс доказательств.

Теорема 3.4. Каждому инвариантному (t,S)-доказательству нижней оценки сложности монотонного вычисления полинома можно сопоставить доказательство оценки $L(UC(n,S)) \ge t(n)$.

Д о к а з а т е л ь с т в о . По определению (t,S)-доказательства в некоторой минимальной схеме S существует t различных вершин $v_1,\dots,v_t$, в которых вычисляются полиномы сложности не

более $S(n)$. Обозначим эти полиномы соответственно P_1 , ... , P_t .

Предположим, что для некоторых i и j ($1 \le i < j \le t$) в универсальной схеме $UC(n,S)$ полиномы P_i и P_j вычисляются в одной вершине при некоторых подстановках констант. Но тогда в силу монотонности полиномы P_i и P_j эквивалентны. В таком случае, "перекинув" начала дуг, идущих из вершины v_j , в вершину v_i и удалив вершину v_j , мы получили бы эквивалентную схему меньшей сложности, что противоречит минимальности схемы S или инвариантности доказательства. □

3.5. Нижняя оценка сложности универсальных схем без нулевых цепей

В этом параграфе доказательство нижней оценки ширины кодовой функции (сп. п.2.9 главы 2) моделируется на универсальной схеме. Поскольку для универсальных схем НОСЛ доказываются значительно легче, то мы можем провести доказательство не только для П-схем, как это делалось для простоты в п.2.9, но для более общего случая схем из функциональных элементов без нулевых цепей.

Понятие схем без нулевых цепей введено С.Е.Кузнецовым [I5]. Оно является естественным переносом на случай схем аналогичного понятия для П-схем, предложенного А.К.Пулатовым [37]. Предлагаемое ниже определение схем без нулевых цепей в некоторых несущественных деталях отличается от определения из [I5].

В этом параграфе мы будем рассматривать схемы из функциональных элементов в базисе $\{\wedge, \vee\}$, полюсам которых могут быть приписаны переменные x_i и их отрицания $\bar{x}_i$. Очевидно, произвольная булева функция может быть вычислена такой схемой. Каждый из двух входов произвольного неизолированного элемента схемы является концом некоторого пути, начинающегося в одном из полюсов. Произвольную пару путей, начинающихся в полюсах схемы и заходящих в некоторую вершину w схемы по двум разным дугам, будем называть ц е п ь ю с х е м ы (с точкой провисания w). Два пути, образующие цепь, называются п л е ч а м и этой цепи.

Цепь схемы называется н у л е в о й , если ее плечи начинаются соответственно в полюсах x_i и $\bar{x}_i$ ($i \in \{1,\dots,n\}$), а точка провисания есть $\wedge$ -вершина. Схема называется с х е м о й б е з н у л е в ы х ц е п е й , если она не содержит нулевых цепей.

Сложность функции f в классе схем без нулевых цепей обозначается $L^*(f)$. Всюду в этом параграфе под схемами подразумеваются схемы без нулевых цепей.

Перейдем к моделированию доказательства НОСЛ для кодовой функции $C(n,d)$ с кодовым расстоянием d из [15] (см. также для сравнения п.2.9, где изложено доказательство НОСЛ для П-схем без нулевых цепей) на универсальных схемах без нулевых цепей.

Разобьем переменные x на группы переменных $x_1,\dots,x_h$ так, чтобы каждая группа содержала d переменных (d – это кодовое расстояние кода $C(n,d)$), кроме разве лишь последней, в которой число переменных d' удовлетворяет условию $d \le d' < 2d$. Очевидно

$$h \le [\, n/d \,]. \qquad (3.6)$$

Сопоставим каждой точке $\tilde\sigma \in C(n,d)$ конъюнкцию $K(\tilde\sigma) = x_1^{\sigma_1}\dots x_n^{\sigma_n}$. Рассмотрим подконъюнкции $K_1(\tilde\sigma),\dots,K_h(\tilde\sigma)$ конъюнкции $K(\tilde\sigma)$, соответствующие разбиению переменных x на подмножества $x_1,\dots,x_h$. Точнее, конъюнкция $K_i(\tilde\sigma)$ содержит в точности те переменные из $K(\tilde\sigma)$, которые входят в x_i, причем в тех степенях, в которых они встречаются в $K(\tilde\sigma)$.

Рассмотрим схему $S(\tilde\sigma)$ без нулевых цепей, построенную в соответствии с формулой

$$(K_1(\tilde\sigma)\wedge\dots\wedge K_h(\tilde\sigma))\wedge(K_1(\tilde\sigma)\wedge\dots\wedge K_h(\tilde\sigma)).$$

Она состоит из двух идентичных подсхем, которые будем называть соответственно левой и правой подсхемами схемы $S(\tilde\sigma)$. Множество схем $S(\tilde\sigma)$ по всем $\tilde\sigma \in C(n,d)$ обозначим $\mathcal{S}$. Рассмотрим произвольную универсальную схему $UC(\mathcal{S})$ без нулевых цепей. Согласно определению, вершины каждой схемы $S \in \mathcal{S}$ отображаются взаимно однозначно в вершины схемы $UC(\mathcal{S})$. Обозначим соответственно символами $a_1(\tilde\sigma),\dots,a_h(\tilde\sigma)$ образы выходных вершин подсхем $K_1(\tilde\sigma),\dots,K_h(\tilde\sigma)$ левой подсхемы схемы $S(\tilde\sigma)$ в универсальной схеме $UC(\mathcal{S})$.

Лемма 3.3. При $\tilde\sigma \ne \tilde\delta$ $\{a_1(\tilde\sigma),\dots,a_h(\tilde\sigma)\} \ne \{a_1(\tilde\delta),\dots,a_h(\tilde\delta)\}$.

Доказательство. Пусть $\sigma_j \ne \delta_j$ для некоторого j $(1 \le j \le n)$. Предположим, что $\{a_1(\tilde\sigma),\dots,a_h(\tilde\sigma)\} = \{a_1(\tilde\delta),\dots,a_h(\tilde\delta)\}$. Обозначим символами $v_\ell(\tilde\sigma)$ и $v_r(\tilde\sigma)$ образы выходных вершин соответственно левой и правой подсхем схемы $S(\tilde\sigma)$. Аналогичные вершины для схемы $S(\tilde\delta)$ обозначим $v_\ell(\tilde\delta)$ и $v_r(\tilde\delta)$. Очевидно, в вершины $v_\ell(\tilde\sigma)$ и $v_\ell(\tilde\delta)$ ведут пути из вершин $a_i(\tilde\sigma)$ $(i=1,\dots,h)$ и, следовательно, из полюсов $x_j^{\sigma_j}$ и $x_j^{\delta_j}$. В вершины $v_r(\tilde\sigma)$ и $v_r(\tilde\delta)$

тоже ведут пути из полюсов $x_j^{\sigma_j}$ и $x_j^{\delta_j}$. Далее, образом выходной вершины схемы $S(\tilde\sigma)$ в универсальной схеме $UC(\mathcal{S})$ является некоторая $\wedge$-вершина v. В нее ведут пути из $v_\ell(\tilde\sigma)$ и $v_r(\tilde\sigma)$ и, следовательно, пути из $x_j^{\sigma_j}$ и $x_j^{\delta_j}$. Но это означает наличие в схеме нулевой цепи (с точкой провисания v), что противоречит отсутствию нулевых цепей в схеме $UC(\mathcal{S})$. □

Комментарий. Как видно из доказательства леммы, принадлежность точек $\tilde\sigma, \tilde\delta$ коду совершенно несущественна. Мы взяли эти точки кодовыми только ради аналогии с моделируемым доказательством из [15]. Там это условие было необходимо (см. также для сопоставления п.2.9), чтобы показать, что в образующих вершинах вычисляются конъюнкции не менее d переменных. Здесь это следует из самого построения схем $S(\tilde\sigma)$.

Обозначим символом A объединение $\bigcup_{\tilde\sigma \in C(n,d)} \{a_1(\tilde\sigma),\dots,a_h(\tilde\sigma)\}$.

Лемма 3.4. $|A| \ge |C(n,d)|^{d/(n+d)}$.

Доказательство. Обозначим $N = |A|$. Из леммы 3.3 следует, что различным точкам кода $C(n,d)$ соответствуют различные h-элементные подмножества множества A. Поэтому $C_N^h \ge |C(n,d)|$, откуда с учетом (3.6) и следует требуемая оценка. □

Комментарий. Сопоставление леммы 3.4 с леммой 2.20 главы 2 показывает, что доказательство нижней оценки сложности универсальной схемы (лемма 3.4) можно рассматривать в качестве модели доказательства нижней оценки ширины (лемма 2.20). Действительно, доказательство леммы 3.4 в главных чертах повторяет доказательство леммы 2.20. При этом доказательство НОСЛ для универсальной схемы существенно проще, поскольку наличие вершин, в которых вычисляются конъюнкции $K_1(\tilde\sigma),\dots,K_h(\tilde\sigma)$, обеспечивается уже определением. Обратим также внимание на то, что множество $\mathcal{S}$, которое определяет схему $UC(\mathcal{S})$ и тем самым доказательство леммы 3.4, состоит из схем малой сложности, вычисляющих ч.б.ф. f, сопоставленные доказательству в п.2.9.

Выбирая конкретные коды $C(n,d)$, можно получать конкретные оценки. Например, взяв в качестве $C(n,d)$ код Рида–Маллера с $n=2^m$, $d=\sqrt{n}$ и обозначив символом $\mathcal{S}$ множество схем, соответствующих в описанном выше смысле точкам этого кода, получим следующее утверждение:

Теорема 3.5. Сложность универсальной схемы без нулевых цепей $UC(S)$ удовлетворяет неравенству

$$L^*(UC(S)) \geq 2^{\sqrt{n}/(2+\varepsilon_n)},$$

где $\varepsilon_n \to 0$ при $n \to \infty$.

З а м е ч а н и е . Как уже отмечалось в комментарии к лемме 3.4, для доказательства лемм 3.3, 3.4 и, следовательно, теоремы 3.5 совершенно несущественно, что схемы из S соответствуют точкам кода $C(n,d)$. Мы взяли здесь кодовое множество единственно для того, чтобы приблизить доказательство нижней оценки для универсальной схемы $UC(S)$ к доказательству нижней оценки для функции f из исходной работы [15]. В нашем случае можно было бы заменить кодовое множество $C(n,d)$ на множество всех точек из B^n и тем самым повысить нижнюю оценку. Более того, поскольку, как мы выяснили, в случае универсальных схем $UC(S)$ кодовость множества $C(n,d)$ несущественна, то несущественной становится и величина d (кодовое расстояние). Поэтому в лемме 3.4 и в теореме 3.5 вместо образов выходных вершин подсхем $K_1(\tilde{\sigma}), \ldots, K_k(\tilde{\sigma})$ можно было бы говорить об образах выходных вершин схем $S(\tilde{\sigma})$ и доказывать, что они различны. Это позволяет поднять нижнюю оценку сложности универсальной схемы $UC(S)$ до 2^n.

Пример схем без нулевых цепей лишний раз показывает, что нижние оценки сложности для универсальных схем доказываются намного проще, чем для функций. Поэтому для выяснения возможностей доказательств НОСЛ для функций на качественном уровне достаточно оценить сначала сложность универсальных схем.

3.6. Сложность универсальных схем ограниченной глубины

В этом параграфе моделируется доказательство НОСЛ для схем ограниченной глубины из п.2.10 главы 2. Напомним, что в этих схемах полюсам могут приписываться не только переменные, но и их отрицания, а каждая внутренняя вершина схемы есть либо $\wedge$ -, либо $\vee$ -вершина. Такие схемы будем называть р е г у л я р н ы м и .

В этом параграфе рассматриваются регулярные схемы. Будем называть сквозным путем схемы произвольный путь, соединяющий один из полюсов схемы с выходом.

Г л у б и н о й п у т и называется число перемен знаков

операций, приписанных внутренним вершинам пути (считается, что при переходе от полюса к внутренней вершине тоже происходит смена операций). Глубина схемы, очевидно, равна максимальной глубине путей схемы.

Регулярную схему будем называть синхронной*, если все сквозные пути схемы имеют одинаковую глубину.

Элемент схемы будем называть с и н х р о н и з а т о р о м , если на его входы подаются равные функции. Другими словами, синхронизатор выполняет преобразование вида $u \wedge u$ или $u \vee u$. Ясно, что с точки зрения вычислений синхронизатор является лишним элементом и его присутствие в схеме может быть оправдано лишь необходимостью синхронизации.

Синхронные схемы имеют более стандартный вид. Внутренние вершины синхронной схемы разбиваются на слои, обладающие следующими свойствами:

(а) всем внутренним вершинам одного слоя приписана одна операция (конъюнкция или дизъюнкция);

(б) вершинам соседних слоев приписаны разные операции;

(в) число слоев равно глубине схемы.

Глубину пути, оканчивающегося в данном слое, будем называть номером слоя.

Лемма 3.5. Для каждой регулярной схемы глубины r сложности s существует эквивалентная синхронная схема той же глубины сложности $O(rs)$.

Д о к а з а т е л ь с т в о . Будем обозначать символами φ и ψ операции "конъюнкция" и "дизъюнкция" (разные операции разными символами). Преобразуем сначала регулярную схему S в схему S', в которой оба родителя каждой вершины имеют одинаковые знаки операций. Для этого поступим следующим образом: если у φ-вершины w родитель u есть φ-вершина, а родитель v есть ψ-вершина, то поместим между вершинами v и w φ-синхронизатор. Если у вершины w родитель u есть полюс, а родитель v есть φ-вершина, то между вершинами u и w поместим φ-синхронизатор. Очевидно, добавляемые вершины уже обладают требуемым свойством. Поэтому при переходе от схемы S к S' будет добавлено не более s вершин. Очевидно также, что схема S' имеет ту же глубину, что и схема S.

---

* Не следует смешивать это понятие синхронности с тем, которое было в п.2.3.

Если в схеме S' некоторый сквозной путь имеет глубину r' менее r, то поместим на ребре этого пути, идущем из полюса, $r-r'$ синхронизаторов с нужной последовательностью операций. При этом добавится $O(rs)$ вершин. □

Определим индуктивно некоторое множество схем $\mathcal{S}_K$. Множество $\mathcal{S}_1^{\wedge}$ состоит из всевозможных конъюнкций переменных x (возможно, с отрицаниями). Если множество $\mathcal{S}_i^{\wedge}$ уже построено, то $\mathcal{S}_{i+1}$ состоит по определению из схем вида $S_1 \vee S_2$, где $S_1, S_2 \in \mathcal{S}_i^{\wedge}$, а множество $\mathcal{S}_{i+2}^{\vee}$ состоит из всех схем вида $S_1 \wedge S_2$, где S_1, $S_2 \in \mathcal{S}_{i+1}^{\vee}$. Верхние индексы при $\mathcal{S}_i^{\wedge}$ и $\mathcal{S}_{i+1}^{\vee}$ иногда будем опускать.

Утверждение 3.I. Если $S \in \mathcal{S}_r$, то в классе регулярных схем

$$L(S) \le n 2^{r-1} - 1 .$$

Доказательство. Если $S \in \mathcal{S}_1$, то очевидно $L(S) \le n-1 = n 2^{1-1} - 1$. Для схемы $S \in \mathcal{S}_r$ по индукции выводим

$$L(S) \le L(S_1) + L(S_2) + 1 \le 2(n 2^{r-2} - 1) + 1 = n 2^{r-1} - 1 . \quad \square$$

Пусть $UC(\mathcal{S}_r)$ есть универсальная схема глубины r, моделирующая схемы из $\mathcal{S}_r$. В качестве $UC(\mathcal{S}_r)$ можно взять, например, схему вида

$$\bigvee_{S_h \in \mathcal{S}_{r-1}} S_h y_h$$

при четном r или схему вида

$$\bigwedge_{S_h \in \mathcal{S}_{r-1}} (S_h \vee y_h)$$

при нечетном r.

Докажем теперь нижнюю оценку сложности схемы $UC(\mathcal{S}_r)$. Как и в п.3.5, 3.6, она основана на доказательстве несовместимости схем.

Лемма 3.6. Вершинам первого слоя произвольной схемы $S \in \mathcal{S}_r$ могут соответствовать лишь вершины первого слоя универсальной схемы $UC(\mathcal{S}_r)$ глубины r.

Доказательство. Универсальные схемы были определены в п.I.4. Пусть вершина a принадлежит первому слою схемы $S \in \mathcal{S}_r$. На пути, соединяющем вершину a с выходом, отметим по одной вершине в каждом из слоев с номерами I, 2, ..., r. В силу свойства (б) универсальных схем этим вершинам соответствуют вершины v_1, $v_2, \ldots, v_r$ из $UC(\mathcal{S}_r)$ с чередующимися операциями. В силу свойства (в) универсальных схем вершины $v_1, v_2, \ldots, v_r$ лежат на ориентированном пути и, следовательно, в разных слоях. Поскольку слоев в схеме $UC(\mathcal{S}_r)$ всего r, то вершина v_1 может лежать лишь в первом слое. □

Очевидно, вершины первого слоя схемы $UC(\mathcal{S}_r)$ реализуют конъюнкции из $\mathcal{S}_1^{\wedge}$. Поэтому можно говорить об отображении множества конъюнкций из $\mathcal{S}_1^{\wedge}$ в множество вершин первого слоя универсальной схемы $UC(\mathcal{S}_r)$. При этом две разные конъюнкции не могут отобразиться в одну вершину универсальной схемы в силу свойства (г) универсальных схем.

Легкость доказательства НОСЛ для универсальных схем ограниченной глубины позволяет без труда моделировать доказательства НОСЛ в этом классе схем.

3.7. Две модели доказательств нижних оценок сложности

Материал глав 2 и 3 позволяет описать две математические модели доказательств нижних оценок сложности. Первая модель (универсальные функции) годится для целого ряда доказательств оценок сложности. Вторая (универсальные доказательства) имеет значительно более широкую сферу приложений. Она годится для подавляющего большинства опубликованных доказательств нижних оценок сложности.

3.7.I. Универсальные функции

Первая модель доказательств нижних оценок сложности, называемая для краткости "универсальные функции", состоит в следующем. В главе 2 (см. заключение к ней) мы показали, что с каждым доказательством нижних оценок сложности можно связать некоторое множество $\mathcal{F}$ ч.б.ф. Рассмотрим универсальную функцию $UF(\mathcal{F})$ этого множества. Доказательства теорем 2.I, 2.3, 2.5, 2.6 и лемм 2.5, 2.6 показывают, что эти множества $\mathcal{F}$ полностью характеризуют доказательства НОСЛ. Они после небольшой модификации слово в слово применимы и к универсальной функции $UF(\mathcal{F})$. Поэтому доказательство НОСЛ для универсальной функции $UF(\mathcal{F})$ можно рассматривать как модель доказательства НОСЛ для исходной функции. Эта модель является весьма точной в следующем смысле. Во-первых, множество $\mathcal{F}$ покрываемых ч.б.ф. переходит в модель без изменений. Во-вторых, исходное доказательство НОСЛ почти дословно переносится на универсальную функцию $UF(\mathcal{F})$.

Модель "универсальные функции" позволяет оценить сверху воз - можности доказательств нижних оценок сложности, покрывающих множество $\mathcal{F}$. Для этого достаточно оценить сверху сложность универсальной функции $UF(\mathcal{F})$, что и будет сделано в следующей главе . При этом сложность $L(UF(\mathcal{F}))$ следует оценивать в терминах числа n переменных исходной функции, а не в терминах общего числа переменных универсальной функции, которая, как известно, содержит еще и дополнительные переменные. Это надо сделать потому, что при моделировании исходного доказательства НОСЛ мы получаем нижнюю оценку всегда в терминах исходного числа переменных.

Модель "универсальные функции" говорит о том, что универсальные функции часто являются наиболее подходящими для доказательств НОСЛ. Это было видно на целом ряде примеров из главы 2 (см. п.2.2 - 2.4), где мы часто формулировали и доказывали нижние оценки в терминах универсальных функций, поскольку в этом случае доказательства становятся наиболее прозрачными. Правда, при этом мы можем несколько ослабить получаемую нижнюю оценку, поскольку ее надо пересчитать на общее число переменных универсальной функции. Но потери, получаемые при этом, незначительны (при разумном выборе универсальной функции) и ими часто можно пренебречь.

Общий вывод, к которому приводит рассмотрение модели "универ - сальные функции", таков: чем больше подфункций содержит функция, тем большую можно ожидать для нее нижнюю оценку сложности. Примерно такие соображения были высказаны еще в работе [52] С.В.Яблонским. Подобную модель, по-видимому, имели в виду Д.Улиг [47] и Л.Харпер, В.Хсай и Дж.Сэвидж [62], которые привели примеры функций линейной сложности с большим числом подфункций. Авторы работ [47, 62] были, чувствуется, обескуражены полученными результатами, поскольку рас - считывали получить высокие НОСЛ для функций, с большим числом под - функций. Результаты главы 4 данной работы говорят о том, что осно - вываясь только на этих соображениях, высокие НОСЛ получить невозможно.

3.7.2. Универсальные доказательства нижних оценок сложности

Модель "универсальные функции" обладает рядом достоинств (это прежде всего точность модели), но имеет ограниченную применимость. Поэтому мы рассмотрим другую модель (универсальные доказательства

НОСЛ), которая, уступая первой модели по точности, намного превосходит ее по применимости. В частности, она годится для всех дока - зательств нижних оценок сложности, рассмотренных в главе 2.

Анализ доказательств нижних оценок сложности (см. п.2.I2 и заключение к главе 2) показывает, что в огромном большинстве случаев доказательство НОСЛ сводится к нижней оценке ширины функции. Другой вывод главы 2: с каждым доказательством НОСЛ естественно связано некоторое множество $\mathcal{F}$ ч.б.ф. исходной функции. Это множество $\mathcal{F}$ в большой степени характеризует доказательство НОСЛ. Поэтому не будет большой ошибкой идентифицировать доказательство НОСЛ символом $\mathcal{F}$.

В этой главе мы сопоставили каждому доказательству нижней оценки ширины из главы 2 доказательство нижней оценки сложности подходящей универсальной схемы $UC(\mathcal{S})$. Это сопоставление обладает рядом свойств. Во-первых, каждой ч.ф. $g \in \mathcal{F}$ соответствует некоторая схема $S \in \mathcal{S}$, которая ее реализует. Во-вторых, сложность соответствующей схемы S по порядку не превосходит сложность ч.ф. g . В-третьих, величина нижней оценки ширины мажорируется сложностью универсальной схемы $UC(\mathcal{S})$. Эти три свойства позволяют рассматривать доказательство нижней оценки сложности универсальной схемы $UC(\mathcal{S})$ как модель доказательства $\mathcal{F}$ нижней оценки ширины.

Убедимся, что доказательствам главы 2 можно сопоставить дока - зательства НОСЛ универсальных схем и это сопоставление обладает тремя указанными свойствами. В случаях неполного базиса $\{K, D\}$, моно - тонных схем для вычисления полиномов, схем без нулевых цепей и схем ограниченной глубины это было показано соответственно в п.3.3 - 3.6. В остальных доказательствах главы 2, а именно, в теоремах 2.I - 2.7, 2.9 и в леммах 2.5, 2.6 нижняя оценка ширины берется тривиальная - по числу входных или выходных полюсов. Поэтому множество $\mathcal{S}$ можно выбрать таким, чтобы сопоставление обладало свойствами I и 2, а обладание свойством 3 является очевидным. Итак, можно считать, что доказательства НОСЛ универсальных схем моделируют доказательства ниж - ней оценки ширины во всех доказательствах, рассмотренных в главе 2. На самом деле это справедливо для значительно более широкого круга доказательств.

Вспомним теперь (см. заключение к главе 2), что для очень многих доказательств НОСЛ величина нижней оценки сложности равна с точностью до множителя $L(\mathcal{F})$ нижней оценке ширины функции.

Эти рассмотрения подводят нас к следующей модели. Будем называть универсальным доказательством $\mathcal{S}$ нижней оценки сложности доказательство НОСЛ для универсальной схемы $UC(S)$. Согласно определению, применением универсального доказательства $\mathcal{S}$ не выводимы нижние оценки сложности, превышающие по порядку величину $LB(S) = L(UC(S)) \cdot L(S)$.

Рассмотрения глав 2 и 3 показывают, что для очень большого числа доказательств НОСЛ имеются моделирующие их универсальные доказательства, причем $L(S) = O(L(F))$, а величина нижней оценки сложности не превышает величины $LB(S)$.

Поскольку при хорошем моделировании $L(S) = O(L(F))$, а при эффективных доказательствах НОСЛ величина $L(F)$ небольшая, то значение величины $LB(S)$, ограничивающей сверху величины НОСЛ, определяется в большой мере величиной $L(UC(S))$. Поэтому для выяснения возможностей доказательства высоких НОСЛ следует оценить сложность универсальной схемы $L(UC(S))$.

Результаты п.3.3 – 3.6 говорят о том, что для схем с ограничениями (а именно, монотонных схем для вычисления полиномов, схем в неполном базисе $\{K, D\}$, схем без нулевых цепей и схем ограниченной глубины) универсальные схемы имеют экспоненциально большую сложность. Это служит предпосылкой доказательства высоких НОСЛ для указанных моделей. Тем самым мы в определенной степени отвечаем на второй вопрос проблемы НОСЛ (см. п.I.I.4 главы I), а именно, вопрос о различиях в трудности доказательства высоких НОСЛ для различных моделей. Наше объяснение состоит в следующем: высокие НОСЛ легче доказываются для тех моделей вычислений, для которых универсальные схемы имеют большую сложность.

Для моделей без ограничений мы не смогли пока установить высокие НОСЛ для универсальных схем, и это не случайно: в главе 4 будет показано, что эти универсальные схемы имеют "малую" сложность.

ГЛАВА 4. СЛОЖНОСТЬ УНИВЕРСАЛЬНЫХ СХЕМ

В предыдущей главе были установлены нижние оценки сложности универсальных схем для различных моделей вычислений. Для целого ряда моделей они оказались экспоненциально высокими. Для других моделей (СФЭ, формулы, синхронные схемы) эти оценки, напротив, весьма скромны по величине.

В этой главе приводятся конструкции универсальных схем. При этом мы ограничиваемся рассмотрением тех моделей, для которых в главе 3 нижние оценки были невысокими. Выясняется, что для этих моделей существуют экономные универсальные схемы. На основе верхних оценок сложности универсальных схем делается заключение о невозможности доказательства высоких НОСЛ для ряда моделей вычислений (СФЭ, формулы, синхронные схемы) в классе универсальных доказательств НОСЛ.

4.I. Реализация универсальных функций

В дальнейшем нас будут интересовать не только булевы функции, но и их обобщение – функции k-значной логики. Поэтому введем ряд дополнительных определений и обозначений.

Пусть $E_k = \{0, 1, \ldots, k-1\}$. Функции, аргументы которых определены на множестве E_k и значения которых тоже принадлежат множеству E_k, называются функциями k-значной логики. При $k = 2$ получаем булевы функции. Множество всех функций k-значной логики обозначается P_k.

Пусть $T \subseteq P_k$. Множество $[T]$ всевозможных суперпозиций функций множества T называется замыканием класса T. Если $[T] = T$, множество T называется замкнутым классом. Исчерпывающее перечисление замкнутых классов для булевского случая ($k = 2$) дано Э.Постом (см. [53]).

Система функций B из замкнутого класса T называется полной в T, если $[B] = T$. При рассмотрении схемных вопросов система B называется также базисом класса T. Очевидно, задание

базиса однозначно определяет замкнутый класс T. Если $T \neq P_k$, базис B класса T называется **неполным** (в P_k).

Пусть теперь $X = \{x_1, \ldots, x_n\}$ есть множество переменных со значениями из E_k. Символом $T(n)$ обозначим множество функций из класса T, зависящих (не обязательно существенно) от переменных из X. Понятие универсальной функции, введенное в п.I.4, естественным образом распространяется на k-значный случай. Универсальная функция $UF(T)$ множества $T(n)$ может сама принадлежать классу T, а может принадлежать разности $P_k \setminus T$. Нас интересует прежде всего критерий принадлежности универсальной функции $UF(T)$ замкнутому классу T.

Введем в рассмотрение простейшую универсальную функцию. Функция $V(x_1, x_2, y)$ называется **функцией выбора**, если она равна x_1 при некоторой подстановке констант на места переменных y и равна x_2 при некоторой (другой) подстановке констант на места y. Очевидно, функция $V(x_1, x_2, y)$ является универсальной для множества функций $P = \{x_1, x_2\}$. В качестве примера функции выбора при $k = 2$ можно назвать функцию $x_1 y_1 \vee x_2 y_2$. Оказывается, реализуемость функции выбора решающим образом влияет на принадлежность универсальной функции классу T.

Теорема 4.I. Если в конечном базисе B представима хотя бы одна функция выбора, то замкнутый класс $T = [B]$ содержит универсальную функцию $UF(T(n))$. Если $x \in [B]$, верно и обратное.

Доказательство. Пусть в базисе B представима некоторая универсальная функция $UF(X, Y)$ множества $T(n)$. Очевидно, x_1 и x_2 принадлежат $T(n)$ при $n \geq 2$. Поэтому при некоторой подстановке констант на места переменных y $UF(X, Y) = x_1$, а при другой подстановке констант $UF(X, Y) = x_2$. Поэтому функция $V(x_1, x_2, y) = UF(x_1, x_2, \ldots, x_2, y)$ есть функция выбора.

Пусть теперь в базисе B представима некоторая функция выбора $V(x_1, x_2, y)$. Заметим, что функция $V(x_1, V(x_2, x_3, y), y_1)$ производит выбор уже среди трех переменных x_1, x_2, x_3. Продолжая таким образом, можно построить функцию, которая производит выбор среди произвольного числа k переменных. Такую функцию обозначим $V(x_1, \ldots, x_k, y)$.

Выберем $S = S(n)$ таким образом, чтобы любая функция из $T(n)$ была реализуема некоторой СФЭ в базисе B сложности не более S. Построим теперь универсальную схему $UC(n, S)$ в базисе B, которая моделирует каждую схему сложности не более S в базисе B. Очевидно, такая схема реализует универсальную функцию $UF(T(n))$. Опишем возможную конструкцию схемы $UC(n, S)$.

Если функция имеет сложность $t < S$, то ее можно реализовать схемой сложности S. Для этого достаточно добавить $S - t$ внутренних вершин, не связанных путем с выходом схемы. При этом мы несколько расширяем прежнее понятие схемы, но это не мешает конструируемой схеме $UC(n, S)$ быть универсальной схемой в прежнем смысле слова.

Перенумеруем внутренние вершины моделируемой схемы числами от I до S в порядке вычисления функции, реализуемой схемой. На каждый из входов вершины с номером i ($1 \leq i \leq S$) в этой схеме подается либо одна из переменных $x_1, \ldots, x_n$, либо выход одной из вершин I, ..., i-I.

Универсальная схема $UC(n, S)$ состоит из S последовательно соединенных блоков. i-й блок A_i этой схемы вычисляет функцию i-й вершины моделируемой схемы при помощи переменных y. Входами блока A_i являются переменные $x_1, \ldots, x_n$, выходы блоков $A_1, \ldots, A_{i-1}$ и переменные y. Строение блока A_i показано на рис.4.I. $\varphi_1, \ldots, \varphi_r$ на этом рисунке обозначают базисные функции, $a_1, \ldots, a_{i-1}$ – выходы блоков соответственно $A_1, \ldots, A_{i-1}$.

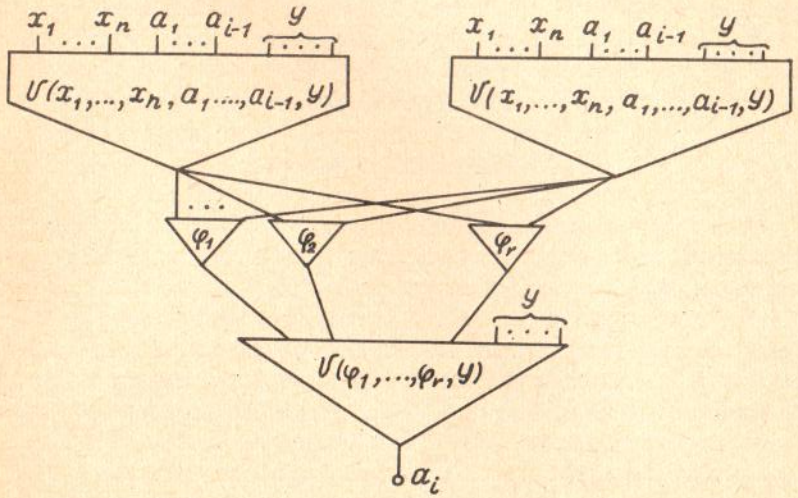

Рис.4.I. Строение блока A_i универсальной схемы

Количество подблоков выбора на верхнем ярусе блока A_i равно максимальному числу переменных базисных функций. Если некоторая базисная функция g_j имеет меньшее число переменных, то на вход подблока g_j подаются выходы не всех, а только первых подблоков выбора верхнего яруса.

Очевидно, что взяв достаточное число переменных y и подобрав их значения, можно добиться того, что схема $UC(n,s)$ моделирует произвольную схему сложности $t \le s$. □

Теорема 4.2. Сложность универсальной схемы для множества схем сложности не более $s(n)$ не превышает $O(s(s+n))$.

Для доказательства можно воспользоваться конструкцией универсальной схемы $UC(n,s)$, описанной при доказательстве предыдущей теоремы. Она содержит s блоков. Ввиду соотношения

$$v(x_1,\dots,x_k,x_{k+1},\dots,x_n) = v(v(x_1,\dots,x_k), v(x_{k+1},\dots,x_n))$$

каждый блок имеет сложность $O(n+s)$. □

Универсальная схема может реализовать универсальную функцию $UF(T(n))$, как это видно из доказательства теоремы 4.I, но эта схема может оказаться не оптимальной для универсальной функции. Действительно, универсальная схема по определению должна воспроизводить структуру каждой из моделируемых схем. При реализации же универсальной функции $UF(\mathcal{F})$ этого не требуется: можно для каждой функции $f \in \mathcal{F}$ выбирать (возможно, не оптимальную) схему, удобную для моделирования. В работе Л.Валианта [89] построены оптимальные по порядку схемы для универсальных функций (сложности $O(n + s\log s)$).

4.2. Универсальные формулы

Для построения универсальных формул конструкция, описанная при доказательстве теоремы 4.I, равно, как и конструкция Валианта, не годится, поскольку в этой конструкции выходы блоков "ветвятся" (см. рис.4.I). Устранение же ветвлений путем распараллеливания блоков приводит к экспоненциальному возрастанию сложности. Для преодоления этой трудности приведем сначала все формулы к каноническому виду.

Формула в базисе $\{0,1,\wedge,\vee,^-\}$ называется приведенной, если она не содержит подформул вида $\bar{\bar{u}}$ и отрицания в ней допускаются лишь над знаками переменных. Приведенной формуле естественным образом сопоставляется бинарное дерево, в котором листьям приписаны символы алфавита $\{0,1,x_1,\dots,x_n,\bar{x}_1,\dots,\bar{x}_n\}$, а внутренним вершинам $\wedge$ или $\vee$.

Формула в базисе $\{\wedge,\vee\}$ называется синхронной, если в дереве этой формулы для каждой вершины все пути, ведущие в вершину из листьев, имеют одинаковую длину.

Приведенная синхронная формула называется регулярной, если в дереве этой формулы всем внутренним вершинам четных ярусов приписана $\vee$, а нечетных ярусов - $\wedge$. Очевидно, для каждой формулы существует эквивалентная регулярная формула. Ее сложность оценивается в следующей теореме:

Теорема 4.3 [86]. Если базис B состоит из двуместных булевых функций, то для любой формулы в базисе B сложности s существует эквивалентная ей регулярная формула сложности $O(s^{2/(\log 3-1)})$.

Регулярные формулы одинаковой глубины имеют изоморфные деревья и могут отличаться лишь символами, приписанными листьям. Такая стандартность облегчает построение для них универсальных формул.

Лемма 4.I. Для класса функций из $P_2^n(x)$, реализуемых регулярными формулами сложности s, в базисе $\{\wedge,\vee,^-\}$ существует универсальная формула сложности $O(ns)$.

Доказательство. Достаточно вместо каждого листа регулярной формулы подставить формулу, реализующую функцию выбора $v(x_1,\dots,x_n,\bar{x}_1,\dots,\bar{x}_n,0,1,y)$ (для разных листьев непересекающиеся множества свободных переменных). Каждая такая формула имеет сложность $O(n)$.

Обозначим символом $u(n,s)$ универсальную функцию множества функций $f(x)$, имеющих формульную сложность не более $s(n)$ (в некотором полном двуместном базисе B, который считается зафиксированным). Напомним, что L_φ обозначает формульную сложность.

Теорема 4.4. В произвольном полном двуместном базисе

$$L_\varphi(u(n,s)) = O(ns^{2/(\log 3-1)}).$$

Доказательство. Пусть функция $f \in P_2^n(x)$ реализуется формулой сложности не более s в базисе B. В силу теоремы 4.3 она реализуется регулярной формулой сложности не более $O(s^{2/(\log 3-1)})$. В силу леммы 4.I для таких формул есть универсальная формула сложности $O(ns^{2/(\log 3-1)})$ в базисе $\{\wedge,\vee,^-\}$. В силу теоремы о сравнении базисов [44а] эту универсальную формулу можно "перевести" в базис B, не увеличивая по порядку сложность.

4.3. Универсальные схемы в неполных базисах

Среди неполных базисов наибольший интерес с позиций нижних оценок сложности представляет монотонный базис $\{\wedge, \vee\}$. Оказывается, что в этом базисе возможно практически такое же построение универсальных формул, что и в случае полного базиса. Это оказывается возможным благодаря переносу теоремы 4.3 на случай базиса $\{\wedge, \vee\}$. Такой перенос сделан в [95].

При доказательстве теоремы 4.I мы видели, что если универсальная функция $U(T(n))$ реализуема в базисе B, то существует экономная реализация универсальной функции. Поэтому естественно искать высокие НОСЛ в тех (неполных) базисах, в которых не реализуема универсальная функция.

Рассмотрим в качестве примера такого базиса множество $B = \{K(x,y), D(x,y)\}$ функций трехзначной логики из п.2.6 (см. табл.2.I). В этом базисе функция выбора не представима, поскольку, например, при $x_2 = 2$ любая функция из $[B]$ равна 2, а не x_1 при некотором y. Поэтому в силу теоремы 4.I универсальная функция $U(T(n))$ не реализуема в базисе B. Это дает основания рассчитывать на высокую нижнюю оценку сложности. Такая оценка (величины $2C_n^{[n/2]} - 1$) действительно получена в п.2.6.

Примеры неполных базисов с экспоненциальной нижней оценкой сложности построены довольно давно (см. [45], а также п.2.6). В булевском случае, то есть при $k = 2$, построение таких примеров вызвало значительные трудности и удалось [I, 38] только благодаря разработке принципиально новых методов доказательства НОСЛ, не сводящихся к нижней оценке ширины. Почему при $k = 2$ нельзя получить высокие НОСЛ в неполных базисах путем оценки снизу ширины? Предлагаемое нами объяснение состоит в том, что в булевском случае замкнутые классы T, не допускающие универсальной функции, очень "жидкие" и потому содержат лишь очень простые функции. Поясним это подробнее.

Перечислим некоторые замкнутые классы из диаграммы Поста, следуя обозначениям работы [53].

Классы $O_1 - O_9$ – это самые "бедные" классы. Функции этих классов имеют не более одной существенной переменной. Очевидно

Утверждение 4.I. В любом базисе класса O_i $(i = 1, \ldots, 9)$
$$L(O_i) = O(1) .$$

В классах S_1, S_3, S_5, S_6 представимы все логические суммы $\bigvee_{j=1}^{n} x_j$ и в зависимости от нижнего индекса некоторые из констант 0 и I. Классы P_1, P_3, P_5, P_6 двойственны классам S_1, S_3, S_5, S_6.

Утверждение 4.2. В любом базисе класса S_i (соответственно P_i) $(i \in \{I,3,5,6\})$
$$L(S_i(n)) = O(n) , \quad L(P_i(n)) = O(n) .$$

Классы L_1, L_2, L_3, L_4, L_5 задаются соответственно базисами $\{x \oplus y, 1\}$, $\{x \oplus y \oplus 1\}$, $\{x \cdot y\}$, $\{x \oplus y \oplus z\}$ и $\{x \oplus y \oplus z \oplus 1\}$. Очевидно

Утверждение 4.3. В любом базисе класса L_i (i = I, ..., 5)
$$L(L_i(n)) = O(n) .$$

Классы D_2, F_2^∞ и F_6^∞ имеют соответственно базисы $\{xy \vee yz \vee xz\}$, $\{x \vee yz\}$ и $\{x(y \vee z)\}$.

Лемма 4.2. В замкнутых классах $[D_2 \cup \{0,1\}]$, $[F_2^\infty \cup \{0,1\}]$ и $[F_6^\infty \cup \{0,1\}]$ представимы конъюнкция и дизъюнкция.

Доказательство. В классе D_2 представима функция $xy \vee yz \vee xz$. При $z = 0$ она равна xy, а при $z = I$ равна $x \vee y$. Аналогично поступаем с классами F_2^∞ и F_6^∞.

Следствие. Замкнутые классы D_2, F_2^∞, F_6^∞ и все включающие их замкнутые классы содержат универсальные функции.

Теорема 4.5. При $k = 2$, если замкнутый класс T не содержит универсальной функции $U(T(n))$, то для произвольного базиса этого класса $L(T(n)) = O(n)$.

Доказательство. Из следствия леммы 4.2 и диаграммы Поста (см., например, [53]) видно, что замкнутыми классами, не содержащими универсальной функции, могут быть лишь классы S_i, P_i (i = I,3,5,6), $L_1 - L_5$ и $O_1 - O_9$. Но в силу утверждений 4.I–4.3 функции этих классов имеют сложность $O(n)$. □

4.4. Более экономные конструкции универсальных схем

Конструкция универсальной схемы $UC(n,s)$, предложенная при доказательстве теоремы 4.I, служит для доказательства существования универсальных функций. По сложности эта конструкция далеко не оптимальна. Укажем более экономные конструкции.

Под глубиной схемы в этом параграфе понимается длина самого длинного ориентированного пути в схеме.

Утверждение 4.4 [89]. Существует схема сложности $O(ds\log s)$ и глубины $O(d\log s)$, которая универсальна для множества схем сложности $s(n)$ и глубины d.

Доказательство основано на применении конструкции перестановочной схемы (см., например, [82]), которая позволяет на M выходах получать произвольную перестановку M входов за счет использования $O(M\log M)$ дополнительных входов.

Конструкция из утверждения 4.4 дает экономную схему при малых значениях глубины, а именно, при $d\log s = O(s)$. Если же глубина никак не ограничена (точнее, ограничена сверху только сложностью $s(n)$), оценка утверждения 4.4 даже уступает оценке теоремы 4.2. Укажем теперь более экономную конструкцию универсальной схемы при произвольной глубине.

Мы проведем оценку сложности универсальной схемы в терминах памяти схем. Введем сначала понятие памяти схем.

Перенумеруем внутренние вершины СФЭ сложности s натуральными числами от $n+1$ до $n+s$ в порядке вычисления функции схемы в вершинах схемы. Такие нумерации будем называть правильными. Точнее, нумерация π вершин схемы числами $n+1,\dots,n+s$ называется правильной, если из условия $\pi(u)>\pi(v)$ следует, что вершина u не является предком вершины v. Правильная нумерация, вообще говоря, далеко не единственна. СФЭ вместе с правильной нумерацией вершин будем называть неветвящейся программой (НП). Полюсы НП занумеруем числами от I до n в соответствии с индексом приписанной переменной.

НП можно представить в виде последовательности s команд вида

$$a := b \circ c ,$$

где a, b, c – некоторые переменные, причем b и c либо встречались в левой части предшествующих команд, либо совпадают с одной из переменных $x_1,\dots,x_n$, а $\circ$ есть одна из базисных операций (здесь для простоты предполагается, что базис состоит из двуместных функций).

Величина памяти НП на i-м шаге (обозначение $M(i)$) – это число вершин с номерами не более i, из которых идут дуги в вершины с номерами больше i. Содержательно, это число булевых переменных, которые нужно хранить в памяти, поскольку они понадобятся на

последующих шагах вычисления. Память НП p (обозначение $M(p)$) равна по определению $\max_{n+1\le i\le n+s} M(i)$. Память схемы S (обозначение $M(S)$) равна по определению $\min M(p)$, где минимум берется по всем НП, получающимся из схемы S при правильных нумерациях.

Положим $M(n,s,d)=\max M(S)$, где максимум берется по всем схемам S с n входами, имеющим сложность не более s и глубину не более d.

Теорема 4.6. Существует универсальная схема сложности $O(\min(sM, dM\log M))$, которая универсальна для множества схем сложности не более $s(n)$ и глубины не более $d(M=M(n,s,d))$.

Доказательство. Преобразуем схему из доказательства теоремы 4.I (см. рис.4.I), оставив на входах блока A_i лишь M переменных из числа величин $x_1,\dots,x_n,a_1,\dots,a_{i-1}$, которые могут использоваться при последующих вычислениях. Далее, после блока, вычисляющего a_i, добавим блок, который определяет, какую переменную из числа M хранившихся переменных замещает переменная a_i. Сложность такого блока есть $O(M)$. Поэтому сложность всей схемы есть $O(sM)$. Аналогично преобразуем конструкцию из утверждения 4.4. □

4.5. Универсальные синхронные схемы

Поскольку не доказано, что синхронные схемы полиномиально эквивалентны обычным схемам, то возникает вопрос, существуют ли экономные универсальные синхронные схемы. В этом параграфе дается положительный ответ на этот вопрос.

Преобразуем универсальную схему $UC(n,s)$ из доказательства теоремы 4.I так, чтобы сделать ее синхронной. Для этого достаточно добиться, чтобы все входы каждого подблока модифицированного блока A_i' (см. рис.4.I) вычислялись бы синхронными схемами одинаковой глубины. Покажем, как можно этого достичь. Будем считать, что выходами модифицированного блока A_i' являются наряду с a_i также все входы этого блока. Очевидно, эти дополнительные выходы нет необходимости вычислять, поскольку они уже имеются на входе блока. Дело только за тем, чтобы соблюсти условие синхронности. Для этого достаточно, например, протянуть от входа x блока A_i' до его выхода x цепочку вершин, каждая из которых производит тождествен-

ное преобразование вида $\varphi(z,z)=z$ (в качестве элемента φ можно взять конъюнкцию или дизъюнкцию). Аналогично следует поступить с переменными y, которые подаются на последующие подблоки блока A_i'. Кроме того, через блок A_i' надо пропустить переменные y, которые понадобятся лишь в последующих блоках $A_{i+1}', \ldots, A_s'$. Число таких переменных y по порядку не превышает $(n+s)s$.

Длины добавленных цепочек не превышают глубины блока A_i, то есть $\log(n+i)$ по порядку. Итак, в i-й блок всего добавляется $s(n+s)\log(n+s)$ вершин (по порядку). Поскольку число блоков A_i равно s, то тем самым доказана

Теорема 4.7. Сложность синхронной схемы, универсальной для класса синхронных схем сложности не более $s(n)$, не превышает по порядку величины $s^2(n+s)\log(n+s)$.

4.6. Невозможность доказательства высоких нижних оценок сложности для некоторых моделей вычислений в классе универсальных доказательств НОСЛ

Универсальные доказательства НОСЛ были определены в предыдущей главе. Согласно определению с каждым универсальным доказательством НОСЛ связывается некоторое множество $\mathfrak{S}$ схем, реализующих покрываемые этим доказательством ч.б.ф. из некоторого множества $\mathcal{F}$. Множество $\mathfrak{S}$ полностью характеризует доказательство. Поэтому универсальное доказательство можно идентифицировать тем же символом $\mathfrak{S}$. Величина нижней оценки сложности, устанавливаемой универсальным доказательством $\mathfrak{S}$, согласно определению, не превосходит по порядку величины $L(UC(\mathfrak{S}))\cdot L(\mathfrak{S})$, где $L(UC(\mathfrak{S}))$ есть сложность минимальной универсальной схемы множества $\mathfrak{S}$, а $L(\mathfrak{S})$ есть максимальная сложность схем множества $\mathfrak{S}$.

Мы видели в предыдущей главе, что сложность $L(UC(\mathfrak{S}))$ универсальной схемы множества $\mathfrak{S}$ может быть экспоненциально большой для целого ряда моделей с ограничениями (монотонные схемы для вычисления полиномов, схемы без нулевых цепей, схемы ограниченной глубины, схемы в некоторых неполных базисах). Это является предпосылкой доказательства высоких НОСЛ для этих моделей. В то же время для таких моделей, как схемы из функциональных элементов, формулы, синхронные схемы, теоремы 4.2, 4.4, 4.6, 4.7 говорят о существовании экономных универсальных схем. Это означает, что, ограничившись эффективными доказательствами НОСЛ, для этих моделей невозможно установить высокие НОСЛ.

Теорема 4.8. Для произвольного множества $\mathfrak{S}$ схем с полюсами из множества $X(|X|=n)$ в классе схем из функциональных элементов универсальным доказательством $\mathfrak{S}$ не выводимы нижние оценки сложности, превосходящие по порядку $s^2(s+n)$, если $L(\mathfrak{S})\le s(n)$.

Доказательство. В силу утверждения I.I универсальная схема $UC(n,s)$ является универсальной и для множества $\mathfrak{S}$. Поэтому в силу теоремы 4.2 $L(UC(\mathfrak{S}))=O(s(n+s))$. Тогда из определения универсального доказательства $\mathfrak{S}$ следует, что максимальная НОСЛ, выводимая универсальным доказательством $\mathfrak{S}$, не превышает по порядку $s^2(s+n)$.

Аналогично доказывается

Теорема 4.9. Для произвольного множества $\mathfrak{S}$ схем с полюсами из множества $X(|X|=n)$ в классе синхронных схем универсальным доказательством $\mathfrak{S}$ не выводимы нижние оценки сложности, превосходящие по порядку $s^3(s+n)\log(s+n)$, если $L(\mathfrak{S})\le s(n)$.

4.7. Обсуждение результатов главы

Результаты этой главы позволяют ответить на второй и третий вопросы, сформулированные в п.I.I.4 главы I.

Начнем с третьего вопроса. Это вопрос о прогнозировании возможностей доказательства высоких НОСЛ. Изучение конструкции универсальной схемы $UC(n,s)$, описанной в п.4.I, показывает, что эта схема имеет большую глубину (в смысле чередования знаков операций), содержит нулевые цепи (в случае базиса $\{\wedge,\vee,^-\}$) и требует реализуемости функции выбора. Поэтому, если наложить ограничение на глубину схем, запретить нулевые цепи или исключить возможность реализации функции выбора за счет неполноты базиса, появятся большие трудности при построении универсальных схем. Если эти трудности не удастся быстро преодолеть, нужно попробовать доказывать высокие НОСЛ для универсальных схем. Построения главы 3 показывают, что если это в принципе возможно, то делается без больших осложнений. С другой стороны, конструкции этой главы говорят о том, что если экономная универсальная схема существует, то ее можно построить без труда.

Одним словом, для универсальных схем одна из двух противоположных задач (построение экономной универсальной схемы и доказательство высоких НОСЛ для нее) решается несложно (и тем самым исклю-

чает возможность решения другой). Поэтому, столкнувшись с новой моделью вычислений, полезно изучить сложность универсальных схем для этой модели. Если эта сложность окажется малой, то задача доказательства высоких НОСЛ для этой модели скорее всего, встретит очень большие трудности. Если же универсальная схема окажется экспоненциально сложной, то это дает хорошие шансы эффективного доказательства высоких НОСЛ.

Результаты этой главы дают объяснение еще одному феномену из теории сложности. Он относится к сравнению схем без нулевых цепей с монотонными схемами в базисе $\{\wedge, \vee\}$. Ясно, что последние являются частным случаем схем без нулевых цепей. Для схем без нулевых цепей установлены [37, I5, I6] высокие НОСЛ. Поэтому, казалось бы, они должны тем более получаться для частного случая этих схем. Однако, как это ни парадоксально, доказательство высоких НОСЛ для частного случая оказалось существенно труднее [I, 38], чем для более общего случая. Чем это объяснить? Объяснение опять-таки получается при сравнении сложностей универсальных схем для этих двух моделей вычислений. В то время как в классе схем без нулевых цепей универсальные схемы имеют экспоненциальную сложность (см. главу 3), в классе монотонных схем сложность есть всего лишь $O(s(n+s))$ (см. п.4.3). Поэтому для получения высоких НОСЛ для монотонных схем надо выйти за пределы класса универсальных доказательств, а сделать это совсем не легко.

Вспомним теперь второй вопрос из п.I.I.4. Он предлагает объяснить, почему для одних моделей вычислений высокие НОСЛ доказываются, а для других это не удается сделать. Частично ответ на этот вопрос уже был дан в главе 3. Он говорил о том, что высокие НОСЛ удается доказать тогда, когда это удается сделать для универсальных схем. Данная глава позволяет ответить на этот вопрос не только на качественном, но и на количественном уровне. Теоремы 4.8 и 4.9 дают количественные пределы для величины НОСЛ, если ограничиться универсальными доказательствами. Поскольку при эффективных доказательствах величины $s(n)$ в теоремах 4.8 и 4.9 есть $O(n)$, то эти теоремы говорят о невозможности доказать НОСЛ, превышающие по порядку величины n^3 и $n^4 \log n$ соответственно для схем и синхронных схем. Эти величины на качественном уровне согласуются с установленными до сих пор нижними оценками (соответственно cn и $cn \log n$).

Разумеется, результаты о невыводимости высоких НОСЛ, доказанные в этой главе, распространяются только на описанные в этой работе модели, а именно, на универсальные доказательства НОСЛ. Поэтому не следует абсолютизировать выводы, сделанные в предыдущем абзаце. Их следует рассматривать скорее как объяснение трудностей доказательства высоких НОСЛ. Объяснение состоит в трудностях выхода за пределы класса универсальных доказательств. До сих пор это никому не удавалось сделать (в случае схем и формул в полном базисе).

Л И Т Е Р А Т У Р А

I. А н д р е е в А.Е. Об одном методе получения нижних оценок сложности индивидуальных монотонных функций // ДАН СССР. – I985. – Т.282, № 5. – С.I033–I037.

2. Б а р з д и н ь Я.М. Сложность распознавания симметрии на машинах Тьюринга // Проблемы кибернетики. – М., I965. – Вып.I5. – С.245–248.

3. Б е л ь т ю к о в А.П. Нижние оценки сложности для машинных моделей вычислений // Зап. научн. семинаров ЛОМИ АН СССР. –Л., I982. – Т.II8. – С.4–24.

4. В а с и л ь е в Ю.Л., Г л а г о л е в В.В. Метрические свойства дизъюнктивных нормальных форм // Дискретная математика и математические вопросы кибернетики / Под ред. С.В.Яблонского, О.Б.Лупанова. – М., I974. – С.99–I48.

5. Г о р е л и к Е.С. О сложности реализации элементарных конъюнкций и дизъюнкций в базисе $\{x \mid y\}$ // Проблемы кибернетики.– М., I975. – Вып.26. – С.27–36.

6. Г р и г о р ь е в Д.Ю. Об одной нижней оценке сложности вычисления семейства дизъюнкций в монотонном базисе // Зап. научн. семинаров ЛОМИ АН СССР. – Л., I977. – Т.68. – С.I9–25.

7. Г р и г о р ь е в Д.Ю. Нижние оценки в алгебраической сложности вычислений // Зап. научн. семинаров ЛОМИ АН СССР. – Л., I982. – Т.II8. – С.25–82.

8. Ж у р а в л е в Ю.И. Теоретико-множественные методы в алгебре логики // Проблемы кибернетики. – М., I962. – Вып.8. – С.5–44.

9. Ж у р а в л е в Ю.И. Оценки сложности алгоритмов построения минимальных дизъюнктивных нормальных форм для функций алгебры логики // Дискретный анализ. – Новосибирск, I964. – Вып.3. –С.4I–77.

I0. Ж у р а в л е в Ю.И. Локальные алгоритмы вычисления информации, I, II // Кибернетика. – Киев, I965. – № I. – С.I2 – I9; I966. – № I. – С.I–II.

II. Ж у р а в л е в Ю.И. Алгоритмы построения минимальных дизъюнктивных нормальных форм для функций алгебры логики // Дискретная математика и математические вопросы кибернетики / Под ред. С.В.Яблонского, О.Б.Лупанова. – М., I974. – С.67–98.

I2. К л о с с Б.М., М а л ы ш е в В.А. Оценки сложности некоторых классов функций // Вестн. Моск. ун-та. Серия матем., мех. – I965. – № 4. – С.44–5I.

I3. К л о с с Б.М. Оценки сложности решения систем линейных уравнений // ДАН СССР. – I966. – Т.I7I, № 4. – С.78I–783.

I4. К о с о в с к и й Н.К. Примеры простых переборных задач с полиномиальными нижними границами времени их решения // Кибернетика. – Киев, I984. – № 2. – С.I09–II0.

I5. К у з н е ц о в С.Е. Схемы из функциональных элементов без нулевых цепей в базисе $\&$, $\vee$, $-$ // Известия вузов. Математика. – Казань, I98I. – № 5. – С.56–63.

I6. К у з н е ц о в С.Е. Влияние нулевых цепей на сложность контактных схем // Вероятностные методы и кибернетика. – Казань, I984. – Вып.20. – С. 6I–87.

I7. Л у п а н о в О.Б. О реализации функций алгебры логики формулами из конечных классов (формулами ограниченной глубины) в базисе $\&$, $\vee$, $-$ // Проблемы кибернетики. – М., I96I. – Вып.6. – С. 5–I4.

I8. Л у п а н о в О.Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. – М., I970. – Вып.23. – С. 43 – 8I.

I9. Л у п а н о в О.Б. Об асимптотических оценках сложности управляющих систем // Международный конгресс математиков в Ницце. I970. Доклады советских математиков. – М., I972. – С.I62–I67.

20. Л у п а н о в О.Б. О методах получения оценок сложности и вычисления индивидуальных функций // Дискретный анализ. – Новосибирск, I974. – Вып. 25. – С. 3–I8.

2I. Л у п а н о в О.Б. О реализации функций алгебры логики схемами из функциональных элементов "ограниченной глубины" в базисе $\&$, $\vee$, $-$ // Труды ВЦ АН СССР. – М., I977. – Вып.2. – С.3–8.

22. М а л ы ш е в В.А. Класс "почти всех" функций с нелинейной сложностью при реализации П-схемами // Проблемы кибернетики. – М., I967. – Вып. I9. – С. 299–307.

23. Н е ч и п о р у к Э.И. Об одной булевской функции // ДАН СССР. – I966. – Т. I69, № 4. – С. 765–766.

24. Нечипорук Э.И. Об одной булевской матрице //Проблемы кибернетики. – М., 1969. – Вып. 21. – С. 237–241.

25. Нигматуллин Р.Г. Проблема нижних оценок сложности и теория NP -полноты // Известия вузов. Математика. – Казань, 1981. – № 5. – С.17–26.

26. Нигматуллин Р.Г. Сложность булевых функций. – Казань, Изд-во Казан. ун-та, 1983. – 208 с.

27. Нигматуллин Р.Г. Сложность универсальных функций и нижние оценки сложности // Известия вузов. Математика. – Казань, 1984. – № 11. – С. 10–20.

28. Нигматуллин Р.Г. К задаче отыскания максимальных нижних оценок сложности // Седьмая всесоюзная конференция по математической логике. Тезисы докладов. – Новосибирск, 1984. – С. 121.

29. Нигматуллин Р.Г. Нижние оценки сложности монотонного вычисления полиномов и универсальные схемы // Известия вузов. Математика. – Казань, 1985. – № 8. – С. 35–42.

30. Нигматуллин Р.Г. Нижние оценки сложности и сложность универсальных схем // УII Всесоюзная конференция "Проблемы теоретической кибернетики". Тез. докл. – Иркутск, 1985. – Ч.I. – С. 150–151.

31. Нигматуллин Р.Г. Нижние оценки сложности суть нижние оценки для универсальных схем? – Казань, 1985. – 18 с. – Библиогр.: 13 назв. – Рукопись представлена Казанским ун-том. Деп. в ВИНИТИ 22.08.85, № 6257–85 Деп.

32. Нигматуллин Р.Г. Экспоненциальное влияние константы ноль на сложность вычисления универсальных полиномов // Вероятностные методы и кибернетика. – Казань, 1985. – Вып. 21. – С. 75–85.

33. Нигматуллин Р.Г. Два класса доказательств нижних оценок сложности // ДАН СССР. – 1987. – Т.294, № 2. – С.272–275.

34. Нигматуллин Р.Г. Экспоненциальные нижние оценки сложности и пошагово моделирующие схемы // Кибернетика. – Киев, 1987. – № 4. – С. 25–28, 35.

35. Окольнишникова Е.А. Монотонная булева система с квадратичной сложностью реализации в базисе $\{\vee, \&, 0, 1\}$// Дискретный анализ. – Новосибирск, 1984. – вып.41. – С. 81–98.

36. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 594 с.

37. Пулатов А.К. Нижние оценки сложности реализации характеристических функций групповых кодов П-схемами // Комбинаторно-алгебраические методы в прикладной математике. – Горький, 1979. – С. 81–95.

38. Разборов А.А. Нижние оценки монотонной сложности некоторых булевых функций // ДАН СССР. – 1985. – Т.281, № 4. – С. 798–801.

39. Редькин Н.П. Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. – М., 1970. – Вып. 23. – С. 83–101.

40. Редькин Н.П. О минимальной реализации двоичного сумматора // Проблемы кибернетики. – М., 1981. – Вып.38. –С.181–216.

41. Романов А.М. Оценка длины кратчайшей дизъюнктивной нормальной формы для отрицания характеристической функции кода Хэмминга // Дискретный анализ. – Новосибирск, 1983. – Вып.39. – С. 88–97.

42. Слисенко А.О. Сложностные задачи теории вычислений // УМН. – 1981. – Т.36, вып.6. – С. 21–103.

43. Сопруненко Е.П. О минимальной реализации некоторых функций схемами из функциональных элементов // Проблемы кибернетики. – М., 1965. – Вып. 15. – С. 117–135.

44. Субботовская Б.А. О реализации линейных функций формулами в базисе $\&$, $\vee$, $-$ // ДАН СССР. – 1961. – Т. 136, №3. – С. 553–555.

44а. Субботовская Б.А. О сравнении базисов при реализации функций алгебры логики формулами // ДАН СССР. – 1963. – Т.149, № 4. – С. 784–787.

45. Ткачев Г.А. О сложности реализации одной последовательности функций k -значной логики // Вестн. Моск. ун-та. Серия выч. мат. и киб. – 1977. – № 1. – С. 45–57.

46. Ткачев Г.А. О сложности реализации одной последовательности булевых функций схемами из функциональных элементов и П-схемами при дополнительных ограничениях на структуру схем // Комбинаторно-алгебраические методы в прикладной математике. – Горький, 1980. – С. 161–207.

47. Улиг Д. Об одной функции алгебры логики, имеющей много подфункций и небольшую сложность реализации // Проблемы кибернетики. – М., 1979. – Вып.35. – С. 133–140.

48. Храпченко В.М. О сложности реализации линейной функции в классе П-схем // Матем. заметки. – 1971. – Т.9, № 1. – С. 35–40.

49. Храпченко В.М. Об одном методе получения нижних оценок сложности П-схем // Матем. заметки. – 1971. – Т.10, № 1. – С. 83–92.

50. Храпченко В.М. Нижние оценки сложности схем из функциональных элементов (обзор) // Кибернетический сборник. – М., 1984. – Вып. 21. – С. 3–54.

51. Шоломов Л.А. Об одной последовательности сложно реализуемых функций // Матем. заметки. – 1975. – Т. 17, № 6. – С. 957–966.

52. Яблонский С.В. Об алгоритмических трудностях синтеза минимальных контактных схем // Проблемы кибернетики. – М., 1959. – Вып. 2. – С. 75–121.

53. Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б. Функции алгебры логики и классы Поста. – М.: Наука, 1966. – 119 с.

54. Яблонский С.В. Обзор некоторых результатов в области дискретной математики // Информационные материалы / Науч – ный совет по комплексной проблеме "Кибернетика". – М., 1970. – Вып. 5 (42): Всесоюзная конф. по проблемам теорет. киберн. (Новосибирск, июнь 1969): Доклады (пленарные и секционные). – С. 5–15.

55. Blum N. A Boolean function requiring 3n network size // Theoret. Comp. Sci. – 1984. – V. 28. – P. 337–345.

56. Cardot C. Quelques resultats sur l'applications de l'algebre de Boole a la synthese des circuits a relais //Annales des Telecommunications. – 1952. – V. 7, N 2. – P. 75–84.

57. Ehrenfeucht A. Practical decidability. Report CU-CS-008-72. – Department of Computer Science, University of Colorado. – 1972.

58. Fischer M.J., Meyer A.R., Paterson M.S. Ω (nlogn) lower bounds on length of Boolean formulas // SIAM J. Comput. – 1982. – V. 11, N 3. – P. 416–427.

59. Furst M., Saxe J.B., Sipser M. Parity, circuits and the polynomial-time hierarchy // Proc. 22nd IEEE Symp. Found. Comp. Sci. – 1981. – P. 260–270.

60. Harper L.H., Savage J.E. On the Complexity of the marriage problem // Adv. Math. – 1972. – V. 9, N 3. – P.299–312.

61. Harper L.H., Savage J.E. Complexity made simple // Colloquio Internazionale sulle Teorie Combinatorie. Roma. 1973. – Roma, 1976. – Tomo II, Atti dei Convegni Lincei N 17. – P. 253–262.

62. Harper L.H., Hsieh W.N., Savage J.E. A class of Boolean functions with linear combinational complexity // Theoret. Comp. Sci. – 1975. – V. 1, N 2. – P. 161–183.

63. Harper L.H. A nlogn lower bound on synchronous combinational complexity // Proc. Amer. Math. Soc. – 1977. – V. 64, N 2. – P. 300–306.

64. Harper L.H., Savage J.E. Lower bounds on synchronous combinational complexity // SIAM J. Comput. – 1979.– V. 8, N 2. – P. 115–119.

65. Hennie F.C. One-tape, off-line Turing machine computations // Inform. and Control. – 1965. – V. 8, N 6. –P.553–578.

66. Hodes L., Specker E. Lengths of formulas and elimination of quantifiers // Contribitions to mathematical Logic. – Amsterdam, 1968. – P. 175–188. (Русский перевод: Кибернетический сборник. – М., 1973. – Вып.10. С.99–113).

67. Hunt H.B. III. On the time and tape complexity of languages // Proc. 5th ACM Symp. on Theory of Computing. – 1973. – P. 10–19.

68. Jerrum M.R., Snir M. Some exact complexity results for straight-line computations over semirings // Journal of the ACM. – 1982. – V. 29. – P. 874–898.

69. Klawe M., Paul W., Pippenger N., Yannakakis M. On monotone formulae with restricted depth // Proc. 16th ACM Symp. on Theory of Computing. – 1984. – P.480–487.

70. Lamagna E.A., Savage J.E. Combinational complexity of some monotone functions // Proc. 15th IEEE Symp. on Switching and Automata Theory. – New Orlean, 1974. – P.140–144.

71. Mehlhorn K. Some remarks on Boolean sums // Acta Informatica. – 1979. – V. 12, N 4. – P. 371–375. (Русский перевод: Кибернетический сборник. – М., 1981. – Вып.18. – С.39–45).

72. Mehlhorn K., Galil Z. Monotone switching circuits and Boolean matrix product // Computing. – 1976. – V. 16, N 1-2. – P. 99–111.

73. Meyer A.R. Weak monadic second order theory of successor is not elementary recursive // Lecture Notes in Mathematics.

- Berlin, Springer, 1975. - V. 453: Proc. Symp. on Logic. - P. 132-154. (Русский перевод: Кибернетический сборник. - М., 1975. - Вып.12. - С.62-77).

74. Nigmatullin R.G. Are lower bounds on the complexity lower bounds for universal circuits?//Lecture Notes in Computer Science.- Berlin,Springer,1985.- V.199: Fundamentals of Computation Theory-. - P. 331-340.

75. Paterson M.S. Complexity of monotone networks for Boolean matrix product // Theoret. Comput. Sci. - 1975. - V. 1, N 1. - P. 13-20. (Русский перевод: Кибернетический сборник. - М., 1978. - Вып.15. - С.28-37).

76. Paul W. A 2.5n lower bound on the combinational complexity of Boolean functions // SIAM J. Comput. - 1977. - V.6, N 3. - P. 427-443. (Русский перевод: Кибернетический сборник. - М.,1979. - Вып.16. - С. 23-44).

77. Paul W.J. Realizing Boolean functions on disjoint sets of variables // Theoret. Comput. Sci. - 1976. - V. 2. - P. 383 - 396.

78. Pippenger N. On another Boolean matrix. IBM Research Report. - 1977. - V. 6914.

79. Pratt V.R. The power of negative thinking in multiplying Boolean matrices // SIAM J. Comput. - 1975. - V. 4, N 3. - P. 326-330.

80. Pudla'k P. Bounds for Hodes-Specker Theorem // Lecture Notes in Computer Science. - Berlin, Springer, 1984. - V. 171: Logic and Machines: Decision Problems and Complexity. - P.421-445.

81. Riordan J., Shannon C.E. The number of two-terminal series parallel networks // J. Math. Phys. - 1942. - V.21, N 2. - P. 83-93. (Русский перевод: Шеннон К.Э. Работы по теории информации и кибернетике. - М.: ИЛ, 1963. - С. 46-58).

82. Savage J.E. The complexity of computing. - New York: Wiley-Interscience, 1976. - 390 p.

83. Schnorr C.P. Zwei lineare untere Schranken fuer die Komplexitaet Boolescher Functionen // Computing. - 1974. - V. 13, N 2. - P. 155-171.

84. Schnorr C.P. The combinational complexity of equivalence // Theoret. Comput. Sci. - 1976. - V. 1, N 4. - P.289-295. (Русский перевод: Кибернетический сборник. - М., 1979. - Вып. 16. - С. 74-81).

85. Schnorr C.P. A lower bound on the number of additions in monotone computations // Theoret. Comput. Sci. - 1976. - V. 2, N 3. - P. 305-315. (Русский перевод: Кибернетический сборник. - М., 1981. - Вып.18. - С. 5-20).

86. Spira P.M. On time-hardware complexity tradeoffs for Boolean functions // Proc. 4th Hawaii Int. Symp. System Sciences. - 1971. - P. 525-527.

87. Stockmeyer L.J. The complexity of decision problems in automata theory and logic. Project MAC, Technical Report MIT. - Cambridge, Mass., 1974. - V. 133. - 224 p.

88. Stockmeyer L.J. On the combinational complexity of certain symmetric Boolean functions // Math. Systems Theory. - 1976/1977. - V. 10, N 4. - P. 323-336. (Русский перевод: Кибернетический сборник. - М., 1979. - Вып. 16. - С. 45-61).

89. Valiant L.G. Universal circuits // Proc. 8th ACM Symp. Theory Computing. - 1976. - P.196-203.

90. Valiant L.G. Negation can be exponentially powerful // Theoret. Comp. Sci. - 1980. - V. 12. - P. 303-314.

91. Valiant L.G. Exponential lower bounds for restricted monotone circuits // Proc. 15th ACM Symp. Theory Computing. - 1983. - P. 110-117.

92. Wegener I. Switching functions whose monotone complexity is nearly quadratic // Theoret. Comput. Sci. - 1979. - V. 9, N 1. - P. 83-97. (Русский перевод: Кибернетический сборник. - М., 1981. - Вып.18. - С. 55-74).

93. Wegener I. A new lower bound on the monotone network complexity of Boolean sums // Acta Informatica. - 1980. -V.13. - P. 109-114.

94. Wegener I. Boolean functions whose monotone complexity is of size $n^2/\log n$ // Theoret. Comput. Sci. - 1982. - V. 21, N 2. - P. 213-224. (Русский перевод: Кибернетический сборник. - М., 1984. - Вып.21. - С. 69-84).

95. Wegener I. Relating monotone formula size and monotone depth of Boolean functions. Interner Bericht 6/82. - Fachbereich Informatik, Universitaet Frankfurt, 1982. - 4 p.

96. Yablonski S.V. A survey of some results in the field of discrete mathematics // Proc. IFIP Congress, 1968, Edinburgh. - Amsterdam, 1969. - P. 266-270.

97. Yao A.C.C. Separating the polynomial-time hierarchy by oracles. Techn.Rep. of the Standford university. -1985. - 10 p.

ПРИЛОЖЕНИЕ

Список сокращений и обозначений

ДНФ – – дизъюнктивная нормальная форма
НОСЛ – нижняя оценка сложности
П-схема – параллельно-последовательная контактная схема
СФЭ – схема из функциональных элементов
ч.б.ф. – частичная булева функция
Оп (v) – операция, приписанная вершине v
Функ (v) – функция, вычисляемая в вершине v
Сын (v) – множество вершин, непосредственно следующих за вершиной v
Род (v) – множество вершин, непосредственно предшествующих вершине v
B^n – множество вершин единичного n -мерного куба
$\vee$-вершина – вершина с операцией $\vee$
$\wedge$-вершина – вершина с операцией $\wedge$
$L(S)$ – сложность схемы S
$L(f)$ – сложность функции f
L_Φ – сложность в классе формул
L_Π – сложность в классе П-схем
N_f – множество точек из B^n, в которых функция f из P_2^n равна I
P_2 – множество булевых функций
P_2^n – множество булевых функций n переменных
P_k – множество функций k -значной логики
(S,t) – схема с выходной вершиной t
(S,v) – подсхема схемы S, порождаемая вершиной v
$W(f)$ – ширина функции f
$W_e(f)$ – реберная ширина функции f
$W_c(f)$ – ширина сечения функции f
x – множество переменных булевой функции
y – множество дополнительных переменных функции
$Uf(F)$ – универсальная функция множества F
$UC(S)$ – универсальная схема множества схем S
$\rho(\tilde{\alpha},\tilde{\beta})$ – расстояние Хэмминга между $\tilde{\alpha}$ и $\tilde{\beta}$

ОГЛАВЛЕНИЕ

Рошаль Габдулхаевич Нигматуллин

НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ И СЛОЖНОСТЬ УНИВЕРСАЛЬНЫХ СХЕМ

Редактор А.М.Габитова
Корректор И.Г.Кондратьева
Обл.художника Г.Е.Трифонова