

Московский Государственный Университет
имени М.В. Ломоносова
Российская Академия Наук
Международная Академия Технологических Наук
Российская Академия Естественных Наук

Интеллектуальные Системы.

Теория и приложения

ТОМ 23 ВЫПУСК 3 * 2019

МОСКВА

Главный редактор: д.ф.-м.н., профессор В. Б. Кудрявцев

Редакционная коллегия:

д.ф.-м.н., проф. А. Е. Андреев (зам. главного редактора)
д.ф.-м.н., проф. Э. Э. Гасанов (зам. главного редактора)
к.ф.-м.н., доц. А. С. Строгалов (зам. главного редактора)
к.ф.-м.н., м.н.с. В. В. Осокин (ответственный секретарь)
д.ф.-м.н., проф. В. В. Александров, д.ф.-м.н., проф. С. В. Алешин, д.ф.-м.н., проф. Д. Н. Бабин, академик РАН, д.ф.-м.н., проф. Ю. Л. Ершов, академик РАН, д.ф.-м.н., проф. Ю. И. Журавлев, д.ф.-м.н., проф. В. Н. Козлов, чл.-корр. РАН, д.ф.-м.н., проф. А. В. Михалев, к.ф.-м.н., проф. В. А. Носов, д.ф.-м.н., проф. А. С. Подколзин, д.т.н., проф. Д. А. Поспелов, д.ф.-м.н., проф. Ю. П. Пытьев, академик РАН, д.т.н., проф. А. С. Сигов, д.ф.-м.н., проф. А. В. Чечкин

Международный научный совет журнала:

С. Н. Васильев (Россия), К. Вашик (Германия), В. В. Величенко (Россия), А. И. Галушкин (Россия), И. В. Голубятников (Россия), Я. Деметрович (Венгрия), Г. Килибарда (Сербия), Ж. Кнап (Словения), П. С. Краснощеков (Россия), А. Нозаки (Япония), В. Н. Редько (Украина), И. Розенберг (Канада), А. П. Рыжов (Россия) — ученый секретарь совета, А. Саломаа (Финляндия), С. Саксида (Словения), Б. Тальхайм (Германия), Ш. Ушчумлич (Сербия), Фан Дин Зиеу (Вьетнам), А. Шайеб (Сирия), Р. Шчепанович (США), Г. Циммерман (Германия)

Секретари редакции: И. О. Бергер, М. А. Ильгова

В журнале «Интеллектуальные системы. Теория и приложения» публикуются научные достижения в области теории и приложений интеллектуальных систем, новых информационных технологий и компьютерных наук.

Издание журнала осуществляется под эгидой МГУ имени М. В. Ломоносова, Научного Совета по комплексной проблеме «Кибернетика» РАН, Отделения «Математическое моделирование технологических процессов» МАТН, Секции «Информатики и кибернетики» РАЕН.

Учредитель журнала: ООО «Интеллектуальные системы».

Журнал входит в список изданий, включенных ВАК РФ в реестр публикаций материалов по кандидатским и докторским диссертациям по математике и механике.

Спонсором издания является:

ООО «Два Облака»

Разработка корпоративных информационных систем
<http://www.dvaoblaka.ru>

Индекс подписки на журнал: 64559 в каталоге НТИ «Роспечать».

Адрес редакции: 119899, Россия, Москва, Воробьевы Горы, МГУ, ГЗ, механикоматематический факультет, комн. 12-01.

Адрес издателя: 115230, Россия, Москва, Хлебозаводский проезд, д. 7, стр. 9, офис 9. Тел. +7 (495) 939-46-37, e-mail: mail@intsysjournal.org

*) Прежнее название журнала: «Интеллектуальные системы».

© ООО «Интеллектуальные системы», 2018.

ОГЛАВЛЕНИЕ

Часть 1. Общие проблемы теории интеллектуальных систем

Менькин М.И. Автоматический перевод правил дорожного движения в теоретико-графовую формальную модель 7

Часть 2. Специальные вопросы теории интеллектуальных систем

Боков Г.В. О графовом расширении метода резолюции для булевых формул 35

Еременко А.Р., Яшунский А.Д. О весе функций, заданных неповторными И/ИЛИ формулами 41

Козлов В.Н. Коды, определяющие изображения с точностью до аффинных преобразований 57

Сытдыков Т.Р. Сложность синтеза многомерных прямоугольных схем 61

Часовских А.А. О числе максимальных надклассов в классе линейных автоматов 81

Часть 3. Математические модели

Бабин Д.Н. Автоматы с линейными переходами 87

Попков К.А. Короткие единичные проверяющие тесты для контактных схем при обрывах и замыканиях контактов 97

Коновалов А. Ю. Некорректность интуиционистской теории множеств относительно конструктивной семантики, основанной на гиперарифметических видах 131

Часовских А.А. О классах передаточных функций линейных автоматов . 135

Часть 4. Материалы семинара «Теория автоматов»

Доклады семинара «Теория автоматов» 147

Часть 1.
Общие проблемы теории
интеллектуальных систем

Автоматический перевод правил дорожного движения в теоретико-графовую формальную модель

Менькин М.И.

Данная работа относится к области семантического анализа юридических документов. В статье приводится один из возможных подходов по моделированию правил движения. Описаны основные этапы семантического разбора некоторого класса предложений.

Ключевые слова: семантический анализ нормативно-правовых актов, прагматический анализ, построение семантической модели текста.

1. Введение

Данная статья продолжает работу по семантическому анализу текста Постановления Правительства РФ «О правилах дорожного движения» (далее — ПДД) [1], начатую в [2].

Суть работы заключается в следующем. У нас есть текст на естественном языке (ЕЯ), и мы хотим понять его содержание («смысл»). Ограничимся классом текстов, «смысл» которых можно формализовать. Здесь наиболее удачным выбором являются юридические документы, в частности, Правила дорожного движения, т.к. текст этого документа фактически является алгоритмом (т.е. набором действий для всех участников движения в разных дорожных ситуациях), написанного текстом. И мы хотим перевести эти алгоритмы, выраженные текстом на ЕЯ, в формальную модель (т.е. извлечь «смысл»). В нашем случае такая формальная модель представлена моделью дорожных ситуаций, основанная на теоретико-графовом подходе. Модель правил представлена функцией на графах.

2. Основные определения и постановка задачи

Позаимствуем основные определения из [2] с небольшими изменениями.

Участок дороги (УД) — часть полосы движения, инвариантная относительно действующих на ней правил движения.

Граф дороги — раскрашенный граф $D = (V, E, P)$, где V — множество вершин, каждому элементу которого соответствует один УД, E — множество рёбер, каждому элементу которого соответствует одно отношение соседства «УД»–«УД» (т.е. ребром соединяем только примыкающие друг к другу УД), $P = P_v \times P_e$ — множество цветов, P_v — атрибуты вершин, P_e — атрибуты рёбер. Рёбра из E , которые соединяют УД, принадлежащие одной полосе, ориентированы по направлению движения на этой полосе.

Примеры цветов вершин: «тип перекрёстка» (если УД — перекрёсток), «главная дорога» (если УД является частью главной дороги), «жилая зона» (если УД — часть жилой зоны). Примеры цветов рёбер: «вид горизонтальной разметки» (если есть горизонтальная разметка), «наличие светофора», «сигнал светофора» (при наличии светофора).

Манёвр — потенциально возможное действие транспортного средства (ТС), в результате которого оно изменяет УД (например, меняет полосу движения, выезжает на перекрёсток или на УД с новым действующим знаком, и т.д.) или заметно изменяет свою скорость. В зависимости от дорожной ситуации, манёвр имеет статус «обязателен для исполнения», либо «допустим», либо «запрещён».

Перечислим манёвры, разбив их на четыре класса (в скобках — пример пункта, где манёвр встречается в ПДД):

- 1) Траекторные (относящиеся к изменению направления движения): перестроение (п. 8.1), разворот (п. 8.1), поворот (п. 8.1), обгон (п. 9.2), объезд (п. 9.2), опережение (п. 11.5);
- 2) Участковые (связанные с изменением участка дороги): съезд (п. 8.3), выезд (п. 9.4), въезд (п. 12.4);
- 3) Скоростные (относящиеся к изменению скорости): начало движения (п. 8.1), остановка (п. 8.1), повышение скорости (п. 10), снижение скорости (п. 10), резкое торможение (п. 10.5);
- 4) Уступить дорогу (не создавать помех) (п. 11.7) — сложный / условный манёвр; является комбинацией других манёвров, которая за-

висит от ДС; другими словами, этот манёвр — это совокупность других манёвров с условиями их применимости.

Пусть $D = (V, E, P)$ — граф дороги, T — множество ТС, M — множество манёвров. Тогда *дорожная ситуация* (ДС) — это пятёрка $S = (D, M, T, f, g)$, где $f: T \rightarrow V$ — функция позиционирования, которая каждому ТС из T ставит в соответствие один УД из V , $g: T \rightarrow M \cup \{*\}$ — функция назначения манёвра, которая каждому ТС из T ставит в соответствие один манёвр из M . Если функция назначения манёвра принимает значение $*$, то это понимается как «манёвр не определён». Множество T не обязательно должно содержать все ТС, которые находятся на дороге. Множество M не обязательно должно содержать все возможные манёвры.

Разрешение дорожной ситуации для данного транспортного средства — определение всех допустимых манёвров для данного ТС в данной ДС.

Разрешение дорожной ситуации — разрешение ДС для тех ТС, у которых значение манёвра неопределенно.

Уступить дорогу (не создавать помех) — сложный / условный манёвр; является комбинацией других манёвров, которая зависит от ДС; другими словами, этот манёвр — это совокупность других манёвров с условиями их применимости [2].

Текущая задача — моделирование правил, касающихся конкретного манёвра, для разрешения дорожной ситуации. Будем рассматривать предложения из ПДД, которые содержат манёвр «Уступить дорогу» (и двойственный ему «Имеет преимущество»). Этот манёвр представляется наиболее сложным и интересным для изучения.

3. Примеры предложений с манёвром «Уступить дорогу»

Всего в ПДД есть 48 предложений, содержащих ключевые слова «уступить» или «преимущество» (из которых 28 предложений соответствуют приводимому ниже синтаксическому шаблону). Поиск осуществлялся по ключевым словам «Уступить дорогу» и «Имеет преимущество». Приведём несколько таких предложений в качестве примера (здесь и далее нумерация предложений сквозная, по всему тексту ПДД):

520) При повороте налево или развороте вне перекрестка водитель безрельсового транспортного средства обязан уступить дорогу встречным транспортным средствам и трамваю попутного направления.

719) При повороте направо или налево водитель обязан уступить дорогу пешеходам и велосипедистам, пересекающим проезжую часть дороги, на которую он поворачивает.

735) Если сигналы светофора или регулировщика разрешают движение одновременно трамваю и безрельсовым транспортным средствам, то трамвай имеет преимущество независимо от направления его движения.

4. Шаблон дороги

Центральное место в нашей модели занимает «Шаблон дороги».

Правила движения ТС иногда зависят не только от того, какого типа участок дороги, на котором находится данное ТС (например, «разворот на мосту запрещён»), но и от того, какие участки дороги являются соседними для данного ТС (например, «на нерегулируемом перекрёстке при движении по неглавной дороге водитель должен уступить дорогу другим ТС, которые движутся по главной»). Для семантического разбора предложений и формализации понятия «правило движения (ТС)» необходимо ввести понятие «шаблон дороги».

Поясним, что будем понимать под шаблоном дороги. Для этого рассмотрим ТС, находящееся на дороге (рис. 2а). Можно считать, что дорога делится на 8 частей относительно ТС (рис. 2б). Эти части дороги можно схематично изобразить как показано на рис. 2в. Схему можно упростить, опустив цифры, и далее будем использовать упрощённый вид шаблона дорог, изображённый на рис. 2г. Чёрный квадрат в центре — ТС (для которого определяется правило движения); если скорость ТС отличная от нуля, предполагаем, что ТС движется в квадрат «вверх». Белые недиагональные квадраты — это части УД, ограниченные по размеру ТС (или шириной полосы движения). Белые диагональные квадраты — другие УД (соседние полосы; участки, принадлежащие перекрёстку или съезду с дороги, и т.д.). Некоторые белые квадраты могут отсутствовать (из возможных 8) — значит, правило ничего не требует от типа УД в этом месте (в т.ч. нахождение какого-либо ТС на нём).

Под шаблоном дороги (для каждого правила) будем понимать один из объектов, изображенных на рис. 3. Тогда «правилом движения» будем называть множество шаблонов дороги с указанием свойств для каждого «квадрата» шаблона дороги (тип УД, наличие ТС и их свойств, и т.д.).

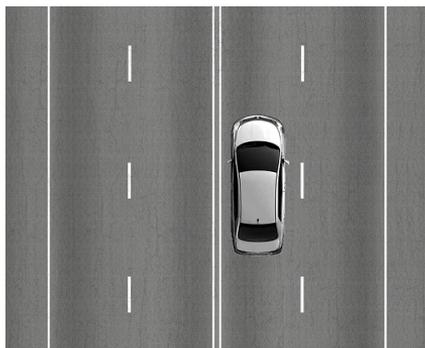


Рис. 2а.



Рис. 2б.

1	2	3
4	ТС	5
6	7	8

Рис. 2в.

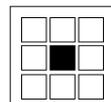


Рис. 2г.

Шаблон дороги для каждого правила определяется манёвром, о котором говорится в правиле. Исключение — манёвр «Уступить дорогу», т.к. этот манёвр состоит из нескольких других простых манёвров, поэтому может содержать более одного шаблона дороги.

«Чёрным квадратом» шаблона дороги для манёвра «Уступить дорогу» будет ТС, относительно которого принимаем решение о допустимости манёвра, «белые квадраты» могут содержать других участников движения. Типы ТС в шаблоне дороги будут множественными типами, каждое ТС будет иметь траекторию в виде упорядоченного множества УД с указанием начала и конца траектории. В качестве начала и конца траектории могут быть выбраны УД или другие участники движения.

Таким образом, «чёрный квадрат» содержит (множественный) тип и свойства (при наличии) ТС, которое уступает дорогу. «Белый квадрат» содержит: тип и свойства (при наличии) участка или участков дорог, которым соответствует «квадрат», и тип и свойства (при наличии) ТС, которые находятся на данном «квадрате».

Правило «Уступить дорогу» будет определяться совокупностью всех шаблонов дорог, относящимися к этому манёвру.

Если говорить о произвольных манёврах, то шаблон дороги — модель дорожной ситуации, где для ТС (изображенного чёрным квадратом) определяется допустимость того или иного манёвра в зависимости от типа текущего участка дороги, типов соседних участков дорог и дру-

гих участников движения, которые могут находиться на соседних участках дороги.

Шаблоны определяются по ключевым словам, соответствующим названиям шаблонов. Расскажем подробно про каждый шаблон дороги (рис. 3), при необходимости используя нумерацию «белых квадратов» согласно рис. 5в.

Шаблон 1. «При приближении...». Данный шаблон работает в ситуации, когда речь идёт о преимуществе другого ТС, независимо от его местоположения (по отношению к нашему ТС). В зависимости от контекста речь может идти, например, о приближении справа (квадраты 3, 5 и 8).

Шаблон 2. «Обгон». Шаблон, помимо обгона, в некоторых ситуациях соответствует объезду (слева). Квадраты 1 и 4 говорят о необходимости уступить дорогу встречным ТС (на этих квадратах). Квадраты 4, 6 и 7 — о необходимости уступить дорогу тем ТС, которые уже начали обгон (опережение, объезд).

Шаблон 3. «Объезд справа». Этот шаблон также соответствует опережению (справа). Комментарии аналогичны шаблону №2 (с поправкой на то, что обгона справа не существует).

Шаблоны 4.1, 4.2. «Перестроение» (левое и правое). Также соответствует опережению (слева и справа). Комментарии аналогичны шаблону №2 и №3, с той разницей, что нет встречных ТС.

Шаблон 5. «Разворот» и «Поворот налево». При совершении данных манёвров необходимо уступить дорогу ТС, движущимся с квадратов 2 и 3 в сторону 1 квадрата, встречным ТС с квадрата 1, а также трамваю и попутным ТС с квадратов 4 и 6.

Шаблон 6. «Поворот направо». Также используется в ситуации выезда на круговой перекрёсток и при выезде на перекрёсток неравнозначных дорог со стороны второстепенной дороги. Дорога уступается ТС, движущимся с квадратов 1 и 2 (в сторону 3 квадрата) — если поворот направо или круговой перекрёсток, при этом при повороте направо в некоторых ситуациях необходимо уступать дорогу квадрату 3 (например, пешеходам, которые переходят дорогу во время совершения манёвра). При выезде на перекрёсток неравнозначных дорог со стороны второстепенной дороги нужно уступать дорогу квадратам 1 и 3, а также тем ТС, которые двигаются по 2 квадрату с направлений 1-го и 3-го.

Шаблон 7. «Выезд» (кроме выездов на перекрёсток). Также соответствует съезду и въезду. Используется в случае, если ТС меняет участок дороги, и ТС нового УД имеют преимущество. Шаблон имеет

несколько разновидностей, белым квадратом может быть 2, 4, 5 или 7, но только один (на рисунке белый квадрат — 2).

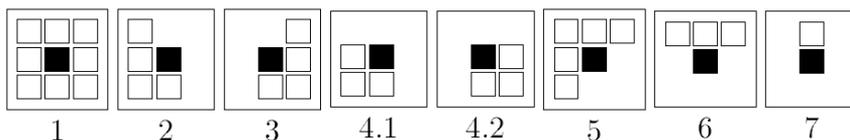


Рис. 3. Шаблоны дорог.

5. Синтаксические шаблоны предложений

Для конструирования «правил движения» необходимо извлечь всю информацию, которая выражена текстом в документе для рассматриваемого манёвра (под конструированием подразумеваем размещение ТС, перечисленных в тексте, на «квадратах» шаблона дороги, с указанием их свойств и свойств УД, и т.д.). Каждое «правило движения» обязательно содержит объект, который выполняет манёвр — «чёрный квадрат» (КТО_УСТУПАЕТ) и (возможно) объекты, которым надо уступить дорогу, находящихся на «белых квадратах» (КОМУ_УСТУПИТЬ). Также правила могут содержать в себе условия на особенности данной дорожной ситуации (СИТУАЦИЯ).

Общий вид предложений, для которых ниже перечислены синтаксические шаблоны, приведён на рис. 4 (на примере шаблона «должен уступить»). Выбор именно таких предложений обусловлен тем, что таких предложений больше (поэтому другие можно считать «исключениями»). Предложения, которые синтаксически устроены иначе (другое устройство синтаксического дерева и другие синтаксические шаблоны), в данной работе рассматриваться не будут.

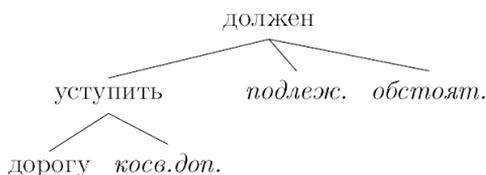


Рис. 4. Шаблон синтаксического дерева для манёвра «Уступить дорогу».

Помимо прочего, в правилах иногда встречается условие про «пересечение траекторий ТС», но оно подразумевается всегда (т.е. и в том случае, когда не говорится об этом), поэтому при разборе предложений эти слова будем игнорировать.

СИТУАЦИЯ может содержать в себе:

- условия на движение по текущему УД или планируемому для проезда;
- простые манёвры, совершаемые КТО_УСТУПАЕТ (например, «разворот»);
- место движения (тип УД).

КТО_УСТУПАЕТ и КОМУ_УСТУПИТЬ содержат списки ТС с указанием их типов и свойств.

Ниже приведём детальную характеристику возможных синтаксических шаблонов предложений, которые соответствуют значениям полей для каждого объекта правила движения, и которые в дальнейшем будут использоваться для алгоритма разбора предложений. Указывать значения полей будем четвёрками (слово, часть речи, семантический класс, ярус синтаксического дерева). Под семантическим классом будем понимать названия множества слов с эквивалентной семантикой, при этом применяя онтологию Linguistic [5]. Семантические классы понятны по их названию.

Используемые сокращения для синтаксических ролей слов предложения:

- подлежаж. — подлежащее
- сказ. — сказуемое
- согл.определ. — согласованное определение
- несогл.определ. — несогласованное определение
- прям.доп. — прямое дополнение
- косв.доп. — косвенное дополнение
- обстоят. — обстоятельство

Смежные (по синтаксическому дереву) слова обозначим знаком «+». Словом *обстоятельство* обозначаем произвольное слово, являющееся одноимённой частью речи.

Отметим важную деталь относительного синтаксического разбора предложений — для автоматического разбора предложения по синтаксическому шаблону с фиксированным множеством слов для каждой части шаблона (т.е. в каждом шаблоне множество возможных используемых слов полностью определено), для каждого слова предложения требуются наличие следующих свойств:

- слово-родитель — требуется всегда;
- синтаксическая роль — требуется всегда;
- порядок слова в предложении (или иначе, слова-соседи) — требуется при наличии у слова зависимых служебных частей речи или однородных с ним членов.

5.1. Начало разбора

Среди предложений, которые относятся к манёвру «Уступить дорогу» в данной статье мы будем рассматривать только следующие базовые конструкции. Остальные типы предложений в рамках данной статьи не рассматриваются. В предложениях, связанных с манёвром «Уступить дорогу», встречаются следующие базовые конструкции:

- (должен / должны, сказ., MODAL, 0) + (уступить, прям.доп., TO_CEDE, 1) + (дорогу, прям.доп., ROAD, 2);
- (обязан, сказ., TO_OBLIGE, 0) + (уступить, прям.доп., TO_CEDE, 1) + (дорогу, прям.доп., ROAD, 2);
- (имеет, сказ., EXISTENCE_AND_POSSESSION, 0) + (преимущество, прям.доп., CH_BENEFIT, 1)

5.2. Объект КТО_УСТУПАЕТ

В данном пункте перечислим существующие типы КТО_УСТУПАЕТ, встречающихся в ПДД:

- (водитель / водители, подлежаж., TRANSPORT_DRIVER, 1);
- (трамвай, подлежаж., TRAM, 1);
- (пешеходы, подлежаж., ON_FOOT, 1);
- (велосипедисты, подлежаж., CYCLIST, 1).

Для «водитель» возможно наличие такого свойства:

- (безрельсового, согл.определ., NO_PREFIXOID + RAIL, 4–3) + (транспортного, согл.определ., TRANSPORT, 3) + (средства, несогл.определ., TRANSPORT, 2).

5.3. Объект СИТУАЦИЯ

В рассматриваемых предложениях может быть несколько типов возможных синтаксических конструкций, которые могут встречаться в СИТУАЦИЯ.

«Условие на событие» характеризуется наличием следующих синтаксических конструкций:

- ((в) случае / (в) случаях / (кроме) случаев, обстоят., CASE, 1)
- ((при) наличии, обстоят., EXISTENCE_AND_POSSESSION, 2) + (препятствия, несогл.определ., OBSTACLE_AS_OBJECT_BY_FUNCTION, 3)
- ((при) включении, обстоят., TO_ACTIVATE, 1) + (сигнала, несогл.определ., SIGNALING_ACTION, 2) + (светофора, несогл.определ., TRAFFIC_LIGHTS, 3)

«Условие на движение» характеризуется наличием следующих синтаксических конструкций:

- ((при) движении, обстоят., GENERAL_MOTION, 1) + *обстоятельство*;
- ((при) выезде, обстоят., MOTION_ON_DEVICES, 1) + *обстоятельство*;
- ((при) съезде, обстоят., MOTION_ON_DEVICES, 1) + *обстоятельство*;
- ((при) перестроении, обстоят., TO_PLACE_IN_ORDER, 1) + ((транспортных) средств, несогл.определ., TRANSPORT, 2) + (движущихся, согл.определ., GENERAL_MOTION, 3) + *обстоятельство*;
- ((при) повороте, обстоят., TO_TURN, 1) + *обстоятельство*;
- ((при) развороте, обстоят., TO_TURN, 1) + *обстоятельство*;

«Тип УД» характеризуется наличием следующих синтаксических конструкций:

- ((на) перекрёстке, обстоят., CROSS_PLACE, 1) + (дорог, несогл.определ., ROAD, 2) + (равнозначных / неравнозначных, согл.определ., EQUAL_SAME, 3)
- ((в) пунктах, обстоят., INHABITED_LOCALITY, 1) + (населённых, согл.определ., POPULATION_DENSITY, 2)

- ((в) зоне, обстоят., ZONE, 1) + (жилой, согл.определ., RESIDENTIAL, 2)
- ((в) зоне, обстоят., AREA_OF_ACTIVITY_AS_WHOLE, 1) + (велосипедной, согл.определ., BICYCLE, 2)
- (вне, обстоят., ZONE, 1) + (перекрёстков, косв.доп., CROSS_PLACE, 2)

5.4. Объект КОМУ_УСТУПИТЬ

В данном пункте перечислим существующие типы КОМУ_УСТУПИТЬ:

- ((транспортному) средству / (транспортным) средствам, косв.доп., TRANSPORT, 2);
- (пешеходам, косв.доп., ON_FOOT, 2);
- (велосипедистам, косв.доп., CYCLIST, 2);
- (трамваю, косв.доп., TRAM, 2).

Перечислим возможные свойства типов КОМУ_УСТУПИТЬ:

- (движущимся / движущегося, согл.определ., GENERAL_MOTION, 3) + *обстоятельство*;
- (находящемуся, согл.определ., POSITION_IN_SPACE, 3) + *обстоятельство*;
- (приближающимся / приближающегося, согл.определ., TO_GO_AND_TRANSFER, 3)
- (встречным, согл.определ., OPPOSITE, 3);
- (попутного, согл.определ., FOLLOWING, 4) + (направления, несогл.определ., REFERRAL, 3);
- (начинающим / завершающим, согл.определ., BEGIN / END_TO_TAKE_PLACE, 3) + (движение, прям.доп., GENERAL_MOTION, 4);
- для пешеходов: (переходящим, согл.определ., TO_WALK, 3)
- для пешеходов: (вступившим, согл.определ., TO_STEP, 3)

6. Основные этапы разбора

Как было сказано в предыдущем разделе, несмотря на то, что семантически предложения о манёвре «Уступить дорогу» выглядят одинаково

(можно однозначно выделить части предложений, определяющие тип манёвра, КТО_УСТУПАЕТ, КОМУ_УСТУПИТЬ, СИТУАЦИЯ), синтаксически они устроены по-разному. Разнообразие синтаксических конструкций делает юридический документ более читабельным, но усложняет его автоматический разбор.

Поэтому перед проведением разбора предложений необходимо отсеять от всего текста только те, которые, во-первых, относятся к рассматриваемому нами манёвру и, во-вторых, совпадают с синтаксическими шаблонами «Начало разбора», приведённым в предыдущем разделе. Первые три пункта — поиск именно таких предложений. Последующие пункты — семантический разбор (т.е. построение соответствия «текст»–«правило движения»).

1. Ищем ключевые слова «уступить» или «преимущество» (найдено: 48).

2. Среди найденных предложений ищем те, у которых корневое слово синтаксического графа — сказуемое «должен», «обязан», «имеет» (найдено: 33).

3. Среди найденных предложений ищем один из шаблонов «должен уступить», «обязан уступить», «имеет преимущество» (найдено: 28).

Перечислим этапы разбора для предложений, найденных после третьего пункта. При этом используя синтаксические шаблоны из предыдущего раздела.

4. Определяем тип манёвра — «Уступить дорогу» или «Имеет преимущество».

5. Определяем тип предложения — простое или сложное. Предложение будет считаться сложным, если сказуемых, которые относятся к манёвру больше одного; либо есть фразы «кроме случаев», «однако»; либо в предложении (а точнее, в обстоятельстве предложения) указано более одного манёвра (через запятую или слово «или»). Т.е., в нашем понимании, сложное предложение — это то, которое содержит более одного правила (но не всегда разным правилам соответствуют разные шаблоны дорог, см. примеры ниже). Например, синтаксические шаблоны «обязан уступить при съезде ..., а также при выезде с ...» и «должен уступить ..., кроме случаев ...» соответствуют сложным предложениям, которые содержат в себе по два правила сразу. Если предложение окажется сложным, то следующие пункты (6–9) применяем поочерёдно к каждой части предложения, содержащей своё правило.

6. Подлежащее (зависящее от «должен» / «обязан» / «имеет») и его зависимые слова проверяем на наличие шаблонов КТО_УСТУПАЕТ.

7. Обстоятельство (зависящее от «должен» / «обязан» / «имеет») и его зависимые слова проверяем на наличие шаблонов СИТУАЦИЯ. Выбираем шаблоны дороги, которые соответствуют СИТУАЦИЯ. Определяем типы «белых квадратов».

8. Косвенные дополнения (зависящие от «уступить» / «преимущество») и их зависимые слова проверяем на наличие шаблонов КОМУ_УСТУПИТЬ. Определяем перечень других ТС и их свойства.

9. Определяем местоположение ТС на шаблоне дороги. Если манёвр «Уступить дорогу», то «чёрный квадрат» — КТО_УСТУПАЕТ, «белые квадраты» — КОМУ_УСТУПИТЬ. Если манёвр «Имеет преимущество», то «чёрный квадрат» — КОМУ_УСТУПИТЬ, «белые квадраты» — КТО_УСТУПАЕТ (т.е. меняем значение таким образом, чтобы правило всегда означало «чёрный квадрат уступает»).

7. Примеры разбора предложения

Приведём примеры разборов некоторых предложений, содержащих манёвр «Уступить дорогу». Синтаксический анализ предложений осуществлялся при помощи АБВУУ InfoExtractor Demo. Результат работы продукта — XML-файл с разбором всех предложений документа. В первом примере в квадратных скобках указаны элементы и атрибуты элементов XML-файла, которые используются для анализа предложения. Также для первого примера приведено полное синтаксическое дерево предложения.

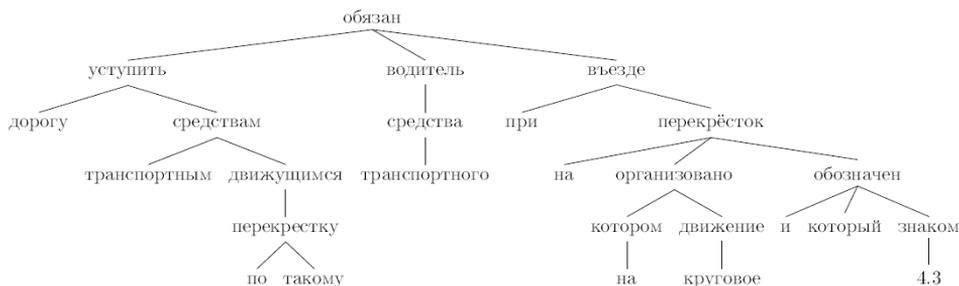


Рис. 5а. Синтаксическое дерево (пример 1).

Пример 1. «При въезде на перекресток, на котором организовано круговое движение и который обозначен знаком 4.3, водитель транспортного средства обязан уступить дорогу транспортным средствам, дви-

жущимся по такому перекрестку». На рис. 5а приведён синтаксический граф предложения.

1. Манёвр один, сказуемое манёвра одно, ключевые слова «однако» и «кроме» отсутствуют, значит предложение простое.

2. Шаблон «начала разбора» — «обязан уступить», значит тип манёвра — Уступить дорогу.

3. Определяем КТО_УСТУПАЕТ. Это должно быть подлежащее [`<syntactic_role>=Subject`], зависящее [`<syntactic_parent>`] от сказуемого «обязан» [`<syntactic_role>=Predicate`]. В данном случае — «водитель». От «водитель» идут зависимые [`<syntactic_parent>`] слова «транспортного» [`<syntactic_role>=AgreedAttribute`] средства [`<syntactic_role>=NonAgreedAttribute`]. Дополнительных свойств нет. Значит, КТО_УСТУПАЕТ — ТС (без каких-либо свойств, т.е. любое).

4. Определяем СИТУАЦИЯ. Обстоятельство, зависящее от сказуемого — «(при) выезде» [`<syntactic_role>=AdverbialModifier`]. Предварительный шаблон для правила — номер 7 («выезд»). Продолжаем разбор, смотрим на зависимые [`<syntactic_parent>`] от «при выезде» слова. Это обстоятельство «(на) перекрёсток» [`<syntactic_role>=AdverbialModifier`]. Нужно определить свойства перекрёстка, продолжаем разбор от слов «на перекрёсток». Определяем, что это перекрёсток с круговым движением. Изменяем шаблон на номер 6 («поворот направо»), т.к. это выезд на перекрёсток с круговым движением. Определяем свойства «белых квадратов» перед ТС — «круговой перекрёсток».

5. Определяем тип КОМУ_УСТУПИТЬ. Смотрим на косвенное дополнение, зависящее от прямого дополнения «уступить». Это «(транспортным) средствам» [`<syntactic_role>=ObjectIndirect`], значит множественный тип КОМУ_УСТУПИТЬ — ТС. Определяем возможные свойства, продолжаем разбор от слова «средствам». Единственное зависимое [`<syntactic_parent>`] слово — «движущимся» [`<syntactic_role>=AgreedAttribute`] и от него «по перекрестку такому». Это полностью соответствует «белым квадратам» шаблона, дополнительных свойств нет.

Разбор предложения завершён (рис. 5б).

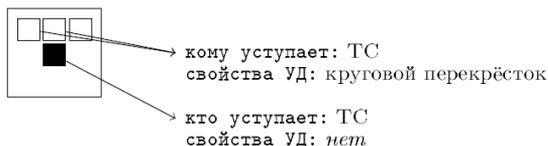


Рис. 5б. Разбор предложения (пример 1).

Пример 2. «При выезде на дорогу с прилегающей территории водитель должен уступить дорогу транспортным средствам и пешеходам, движущимся по ней, а при съезде с дороги — пешеходам и велосипедистам, путь движения которых он пересекает».

1. Присутствует эллипсис сказуемого «должен» и два манёвра — «при выезде» и «при съезде», значит предложение сложное. Предложение содержит два правила — «должен уступить при выезде...» и «должен уступить при съезде...».

Разделим дальнейший предложения разбор на 2 части, начнём с «должен уступить при выезде...».

2.1. Шаблон «начала разбора» — «должен уступить», значит тип манёвра — Уступить дорогу.

2.2. Определяем КТО_УСТУПАЕТ, это подлежащее, зависящее от сказуемого «должен». В данном случае — «водитель». От «водитель» нет зависимых слов. Дополнительных свойств нет. Значит, КТО_УСТУПАЕТ — ТС (без каких-либо свойств, т.е. любое).

2.3. Определяем СИТУАЦИЯ. Обстоятельство, зависящее от сказуемого — «при выезде». Предварительный шаблон для правила — номер 7 («выезд»). Продолжаем разбор, смотрим на зависимые от «при выезде» слова. Это обстоятельства «на дорогу» и «с территории». Нужно определить свойства «на дорогу» и «с территории». Продолжаем разбор от слов «на дорогу», зависимых слов нет. Значит, дополнительных свойств нет. Продолжаем разбор от слов «с территории», есть зависимое слово «прилегающей». Определяем, что это прилегающая территория, дополнительных свойств нет. Шаблон остаётся таким же (номер 7, «выезд»). Определяем свойства «белого квадрата» — «дорога». Определяем свойство «чёрного квадрата» — «прилегающая территория».

2.4. Определяем тип КОМУ_УСТУПИТЬ. Смотрим на косвенные дополнения, зависящее от прямого дополнения «уступить». Это «транспортным средствам» и «пешеходам», значит КОМУ_УСТУПИТЬ соответствуют два множественных типа КОМУ_УСТУПИТЬ — ТС и пешеход. Определяем возможные свойства, продолжаем разбор от слов «средствам» и «пешеходам». Единственное зависимое слово — «движущимся», а от него «по ней» в значении «по дороге» (анафора). Это соответствует «белому квадрату» шаблона, дополнительных свойств нет.

Разбор первой части предложения завершён.

Разбираем «должен уступить при съезде...».

3.1. Аналогичен пункту 2.1.

3.2. Аналогичен пункту 2.2.

3.3. Определяем СИТУАЦИЯ. Обстоятельство, зависящее от сказуемого — «при съезде». Предварительный шаблон для правила — номер 7 («выезд»). Продолжаем разбор, смотрим на зависимые от «при съезде» слова. Это обстоятельство «с дороги». Нужно определить свойства дороги, продолжаем разбор от слов «с дороги». Зависимых слов нет, значит нет и дополнительных свойств. Шаблон остаётся таким же (номер 7, «выезд»). Определяем свойство «чёрного квадрата» — «дорога». Т.к. манёвр — съезд, то определяем свойство «белого квадрата» как «НЕ дорога».

3.4. Определяем тип КОМУ_УСТУПИТЬ. Смотрим на косвенное дополнение, зависящее от прямого дополнения «уступить». Это «пешеходам» и «велосипедистам», значит КОМУ_УСТУПИТЬ соответствуют два множественных типа КОМУ_УСТУПИТЬ — пешеход и велосипедист. Определяем возможные свойства, продолжаем разбор от слов «пешеходам» и «велосипедистам». Единственное зависимое слово — «пересекает» в составе конструкции «путь которых он пересекает». Поскольку манёвр «Уступить дорогу» всегда подразумевает пересечение траекторий, то данную конструкцию игнорируем. Других свойств нет.

Разбор второй части, а значит всего предложения завершён (рис. 6).

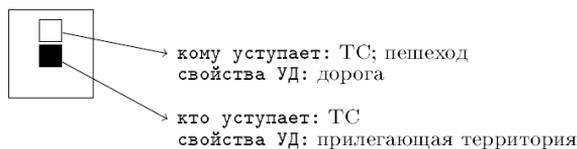


Рис. 6а. Разбор первой части (пример 2).

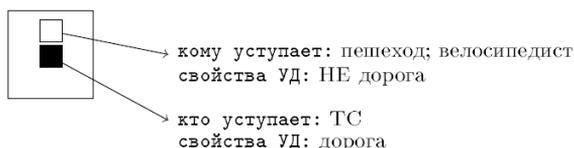


Рис. 6б. Разбор второй части (пример 2).

Пример 3. «При перестроении водитель должен уступить дорогу транспортным средствам, движущимся попутно без изменения направления движения».

1. Манёвр один, сказуемое манёвра одно, ключевые слова «однако» и «кроме» отсутствуют, значит предложение простое.

2. Шаблон «начала разбора» — «должен уступить», значит тип манёвра — Уступить дорогу.

3. Определяем **КТО_УСТУПАЕТ**. Это должно быть подлежащее, зависящее от сказуемого «должен». В данном случае — «водитель». От «водитель» нет зависимых слов, дополнительных свойств нет. Значит, **КТО_УСТУПАЕТ** — ТС (без каких-либо свойств, т.е. любое).

4. Определяем **СИТУАЦИЯ**. Обстоятельство, зависящее от сказуемого — «при перестроении». Предварительный шаблон для правила — номер 4 («перестроение»). Шаблонов, соответствующих перестроению, два (левое и правое перестроение). Поэтому предложению будет соответствовать два шаблона. Продолжаем разбор, зависимых от «при перестроении» слов нет, значит других свойств **СИТУАЦИЯ** нет. Определяем свойства «белых квадратов» — «односторонняя полоса».

5. Определяем тип **КОМУ_УСТУПИТЬ**. Смотрим на косвенное дополнение, зависящее от прямого дополнения «уступить». Это «транспортным средствам», значит множественный тип **КОМУ_УСТУПИТЬ** — ТС. Определяем возможные свойства, продолжаем разбор от слова «средствам». Единственное зависимое слово — «движущимся» и от него две зависимости — «попутно» и «без изменения направления движения». Свойство «попутно» соответствует «белым квадратам» шаблона, дополнительное свойство — «без изменения направления движения».

Разбор предложения завершён (рис. 7).

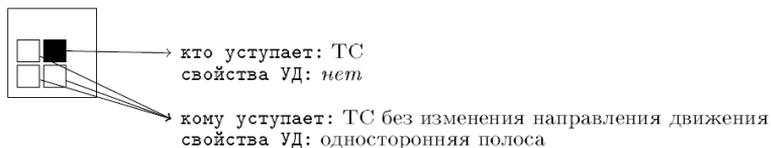


Рис. 7а. Первый шаблон (пример 7).

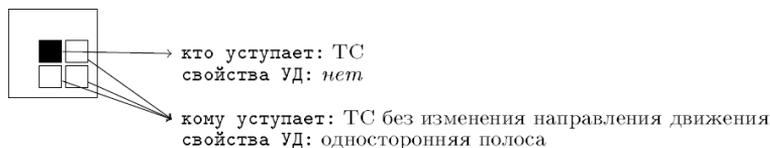


Рис. 7б. Второй шаблон (пример 3).

Пример 4. «При повороте налево или развороте вне перекрестка водитель безрельсового транспортного средства обязан уступить дорогу встречным транспортным средствам и трамваю попутного направления».

1. Присутствуют два манёвра (поворот налево и разворот), значит предложение сложное.

2. Шаблон «начала разбора» — «обязан уступить», значит тип манёвра — Уступить дорогу.

3. Определяем КТО_УСТУПАЕТ. Это должно быть подлежащее, зависящее от сказуемого «обязан». В данном случае — «водитель». От «водитель» идут зависимые слова «транспортного средства» и «безрельсового». Других зависимых слов нет. Значит, КТО_УСТУПАЕТ — ТС с дополнительным свойством «безрельсовое».

4. Определяем СИТУАЦИЯ. Обстоятельства, зависящие от сказуемого — «при повороте налево» и «развороте». И повороту налево, и развороту соответствует один шаблон — номер 5. Продолжаем разбор, смотрим на зависимые от «при повороте налево» и «развороте» слова. Это обстоятельство «вне» с зависимым словом «перекрёстка». Других зависимых слов нет. Определяем свойства «белых квадратов» и «чёрного квадрата» — «НЕ перекрёсток».

5. Определяем тип КОМУ_УСТУПИТЬ. Смотрим на косвенное дополнение, зависящее от прямого дополнения «уступить». Это «транспортным средствам» и «трамваю», значит множественный тип КОМУ_УСТУПИТЬ — ТС и трамвай. Определяем возможные свойства. Продолжаем разбор от слова «средствам». Получаем дополнительное свойство — «встречным». Других зависимых слов от «средствам» нет. Продолжаем разбор от слова «трамваю». Получаем дополнительное свойство — «направления» с зависимым словом «попутного». Других зависимых слов от «трамваю» нет. Значит, КОМУ_УСТУПИТЬ — встречные ТС и попутный трамвай. Т.к. движение правостороннее, а трамвайные пути находятся посередине дороги, то встречные ТС и трамваи могут находиться только на левых квадратах шаблона (это замечание не обязательно нужно учитывать и можно было доопределить и другие квадраты шаблона, т.к. на практике такая ситуация всё равно не возникнет).

Разбор предложения завершён (рис. 8).

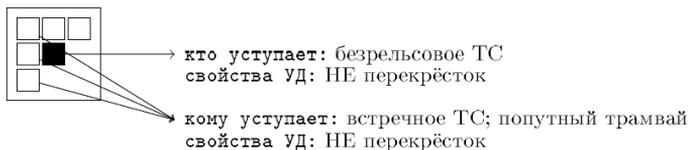


Рис. 8. Итог разбора предложения (пример 4).

Пример 5. «При повороте направо или налево водитель обязан уступить дорогу пешеходам и велосипедистам, пересекающим проезжую часть дороги, на которую он поворачивает».

1. Присутствуют два манёвра (поворот направо и поворот налево), значит предложение сложное.

2. Шаблон «начала разбора» — «обязан уступить», значит тип манёвра — Уступить дорогу.

3. Определяем КТО_УСТУПАЕТ. Это должно быть подлежащее, зависящее от сказуемого «обязан». В данном случае — «водитель». От «водитель» нет зависимых слов, дополнительных свойств нет. Значит, КТО_УСТУПАЕТ — ТС (без каких-либо свойств, т.е. любое).

4. Определяем СИТУАЦИЯ. Обстоятельства, зависящие от сказуемого — «при повороте направо или налево». Повороту налево соответствует шаблон номер 5, повороту направо — шаблон номер 6. Зависимых от обстоятельств слов нет. Значит, у «белых квадратов» и «чёрного квадрата» нет свойств УД.

5. Определяем тип КОМУ_УСТУПИТЬ. Смотрим на косвенное дополнение, зависящее от прямого дополнения «уступить». Это «пешеходам» и «велосипедистам», значит множественный тип КОМУ_УСТУПИТЬ — пешеход и велосипедист. Определяем возможные свойства. Продолжаем разбор, единственное зависимое слово — «пересекающим» и от него конструкция «проезжую часть дороги, на которую он поворачивает». Это соответствует «белому квадрату» №1 шаблона №5 и «белому квадрату» №3 шаблона №6. Других дополнительных свойств нет.

Разбор предложения завершён (рис. 9).

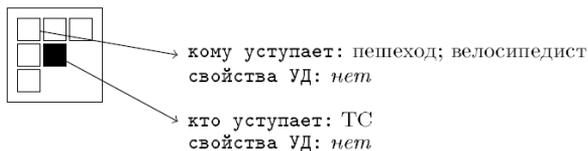


Рис. 9а. Поворот налево (пример 5).

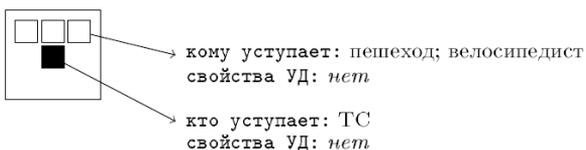


Рис. 9б. Поворот направо (пример 5).

Пример 6. «При повороте налево или развороте по зеленому сигналу светофора водитель безрельсового транспортного средства обязан уступить дорогу транспортным средствам, движущимся со встречного направления прямо или направо.»

1. Присутствуют два манёвра (поворот налево и разворот), значит предложение сложное.

2. Шаблон «начала разбора» — «обязан уступить», значит тип манёвра — Уступить дорогу.

3. Определяем КТО_УСТУПАЕТ. Это должно быть подлежащее, зависящее от сказуемого «обязан». В данном случае — «водитель». От «водитель» идут зависимые слова «транспортного средства» и «безрельсового». Других зависимых слов нет. Значит, КТО_УСТУПАЕТ — ТС с дополнительным свойством «безрельсовое».

4. Определяем СИТУАЦИЯ. Обстоятельства, зависящие от сказуемого — «при повороте налево» и «развороте». И повороту налево, и развороту соответствует один шаблон — номер 5. Других зависимых от обстоятельства слов нет. Однако присутствует условие на событие, у сказуемого «обязан» есть зависимое косвенное дополнение «по сигналу». Далее, у «по сигналу» есть зависимые слова «зелёному» и «светофора». Других зависимых слов нет. Определяем свойство передних «белых квадратов» (№1, №2, №3) — «перекрёсток» и остальных «белых квадратов» и «чёрного квадрата» — «НЕ перекрёсток».

5. Определяем тип КОМУ_УСТУПИТЬ. Смотрим на косвенное дополнение, зависящее от прямого дополнения «уступить». Это «транспортным средствам», значит множественный тип КОМУ_УСТУПИТЬ — ТС. Определяем возможные свойства, продолжаем разбор от слова «средствам». Единственное зависимое слово — «движущимся» и от него фразы «со встречного направления» и «прямо или направо». Значит, КОМУ_УСТУПИТЬ — встречное ТС с направлением движения прямо или направо.

Разбор предложения завершён (рис. 10).

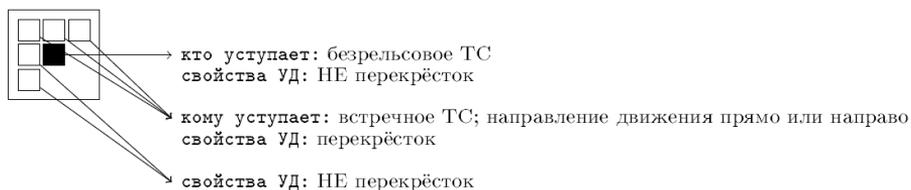


Рис. 10. Итог разбора предложения (пример 6).

Пример 7. «На перекрестке неравнозначных дорог водитель транспортного средства, движущегося по второстепенной дороге, должен уступить дорогу транспортным средствам, приближающимся по главной, независимо от направления их дальнейшего движения».

1. Манёвр один, сказуемое манёвра одно, ключевые слова «однако» и «кроме» отсутствуют, значит предложение простое.

2. Шаблон «начала разбора» — «должен уступить», значит тип манёвра — Уступить дорогу.

3. Определяем КТО_УСТУПАЕТ. Это должно быть подлежащее, зависящее от сказуемого «должен». В данном случае — «водитель». От «водитель» идут зависимые слова «транспортного средства» и «движущегося». От слова «движущегося» идут зависимые слова «по второстепенной дороге». Эта фраза накладывает ограничение на УД. Добавляем свойство «второстепенная дорога» для «чёрного квадрата». У «водитель» других дополнительных свойств нет. Значит, КТО_УСТУПАЕТ — ТС (без каких-либо свойств, т.е. любое).

4. Определяем СИТУАЦИЯ. Обстоятельство, зависящее от сказуемого — «на перекрёстке». Продолжаем разбор, смотрим на зависимые от «на перекрёстке» слова. Это фраза «неравнозначных дорог». Пользуясь фразой из предыдущего пункта о движении по второстепенной дороге, определяем, что это выезд на перекрёсток неравнозначных дорог со стороны второстепенной дороги. Поэтому выбираем шаблон номер 6 («поворот направо»). Определяем свойства «белого квадрата» номер 2 — «перекрёсток неравнозначных дорог», и для других «белых квадратов» — «главная дорога».

5. Определяем тип КОМУ_УСТУПИТЬ. Смотрим на косвенное дополнение, зависящее от прямого дополнения «уступить». Это «транспортным средствам», значит множественный тип КОМУ_УСТУПИТЬ — ТС. Определяем возможные свойства, продолжаем разбор от слова «средствам». Единственное зависимое слово — «приближающимся» и от него «по главной дороге». Это полностью соответствует 1-му и 3-му «белым квадратам» шаблона, дополнительных свойств нет.

6. Также в предложении есть фраза «независимо от направления их дальнейшего движения», но именно это и предполагается по умолчанию во всех шаблонах правил и данная фраза не вносит никаких дополнительных ограничений на свойства ТС.

Разбор предложения завершён (рис. 11).

Пример 8. «При выезде из жилой зоны водители должны уступить дорогу другим участникам движения».

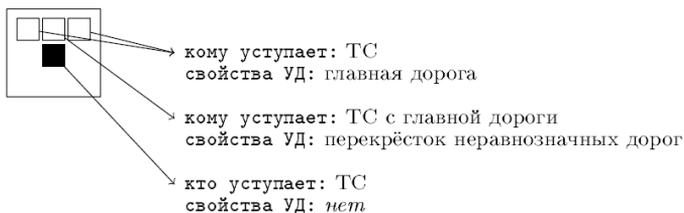


Рис. 11. Итог разбора предложения (пример 7).

1. Манёвр один, сказуемое манёвра одно, ключевые слова «однако» и «кроме» отсутствуют, значит предложение простое.

2. Шаблон «начала разбора» — «должны уступить», значит тип манёвра — Уступить дорогу.

3. Определяем КТО_УСТУПАЕТ. Это должно быть подлежащее, зависящее от сказуемого «должны». В данном случае — «водители». От «водители» нет других зависимых слов. Значит, дополнительных свойств нет. Определяем КТО_УСТУПАЕТ — ТС (без каких-либо свойств, т.е. любое).

4. Определяем СИТУАЦИЯ. Обстоятельство, зависящее от сказуемого — «при выезде». Предварительный шаблон для правила — номер 7 («выезд»). Продолжаем разбор, смотрим на зависимые от «при выезде» слова. Это фраза «из жилой зоны». Шаблон дороги остаётся таким же. Определяем свойство «чёрного квадрата» — «жилая зона». Определяем свойства «белого квадрата» — «НЕ жилая зона».

5. Определяем тип КОМУ_УСТУПИТЬ. Смотрим на косвенное дополнение, зависящее от прямого дополнения «уступить». Это «другим участникам движения», значит множественный тип КОМУ_УСТУПИТЬ — участник движения (подразумевая любого участника движения). Дополнительных свойств нет.

Разбор предложения завершён (рис. 12).

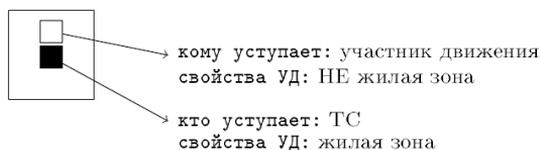


Рис. 12. Итог разбора предложения (пример 8).

8. Заключение

Данная статья является началом работы по автоматизации извлечения знаний из текста предложений (в нашем случае — построение модели правил ПДД). Разобраны предложения, содержащие манёвр «Уступить дорогу» / «Имеет преимущество» и имеющих эквивалентные синтаксические деревья (см. рис 4). Однако, по приведённому выше подходу не может быть осуществлён разбор некоторых типов предложений. А именно:

- предложений, в которых зависимые слова находятся в разных предложениях. Пример (предложения 521-522 из [1]): «Если при развороте вне перекрестка ширина проезжей части недостаточна для выполнения маневра из крайнего левого положения, его допускается производить от правого края проезжей части (с правой обочины). При этом водитель должен уступить дорогу попутным и встречным транспортным средствам». Предложений такого типа — 7.
- предложений с нестандартным (нешаблонным) порядком слов. Например, вместо синтаксического шаблона «должен уступить дорогу» используется дееспричастный оборот с фразой «уступая дорогу» (предложение 796).

Дальнейшая работа будет акцентирована на разработке методов разбора этих типов предложений. Описанные в текущей статье процедуры позволяют разбирать примерно 60% предложений.

Список литературы

- [1] “Постановление Правительства РФ от 23.10.1993 N 1090 (ред. от 04.12.2018) «О правилах дорожного движения»”, *КонсультантПлюс*.
- [2] Менькин М.И., “Объектная модель правил дорожного движения”, *Интеллектуальные системы. Теория и приложения*, **23**:1 (2019), 39–53.
- [3] “АВВУ InfoExtractor Demo”, <http://parsertest.abbyy.com/ru/>.
- [4] Перпер Е.М., Гасанов Э.Э., Кудрявцев В.Б., “О семантическом анализе юридических текстов”, *Интеллектуальные системы. Теория и приложения*, **22**:3 (2018), 45–87.
- [5] “Онтология Linguistic (АВВУ)”, http://comprenoservice.abbyy.com/help/ru/ontologies_linguistic_linguistic.html.

**Auto-translation of rules of the road to formal graph-theoretic
model
Menkin M.**

The present article deals with semantic analysis of legal documents. In this paper, we introduce one possible approach to formal modeling of rules of the road. We describe the basic procedures for semantic analysis of one type of sentences.

Keywords: semantic analysis of legal documents, pragmatic analysis, modeling of text semantic.

Часть 2.
Специальные вопросы теории
интеллектуальных систем

О графовом расширении метода резолюции для булевых формул

Боков Г.В.

В работе описывается новое расширение метода резолюции, использующее графовое представление опровержений булевых формул в конъюнктивной нормальной форме. Доказывается, что невыполнимость булевой формулы равносильна существованию для неё графового опровержения.

Ключевые слова: Метод резолюции, графовые опровержения, невыполнимость, булевы формулы.

Введение

Проблема выполнимости булевых формул является классической комбинаторной проблемой. Она состоит в том, чтобы по любой заданной булевой формуле ответить на вопрос о её выполнимости, т.е. существовании такого набора значений её переменных, на котором формула принимает истинное значение. Важность этой проблемы обуславливается тем, что решение многих комбинаторных проблем удается свести к проблеме выполнимости конкретных булевых формул [1].

Есть несколько частных случаев проблемы выполнимости для ограниченных классов булевых формул. Одним из важнейших на сегодняшний день ограничений является проблема выполнимости булевых формул в конъюнктивной нормальной форме (КНФ), в которой формулы задаются как конъюнкции дизъюнктов, дизъюнкты — как дизъюнкции литералов, литералы — как переменные и их отрицания. Кук [2] и независимо Левин [3] доказали, что любую задачу, разрешимую на недетерминированной машине Тьюринга за полиномиальное время, можно эффективно свести к проблеме выполнимости булевых формул в КНФ.

Каждый набор значений переменных булевой формулы, на которых она принимает истинное значение, является простым сертификатом, удостоверяющим её выполнимость. Проблема выполнимости в этом смысле

ле сводится к поиску простого сертификата. Как быть, если для булевой формулы не существует сертификата, удостоверяющего её выполнимость? Конечно, формула в этом случае будет невыполнима. Но, можем ли мы это эффективно проверить, т.е. можем ли мы по формуле получить простой сертификат, удостоверяющий её невыполнимость? Не смотря на то, что ответа на этот вопрос до сих пор нет, он породил целое направление в теории сложности, связанное с системами доказательств булевых формул [4].

Одной из первой систем доказательств для построения опровержений выполнимости булевых формул был метод резолюции. Метод, будучи примененным к системе дизъюнктов невыполнимой булевой формулы в КНФ, позволяет за конечное число шагов вывести пустой дизъюнкт. Стоит отметить, что число шагов на отдельных семействах формул может достигать экспоненциального размера [5]. Существует несколько расширений метода резолюции [6], в том числе те [7], для которых до сих пор ничего не известно о сложности их доказательств. В данной работе будет предложено новое расширение метода резолюции, основанное на графовом представлении опровержений булевых формул в КНФ.

Основные определения и обозначения

Булевы формулы определяются с помощью логических связок $\{\neg, \wedge, \vee\}$, переменных и скобок стандартным образом:

$$A, B ::= x \mid \bar{A} \mid (A \wedge B) \mid (A \vee B).$$

Для обозначения переменных мы будем использовать буквы x, y, z и т.д. Заглавными буквами A, B, F и т.д. будем обозначать формулы. Также мы будем опускать скобки, если их восстановление определяется контекстом и стандартным приоритетом связок: \neg, \wedge, \vee . Обозначим через $\mathbf{Fm}(n)$ множество булевых формул с n переменными.

Булева формула $F(x_1, \dots, x_n) \in \mathbf{Fm}(n)$ над переменными x_1, \dots, x_n *выполнима*, если существуют такие $a_1, \dots, a_n \in \{0, 1\}$ значения переменных x_1, \dots, x_n , на которых формула принимает значение 1, т.е.

$$F(a_1, \dots, a_n) = 1,$$

в следующем смысле:

x	\bar{x}	x	y	$x \wedge y$	$x \vee y$
0	1	0	0	0	0
0	1	0	1	0	1
1	0	1	0	0	1
1	1	1	1	1	1

Литералом называется всякая переменная x или её отрицание \bar{x} и обозначается через x^a , где $x^1 = x$ и $x^0 = \bar{x}$. Множество всех литералов обозначим через **Lt**. *Дизъюнктом* называется всякая дизъюнкция литералов

$$x_1^{a_1} \vee \dots \vee x_n^{a_n},$$

где $x_i \neq x_j$ для всех $1 \leq i < j \leq n$. Мы будем отождествлять дизъюнкты с множеством их литералов, т.е. дизъюнкты

$$l_1 \vee \dots \vee l_n \text{ и } l_{\sigma(1)} \vee \dots \vee l_{\sigma(n)}$$

совпадают для любой перестановки σ . Обозначим через \perp пустой дизъюнкт.

Булевой формулой в *конъюнктивной нормальной форме* (КНФ) будем называть всякую конъюнкцию дизъюнктов. Например, все следующие формулы являются булевыми формулами в КНФ:

$$x \vee y, x \wedge y, (\bar{x} \vee y) \wedge \bar{z}, (x \vee \bar{y}) \wedge (\bar{x} \vee y \vee z) \wedge (\bar{x} \vee \bar{z}).$$

Мы отождествляем булевы формулы в КНФ с множеством их дизъюнктов. Через **CNF**(n) будем обозначать множество всех булевых формул из **Fm**(n) в КНФ.

Напомним, что *ориентированным ациклическим графом* называется пара (\mathbf{V}, \mathbf{E}) , где \mathbf{V} — конечное множество вершин графа и $\mathbf{E} \subseteq \mathbf{V} \times \mathbf{V}$ — множество его ребер. Ребро $(u, v) \in \mathbf{E}$ называется *исходящим* для вершины u и *входящим* для вершины v . Вершину, не имеющую входящих (исходящих) ребер, назовём *корневой* (*терминальной*). Путем в графе из вершины u в вершину v называется всякая последовательность

$$u = v_1, (v_1, v_2), v_2, \dots, (v_{n-1}, v_n), v_n = v$$

такая, что $(v_i, v_{i+1}) \in \mathbf{E}$ для всех $1 \leq i < n$. Вершина u *доминирует* вершину v , если всякий путь из корневой вершины в v проходит через u . При этом вершину u будем называть *доминирующей* для вершины v .

Графовое расширение метода резолюции

Пусть F — булева формула в КНФ. *Опровержением* формулы F или просто *F -опровержением* будем называть ориентированный ациклический рёберно-размеченный граф $\mathcal{G} = (\mathbf{V}, \mathbf{E}, \lambda, r)$ с функцией разметки

$$\lambda: \mathbf{E} \rightarrow \mathbf{Lt}$$

и единственной корневой вершиной $r \in \mathbf{V}$ такой, что выполнены следующие условия:

- 1) каждая нетерминальная вершина v с исходящими рёбрами e_1, \dots, e_n определяет дизъюнкт F

$$\varphi(v) = \lambda(e_1) \vee \dots \vee \lambda(e_n) \in F;$$

- 2) если e_1, e_2 — входящие рёбра одной и той же вершины v , то $\lambda(e_1) = \lambda(e_2)$. В этом случае полагаем $\lambda(v) = \lambda(e_1) = \lambda(e_2)$;
- 3) либо $\perp \in F$, либо для любой терминальной вершины w существуют такая доминирующая вершина u , что $\lambda(w) = \overline{\lambda(u)}$.

Формулу F , для которой существует F -опровержение, будем называть *опровержимой*. Главным результатом работы является следующая теорема.

Теорема 1. *Если $F \in \mathbf{CNF}(n)$, то F невыполнима $\Leftrightarrow F$ опровержима.*

Доказательство. Рассмотрим булеву формулу $F \in \mathbf{CNF}(n)$ и предположим, что F невыполнима. Построим F -опровержение индукцией по n . Если $n = 0$, то $F = \perp$ и тогда любой граф вида $(\{r\}, \emptyset, \lambda, r)$ является F -опровержением.

Предположим, что для любой невыполнимой формулы $G \in \mathbf{CNF}(n-1)$ существует G -опровержение. Тогда для каждого $a \in \{0, 1\}$ рассмотрим формулу F_a , полученную из F удалением всех дизъюнктов, содержащих литерал x_n^{1-a} , а также удалением всех вхождений литерала x_n^a из оставшихся дизъюнктов. По предположению индукции для F_a существует опровержение $\mathcal{G}_a = (\mathbf{V}_a, \mathbf{E}_a, \lambda_a, r_a)$. Пусть $v_1^a, \dots, v_{m_a}^a$ — все вершины в \mathcal{G}_a , для которых $\varphi(v_i^a) \in F_a \setminus F$. Тогда $\varphi(v_i^a) \cup \{x_n^a\} \in F$ для $1 \leq i \leq m_a$ и $a \in \{0, 1\}$.

Определим граф $\mathcal{G} = (\mathbf{V}, \mathbf{E}, \lambda, r_0)$, для которого $\mathbf{V} = \mathbf{V}_0 \cup \mathbf{V}_1 \cup \{w\}$, где $w \notin \mathbf{V}_0 \cup \mathbf{V}_1$,

$$\mathbf{E} = \mathbf{E}_0 \cup \mathbf{E}_1 \cup \{(v_i^0, r_1) \mid 1 \leq i \leq m_0\} \cup \{(v_i^1, w) \mid 1 \leq i \leq m_1\},$$

$$\lambda(e) = \begin{cases} \lambda_a(e), & e \in \mathbf{E}_a, a \in \{0, 1\}; \\ \bar{x}, & e = (v_i^0, r_1), 1 \leq i \leq m_0; \\ x, & e = (v_i^1, w), 1 \leq i \leq m_1. \end{cases}$$

По построению \mathcal{G} является F -опровержением.

В обратную сторону. Пусть $\mathcal{G} = (\mathbf{V}, \mathbf{E}, \lambda, r)$ — F -опровержение. Докажем, что F невыполнима индукцией по n . Если $n = 0$, то $\perp \in F$ и, следовательно, F невыполнима.

Пусть $n > 0$ и предположение индукции верно для всех формул $G \in \mathbf{CNF}(n - 1)$. Рассмотрим произвольное $a \in \{0, 1\}$ и определим граф \mathcal{G}_a , полученный из графа \mathcal{G} в результате последовательного выполнения следующих преобразований:

- 1) удаление всех ребер $e \in \mathbf{E}$ таких, что $\lambda(e) = x_n^a$;
- 2) для каждой вершины $v \in \mathbf{V}$ такой, что $x_n^{1-a} \in \varphi(v)$, удаление всех исходящих из неё ребер e таких, что $\lambda(e) \neq x_n^{1-a}$;
- 3) удаление всех вершин и ребер графа \mathcal{G} , недостижимых из корневой вершины r .

По построению \mathcal{G}_a является F_a -опровержением и, следовательно, F_a невыполнима по предположению индукции. Из произвольности a заключаем, что F невыполнима. \square

Заключение

Стоит отметить, что использование графового подхода для представления доказательств не является новым. Например, в [8] с помощью графового представления доказательств в минимальной импликативной логике удалось избежать экспоненциального роста при переходе к нормальной форме.

Представляется интересным продолжить исследование предложенного графового представления опровержений булевых формул в следующем направлении. Во-первых, проверить, как с точки зрения полиномиальной сводимости соотносятся между собой метод резолюции, графовое расширение метода резолюции и метод расширенной резолюции. Во-вторых, изучить вопрос об оценке функции Шеннона размера графового опровержения невыполнимой булевой формулы от n переменных в худшем случае.

Список литературы

- [1] *Karp R. M.* Reducibility among combinatorial problems // Complexity of Computer Computations, R.E. Miller and J.W. Thatcher, ed., New York (Plenum Press), 1972, pp. 85–103.
- [2] *Cook S. A.* The complexity of theorem proving procedures // Proceedings of the third annual ACM symposium on Theory of computing, 1971, pp. 151–158.
- [3] *Левин Л. А.* Универсальные задачи перебора // Проблемы передачи информации, т. 9, № 3, 1973, с. 115–116.
- [4] *Бокков Г. В.* От булевых схем к доказательству теорем // Интеллектуальные системы. Теория и приложения, т. 22, № 1, с. 123–130.
- [5] *Haken A.* The intractability of resolution // Theoretical Computer Science, vol. 39, 1985, pp. 297–308.
- [6] *Tseitin G. C.* On the complexity of derivations in propositional calculus // In A. O. Slisenko, editor, Studies in Mathematics and Mathematical Logic, Part II, 1970, pp. 115–125.
- [7] *Kullmann O.* On a generalization of extended resolution // Discrete Applied Mathematics, vol. 96–97, 1999, pp. 149–176.
- [8] *Quispe-Cruz M., Haeusler E. H., Gordeev L.* Proof-graphs for minimal implicational logic // Proceedings 2013 International Workshop on Developments in Computational Models, EPTCS, vol. 144, 2014, pp. 16–29.

Graph based extended resolution for Boolean formulas Bokov G.V.

In this article we consider a graph based extended resolution for representing refutations of Boolean formulas in conjunction normal form. We prove that a Boolean formula is unsatisfiable iff there is its graph based refutation.

Keywords: Resolution, graph based refutation, unsatisfiability, Boolean formulas.

О весе функций, заданных неповторными И/ИЛИ формулами

Еременко А.Р., Яшунский А.Д.

Рассматривается множество функций, заданных неповторными формулами с бинарными операциями конъюнкции (логического И) и дизъюнкции (логического ИЛИ). Для функций, заданных формулами с фиксированным числом операций, исследуются значения весов — числа наборов, на которых функция принимает значение 1. Найдены асимптотические оценки для числа неповторных формул, задающих функции с весом из определенных диапазонов, в частности, — числа формул, задающих функции, у которых доля единиц среди значений не превышает четверти.

Ключевые слова: булева функция, неповторная формула, вес функции, асимптотическая оценка.

1. Введение

Рассмотрим плоское корневое бинарное дерево с n внутренними вершинами. Будем считать, что все листья дерева помечены символами переменных x_1, \dots, x_{n+1} или их отрицаний, причем любым двум различным листам соответствуют различные переменные, а каждая внутренняя вершина помечена либо символом $\&$ (конъюнкция, логическое И), либо символом \vee (дизъюнкция, логическое ИЛИ). Тогда каждому дереву можно сопоставить булеву функцию от переменных x_1, \dots, x_{n+1} . Такая функция будет выражаться *неповторной* формулой, т. е. каждый символ переменной будет встречаться в ней ровно один раз. Подробнее о таких функциях, часто также называемых неповторными, см. [1]. Напомним, что *весом* булевой функции называется число наборов, на которых она принимает значение 1. Очевидно, что вес функции от $n + 1$ переменной — целое число от 0 до 2^{n+1} .

Пусть вместо всех переменных неповторной функции подставлены независимые случайные величины, равные 0 и 1 с вероятностями $\frac{1}{2}$.

Несложно видеть, что в этом случае вероятность обращения функции в единицу будет в точности равна ее весу, разделенному на 2^{n+1} . Кроме того, легко проверить, что эта вероятность (равно как и вес функции) не зависят от расстановки отрицаний на символах переменных, а зависит только от структуры дерева и пометок на его внутренних вершинах.

Множество значений вероятностей (а вместе с ними и возможных весов неповторных функций) можно описать следующей формальной конструкцией. Определим *вероятностные формулы* по индукции. Будем считать, что x — вероятностная формула сложности $L(x) = 0$ со значением $\pi(x) = \frac{1}{2}$. Если Φ_1 и Φ_2 — вероятностные формулы, то выражения $(\Phi_1 \& \Phi_2)$ и $(\Phi_1 \vee \Phi_2)$ также являются вероятностными формулами сложности $L(\Phi_1) + L(\Phi_2) + 1$, а их значения, соответственно равны:

$$\pi((\Phi_1 \& \Phi_2)) = \pi(\Phi_1)\pi(\Phi_2), \quad (1)$$

$$\pi((\Phi_1 \vee \Phi_2)) = \pi(\Phi_1) + \pi(\Phi_2) - \pi(\Phi_1)\pi(\Phi_2). \quad (2)$$

Общее число вероятностных формул сложности n в точности равно числу деревьев с n внутренними вершинами, помеченными символами $\&$ и \vee . Оно выражается как $2^n c_n$, где c_n — числа Каталана, которые можно задать соотношениями $c_0 = 1$ и $c_{n+1} = \sum_{k=0}^n c_k c_{n-k}$.

Из результатов Р. Л. Схиртладзе [2] известно, что значением вероятностных формул могут быть любые двоично-рациональные числа. При этом значениями формул сложности n являются всевозможные дроби с нечетным числителем и знаменателем 2^{n+1} , и только они. С учетом этого факта, положим:

$$f(l, n) = \left| \left\{ \Phi : \pi(\Phi) = \frac{2l-1}{2^{n+1}} \right\} \right|$$

для $l = 1, \dots, 2^n$.

Отметим, что среди неповторных формул, заданных И/ИЛИ деревьями с фиксированным порядком переменных, ровно $f(l, n)$ выражают монотонную функцию веса l от $n+1$ переменной, и ровно $2^{n+1} f(l, n)$ выражают функцию веса l от $n+1$ переменной. При этом, например, количество неповторных монотонных функций веса l от $n+1$ переменной можно оценить сверху величиной $(n+1)! f(l, n)$. Далее в тексте работы мы будем оперировать исключительно с величинами $f(l, n)$ не обращаясь более к их интерпретации через веса соответствующих булевых функций.

Как несложно видеть, при всех n имеет место равенство $\sum_{l=1}^{2^n} f(l, n) = 2^n c_n$. Также по индукции несложно доказать, что у *двойственных* вероятностных формул, т. е. таких, которые получаются друг из друга заменой символов $\&$ на \vee , а \vee на $\&$ соответственно, значения в сумме равны 1. Отсюда вытекает следующее важное соотношение:

$$f(l, n) = f(2^n - l + 1, n). \quad (3)$$

Таким образом, за исключением случая $n = 0$, все вероятностные формулы могут быть разбиты на пары, в которых сумма значений равна 1, следствием чего оказывается выполнение при $n \geq 1$ равенства:

$$\sum_{l=1}^{\frac{1}{2}2^n} f(l, n) = \frac{1}{2}2^n c_n. \quad (4)$$

Отсюда же вытекает, что среднее значение $\pi(\Phi)$ по формулам фиксированной сложности равно $\frac{1}{2}$. Это частный случай более общего свойства вероятностных формул, доказанного в [3].

Дроби с числителем 1 (соответственно $2^n - 1$) могут быть получены только из формулы, содержащей исключительно символы $\&$ (соответственно \vee), поэтому выполнены равенства $f(1, n) = f(2^n - 1, n) = c_n$.

Как следует из равенств (1) и (2) значение $\frac{2l-1}{2^{n+2}}$ может быть получено в том, и только в том случае, если значения $\pi(\Phi_1) = \frac{2l_1-1}{2^{n_1+1}}$ и $\pi(\Phi_2) = \frac{2l_2-1}{2^{n_2+1}}$ удовлетворяют одному из соотношений:

$$\left[\begin{array}{l} \frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} = \frac{2l-1}{2^{n+2}}, \\ \frac{2l_1-1}{2^{n_1+1}} + \frac{2l_2-1}{2^{n_2+1}} - \frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} = \frac{2l-1}{2^{n+2}}. \end{array} \right.$$

Второе из этих соотношений может быть переписано как

$$\frac{2(2^{n_1} - l_1 + 1) - 1}{2^{n_1+1}} \cdot \frac{2(2^{n_2} - l_2 + 1) - 1}{2^{n_2+1}} = \frac{2(2^{n+1} - l + 1) - 1}{2^{n+2}},$$

что, с учетом соображений двойственности (см. равенство (3)) приводит к следующей формуле для $f(l, n + 1)$:

$$f(l, n + 1) = \sum f(l_1, n_1) f(l_2, n_2). \quad (5)$$

$$\frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} \in \left\{ \frac{2l-1}{2^{n+2}}, \frac{2(2^{n+1}-l-1)+1}{2^{n+2}} \right\}$$

Формула (5) позволяет для малых n непосредственно вычислить значения $f(l, n)$. Гистограммы значений $f(l, n)$, а также график нормированной нарастающей суммы $F(x, n) = \frac{1}{2^n c_n} \sum_{1 \leq l \leq x 2^n} f(l, n)$, для случая $n = 10$ приведены на рис. 1. Пунктиром на графике $F(x, 10)$ показана прямая $y = x$.

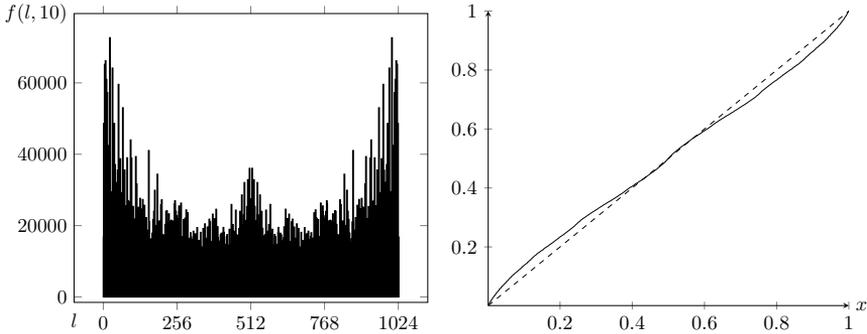


Рис. 1. Графики $f(l, 10)$ и $F(x, 10)$

Графики функций $F(x, n)$ с ростом n постепенно приближаются к прямой $y = x$, и уже для $n = 10$ график расположен достаточно близко от прямой. Это позволяет высказать гипотезу о том, что с ростом n значения $f(l, n)$ для $l = 1, \dots, 2^n$ постепенно выравниваются. Однако, как будет показано далее, эта гипотеза не подтверждается.

2. Неравномерность $f(l, n)$

Рассмотрение в сумме из соотношения (5) лишь части слагаемых позволяет получать нижние оценки для $f(l, n)$.

Дробь $\frac{2l-1}{2^{n+1}}$ может быть представлена в виде $\frac{2l-1}{2^{k+1}} \cdot \frac{1}{2^{n-k-1+1}}$, при условии, что k удовлетворяет неравенству $k \geq \lceil \log_2 l \rceil$. Это позволяет выписать для $f(l, n+1)$ следующую оценку снизу:

$$f(l, n+1) \geq 2 \sum_{k=\lceil \log_2 l \rceil}^n f(l, k) f(1, n-k) = 2 \sum_{k=\lceil \log_2 l \rceil}^n f(l, k) c_{n-k}.$$

Положим $\alpha_0 = 1$ и определим $\alpha_{t+1} = 2 \sum_{s=0}^t \alpha_t c_{t-s}$. Тогда индукцией по n несложно доказать следующее утверждение.

Лемма 1. При $n \geq \lceil \log_2 l \rceil$ выполнено $f(l, n) \geq \alpha_{n - \lceil \log_2 l \rceil} f(l, \lceil \log_2 l \rceil)$.

Выражение для элементов последовательности α_t может быть найдено явно. Обозначим $A(z) = \sum_{t=0}^{\infty} \alpha_t z^t$ производящую функцию последовательности α_t , а через $C(z) = \sum_{n=0}^{\infty} c_n z^n$ — производящую функцию чисел Каталана. Напомним, что для $C(z)$ имеет место равенство $C(z) = \frac{1}{2z}(1 - \sqrt{1 - 4z})$. Тогда из определения последовательности α_t вытекает, что $A(z)$ удовлетворяет уравнению

$$A(z) - 1 = 2zA(z)C(z),$$

из которого вытекает, что $A(z) = \frac{1}{1 - 2zC(z)}$. С учетом выражения для $C(z)$ получаем, что $A(z) = \frac{1}{\sqrt{1 - 4z}}$. Разложение функции $A(z)$ в ряд по степеням z дает явное выражение $\alpha_t = \binom{2t}{t}$. Учитывая известное соотношение $c_n = \frac{1}{n+1} \binom{2n}{n}$, получаем следующее утверждение.

Теорема 1. При $n \geq \lceil \log_2 l \rceil$ выполнено неравенство

$$f(l, n) \geq (n - \lceil \log_2 l \rceil + 1) f(l, \lceil \log_2 l \rceil) c_{n - \lceil \log_2 l \rceil}.$$

В частности, для $l = 2$ в качестве следствия получаем

$$f(2, n) \geq n f(2, 1) c_{n-1} = n c_{n-1}.$$

Поскольку $\frac{nc_{n-1}}{c_n} \rightarrow \infty$ при $n \rightarrow \infty$, доказанное неравенство исключает возможность приближения значений $f(l, n)$ к c_n с ростом n при всех l , как это можно было бы предположить с учетом того, что среднее значение $\frac{1}{2^n} \sum_{l=1}^{2^n} f(l, n)$ в точности равно c_n . Таким образом, если какой-то предельный закон для величин $f(l, n)$ и существует, его характер должен быть существенно сложнее.

3. Рекуррентные неравенства

Дальнейший анализ покажет, что гипотеза о какой бы то ни было равномерности в распределении значений формул не подтверждается даже в самом слабом варианте. Для того, чтобы это продемонстрировать, мы будем оценивать количество формул сложности n , значение которых не превышает $\frac{1}{4}$ — будем обозначать его $q(n)$, а также количество формул

сложности n , значение которых лежит между $\frac{1}{4}$ и $\frac{1}{2}$ — его будем обозначать $r(n)$. Введем соответствующие определения.

Положим $q(0) = 0$, $q(1) = 1$, и далее для $n \geq 2$ определим

$$q(n) = \sum_{l=1}^{\frac{1}{4}2^n} f(l, n).$$

Оценим величину $q(n)$ снизу. Из соотношения (5) вытекает, что $q(n+1)$ в точности равно сумме произведений $f(l_1, n_1)f(l_2, n_2)$ по всевозможным значениям l_1, n_1, l_2, n_2 , удовлетворяющих условиям

$$\left[\begin{array}{l} \frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} \leq \frac{1}{4}, \\ \frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} \geq \frac{3}{4}, \end{array} \right.$$

Оценка снизу для $q(n+1)$ получается рассмотрением только первого из этих двух условий. Заметим, что неравенство $\frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} \leq \frac{1}{4}$ заведомо выполняется, если какая-то из дробей, $\frac{2l_1-1}{2^{n_1+1}}$ или $\frac{2l_2-1}{2^{n_2+1}}$ не больше $\frac{1}{4}$, а также если обе дроби не превышают $\frac{1}{2}$. Объединяя эти два случая, учитывая их пересечение, получаем следующую оценку:

$$q(n+1) \geq \sum_{\substack{n_1+n_2=n, \\ \frac{2l_1-1}{2^{n_1+1}} \leq \frac{1}{2}, \frac{2l_2-1}{2^{n_2+1}} \leq \frac{1}{2}}} f(l_1, n_1)f(l_2, n_2) + 2 \sum_{\substack{n_1+n_2=n, \\ \frac{2l_1-1}{2^{n_1+1}} > \frac{1}{2}, \frac{2l_2-1}{2^{n_2+1}} \leq \frac{1}{4}}} f(l_1, n_1)f(l_2, n_2). \quad (6)$$

Рассмотрим сначала первую сумму, выделив в ней слагаемые, в которых n_1 или n_2 — нулевое:

$$\begin{aligned} & \sum_{\substack{n_1+n_2=n, \\ \frac{2l_1-1}{2^{n_1+1}} \leq \frac{1}{2}, \frac{2l_2-1}{2^{n_2+1}} \leq \frac{1}{2}}} f(l_1, n_1)f(l_2, n_2) = \\ & = f(1, 0) \left(\sum_{l_2 \leq \frac{1}{2}2^n} f(l_2, n) \right) + \left(\sum_{l_1 \leq \frac{1}{2}2^n} f(l_1, n) \right) f(1, 0) + \\ & + \sum_{\substack{n_1+n_2=n, \\ n_1>0, n_2>0}} \left(\sum_{\frac{2l_1-1}{2^{n_1+1}} \leq \frac{1}{2}} f(l_1, n_1) \right) \left(\sum_{\frac{2l_2-1}{2^{n_2+1}} \leq \frac{1}{2}} f(l_2, n_2) \right). \end{aligned}$$

С учетом соотношения (4) рассматриваемая сумма принимает вид:

$$\begin{aligned} \sum_{\substack{n_1+n_2=n, \\ \frac{2l_1-1}{2^{n_1+1}} \leq \frac{1}{2}, \frac{2l_2-1}{2^{n_2+1}} \leq \frac{1}{2}}} f(l_1, n_1)f(l_2, n_2) &= 2 \cdot \frac{1}{2} 2^n c_n + \sum_{\substack{n_1+n_2=n, \\ n_1>0, n_2>0}} \frac{1}{2} 2^{n_1} c_{n_1} \frac{1}{2} 2^{n_2} c_{n_2} = \\ &= 2^n c_n + \frac{1}{4} 2^n \sum_{k=1}^{n-1} c_k c_{n-k} = 2^n c_n + \frac{1}{4} 2^n (c_{n+1} - 2c_n) = \frac{1}{2} 2^n c_n + \frac{1}{8} 2^{n+1} c_{n+1}. \end{aligned}$$

Перейдем теперь к рассмотрению второй суммы из (6). Заметим, что если одно из значений n_1 или n_2 нулевое, то не найдется ни одной пары значений l_1, l_2 , удовлетворяющих условиям $\frac{2l_1-1}{2^{n_1+1}} > \frac{1}{2}$ и $\frac{2l_2-1}{2^{n_2+1}} \leq \frac{1}{4}$. С учетом этого и равенства (4) получаем:

$$\begin{aligned} \sum_{\substack{n_1+n_2=n, \\ \frac{2l_1-1}{2^{n_1+1}} > \frac{1}{2}, \frac{2l_2-1}{2^{n_2+1}} \leq \frac{1}{4}}} f(l_1, n_1)f(l_2, n_2) &= \sum_{k=1}^{n-1} \left(\sum_{\frac{2l_1-1}{2^{k+1}} > \frac{1}{2}} f(l_1, k) \right) \left(\sum_{\frac{2l_2-1}{2^{n-k+1}} \leq \frac{1}{4}} f(l_2, n-k) \right) = \\ &= \sum_{k=1}^{n-1} \frac{1}{2} 2^k c_k q(n-k) = \frac{1}{2} \sum_{k=1}^{n-1} 2^k c_k q(n-k). \end{aligned}$$

Объединяя все выведенные выше неравенства, приходим к следующей рекуррентной оценке.

Лемма 2. При $n \geq 1$ выполнено неравенство:

$$q(n+1) \geq \frac{1}{8} 2^{n+1} c_{n+1} + \frac{1}{2} 2^n c_n + \sum_{k=1}^{n-1} 2^k c_k q(n-k).$$

Определим теперь функцию $r(n)$, положив $r(0) = r(1) = 0$ и далее для $n \geq 2$:

$$r(n) = \sum_{\frac{1}{4} 2^n < l < \frac{1}{2} 2^n} f(l, n) = \sum_{\frac{1}{2} 2^n < l < \frac{3}{4} 2^n} f(l, n),$$

где равенство сумм очевидно имеет место в силу соотношения (3). Из данного определения получаем, что $r(2) = 2$. Отметим также, что при $n \geq 1$ выполнено $q(n) + r(n) = \frac{1}{2} 2^n c_n$.

Представление (5) и симметрия $f(l, n)$, описываемая равенством (3), позволяют получить следующее соотношение для $r(n+1)$ при $n \geq 2$:

$$\begin{aligned}
 2r(n+1) &= \sum_{\frac{1}{4}2^{n+1} < l < \frac{1}{2}2^{n+1}} f(l, n) + \sum_{\frac{1}{2}2^{n+1} < l < \frac{3}{4}2^{n+1}} f(l, n) = \\
 &= \sum_{\frac{1}{4}2^{n+1} < l < \frac{3}{4}2^{n+1}} \sum_{\substack{l_1+n_1=l \\ \frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} \in \left\{ \frac{2l-1}{2^{n+2}}, \frac{2(2^{n+1}-l-1)+1}{2^{n+2}} \right\}}} f(l_1, n_1)f(l_2, n_2) = \\
 &= 2 \sum_{\substack{n_1+n_2=n, \\ \frac{1}{4} < \frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4}}} f(l_1, n_1)f(l_2, n_2).
 \end{aligned}$$

Из данного соотношения естественно вытекает равенство

$$\begin{aligned}
 r(n+1) &= \sum_{\substack{n_1+n_2=n, \\ \frac{1}{4} < \frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4}}} f(l_1, n_1)f(l_2, n_2), \tag{7}
 \end{aligned}$$

которое будем использовать далее для получения рекуррентной нижней оценки величины $r(n+1)$.

В сумме из соотношения (7) выделим слагаемые, в которых n_1 или n_2 меньше 2:

$$\begin{aligned}
 r(n+1) &= 2 \sum_{\substack{\frac{1}{4} < \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4} \\ n_1=1, n_2=n}} f(1, 0)f(l_2, n) + 2 \sum_{\substack{\frac{1}{4} < \frac{3}{4} \cdot \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4} \\ n_1=2, n_2=n-1}} f(2, 1)f(l_2, n-1) + \sum_{\substack{n_1+n_2=n, n_1>1, n_2>1, \\ \frac{1}{4} < \frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4}}} f(l_1, n_1)f(l_2, n_2).
 \end{aligned}$$

В представлении выше удвоение первых двух сумм обусловлено тем, что значение 0 (соответственно 1) может принимать как n_1 , так и n_2 . Во второй сумме выбор $n_1 = 1$ автоматически влечет $l_1 = 2$, так как при $l_1 = 1$, мы получали бы для l_2 заведомо невыполнимое условие $\frac{1}{4} < \frac{1}{4} \cdot \frac{2l_2-1}{2^{n_2+1}}$.

Оценим каждую из сумм в приведенном выше соотношении (напомним, что оно рассматривается для $n \geq 2$). Для первой суммы имеет место точное равенство:

$$\begin{aligned}
 2 \sum_{\substack{\frac{1}{4} < \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4} \\ n_1=1, n_2=n}} f(1, 0)f(l_2, n) &= 2 \sum_{\substack{\frac{1}{4} < \frac{2l-1}{2^{n+1}} < \frac{3}{4} \\ n_1=1, n_2=n}} f(l, n) = 4r(n).
 \end{aligned}$$

Вторая сумма может быть оценена снизу, поскольку значения l_2 , удовлетворяющие неравенствам $\frac{1}{4} < \frac{3}{4} \cdot \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4}$, эквивалентным неравенствам $\frac{1}{3} < \frac{2l_2-1}{2^{n_2}} < 1$, заведомо включают множество значений l_2 ,

удовлетворяющих $\frac{1}{2} < \frac{2l_2-1}{2^n}$:

$$\begin{aligned} 2 \sum_{\substack{\frac{1}{4} < \frac{3}{4} \cdot \frac{2l_2-1}{2^{n-1}+1} < \frac{3}{4} \\ \frac{1}{4} < \frac{3}{4} \cdot \frac{2l_1-1}{2^n} < \frac{3}{4}}} f(2, 1)f(l_2, n-1) &= 2 \sum f(l_2, n-1) \geq \\ &\geq 2 \sum_{\frac{2l_1-1}{2^n} > \frac{1}{2}} f(l, n-1) = 2 \cdot \frac{1}{2} 2^{n-1} c_{n-1} = 2^{n-1} c_{n-1}. \end{aligned}$$

Наконец, рассмотрим третью сумму (отметим, что она содержит какие-либо слагаемые только если $n \geq 4$). Множество значений l_1, n_1 и l_2, n_2 , удовлетворяющих неравенствам $\frac{1}{4} < \frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4}$ заведомо включает наборы, удовлетворяющие соотношениям:

$$\left[\begin{array}{l} \frac{1}{2} < \frac{2l_1-1}{2^{n_1+1}} < \frac{3}{4}, \frac{3}{4} < \frac{2l_2-1}{2^{n_2+1}} < 1; \\ \frac{1}{2} < \frac{2l_1-1}{2^{n_1+1}} < \frac{3}{4}, \frac{1}{2} < \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4}; \\ \frac{3}{4} < \frac{2l_1-1}{2^{n_1+1}} < 1, \frac{1}{2} < \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4}. \end{array} \right.$$

В силу симметрии первого и третьего варианта в совокупности выше, получаем следующую нижнюю оценку:

$$\begin{aligned} \sum_{\substack{n_1+n_2=n, \\ n_1>1, n_2>1, \\ \frac{1}{4} < \frac{2l_1-1}{2^{n_1+1}} \cdot \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4}}} f(l_1, n_1)f(l_2, n_2) &\geq 2 \sum_{\substack{n_1+n_2=n, \\ n_1>1, n_2>1, \\ \frac{1}{2} < \frac{2l_1-1}{2^{n_1+1}} < \frac{3}{4}, \frac{2l_2-1}{2^{n_2+1}} > \frac{3}{4}}} f(l_1, n_1)f(l_2, n_2) + \\ &+ \sum_{\substack{n_1+n_2=n, \\ n_1>1, n_2>1, \\ \frac{1}{2} < \frac{2l_1-1}{2^{n_1+1}} < \frac{3}{4}, \frac{1}{2} < \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4}}} f(l_1, n_1)f(l_2, n_2) = \\ &= 2 \sum_{\substack{n_1+n_2=n, \\ n_1>1, n_2>1}} \left(\sum_{\frac{1}{2} < \frac{2l_1-1}{2^{n_1+1}} < \frac{3}{4}} f(l_1, n_1) \right) \left(\sum_{\frac{2l_2-1}{2^{n_2+1}} > \frac{3}{4}} f(l_2, n_2) \right) + \\ &+ \sum_{\substack{n_1+n_2=n, \\ n_1>1, n_2>1}} \left(\sum_{\frac{1}{2} < \frac{2l_1-1}{2^{n_1+1}} < \frac{3}{4}} f(l_1, n_1) \right) \left(\sum_{\frac{1}{2} < \frac{2l_2-1}{2^{n_2+1}} < \frac{3}{4}} f(l_2, n_2) \right) = \\ &= \sum_{\substack{n_1+n_2=n, \\ n_1>1, n_2>1}} (2r(n_1)q(n_2)+r(n_1)r(n_2)) = \sum_{k=2}^{n-2} r(k) \left(q(n-k) + \frac{1}{2} 2^{n-k} c_{n-k} \right). \end{aligned}$$

Объединяя все полученные оценки, получаем следующее утверждение.

Лемма 3. При $n \geq 2$ выполнено неравенство:

$$r(n+1) \geq 4r(n) + 2^{n-1}c_{n-1} + \frac{1}{2} \sum_{k=2}^{n-2} r(k)2^{n-k}c_{n-k} + \sum_{k=2}^{n-2} r(k)q(n-k).$$

4. Асимптотические оценки

Для получения дальнейших результатов воспользуемся аппаратом производящих функций и подходом, систематизированным Ф. Флажолем и Р. Седжевиком в монографии *Аналитическая комбинаторика* [4]. Этот подход заключается в рассмотрении производящих функций как комплексных функций комплексного переменного. При этом асимптотическое поведение коэффициентов производящей функции оказывается связанным с поведением функции в особых точках, находящихся на границе круга сходимости степенного ряда функции, представляющего ее разложение в точке $z = 0$. Эта связь, в частности, формализуется следующей теоремой, непосредственно используемой в дальнейших рассуждениях.

Теорема 2 (Флажолем—Одлыжко [5]). Пусть функция $f(z) = \sum_{n=0}^{\infty} f_n z^n$ аналитическая в круге радиуса $R > 1$ с центром в точке $z = 0$, рассеченной вдоль действительной оси правее точки $z_0 = 1$. Пусть при этом в окрестности точки $z_0 = 1$ выполнено равенство $f(z) = O((1-z)^{-\alpha})$ где $\alpha \in \mathbb{R}$. Тогда при $n \rightarrow \infty$ имеет место равенство $f_n = O(n^{\alpha-1})$.

Теорема 2 применима в случае, когда $z_0 = 1$ — единственная особая точка на границе круга сходимости функции $f(z)$, однако, как несложно понять, замена переменной в функции $f(z)$ позволяет обобщить теорему на случай, когда единственная особая точка на границе круга сходимости есть $\omega \in \mathbb{R}^+$. В этом случае при выполнении в окрестности $z_0 = \omega$ равенства $f(z) = O((1-\omega z)^{-\alpha})$ коэффициенты f_n будут удовлетворять асимптотическому равенству $f_n = O(\omega^{-n} n^{\alpha-1})$.

Перейдем к получению асимптотических оценок величин $q(n)$ и $r(n)$. Положим $d_n = 2^n c_n$, тогда производящая функция этой последовательности $D(z) = \sum_{n=0}^{\infty} d_n z^n$ удовлетворяет уравнению $D(z) = 1 + 2zD^2(z)$ и может быть выражена следующим образом: $D(z) = \frac{1}{4z}(1 - \sqrt{1-8z})$, где квадратный корень понимается как одна из ветвей соответствующей многозначной аналитической функции (та, которая, в соответствии

с комбинаторным смыслом функции $D(z)$, обеспечивает, что коэффициенты ее разложения в степенной ряд по степеням z действительные и неотрицательные).

Определим последовательность κ_n , положив $\kappa_0 = 0$, $\kappa_1 = 1$ и далее для $n \geq 1$:

$$\kappa_{n+1} = \frac{1}{8}d_{n+1} + \frac{1}{2}d_n + \sum_{k=1}^{n-1} d_k \kappa_{n-k}, \quad (8)$$

где при $n = 1$ сумма в соотношении выше считается нулевой. Тогда из леммы 2 и определения κ_n индукцией по n легко выводится соотношение $q(n) \geq \kappa_n$.

Аналогично определим последовательность ρ_n , положив $\rho_0 = \rho_1 = 0$, $\rho_2 = 2$ и далее для $n \geq 2$:

$$\rho_{n+1} = 4\rho_n + d_{n-1} + \frac{1}{2} \sum_{k=2}^{n-2} \rho_k d_{n-k} + \sum_{k=2}^{n-2} \rho_k \kappa_{n-k}, \quad (9)$$

где суммы считаются нулевыми, если верхний предел меньше нижнего. Из леммы 3 и определения последовательности ρ_n также как и в случае выше вытекает, что $r(n) \geq \rho_n$.

С учетом значений последовательностей κ_n , ρ_n и d_n при $n = 0$ и $n = 1$ рекуррентные соотношения (8) и (9) могут быть преобразованы следующим образом:

$$\begin{aligned} \kappa_{n+1} &= \frac{1}{8}d_{n+1} + \frac{1}{2}d_n + \sum_{k=0}^n d_k \kappa_{n-k} - \kappa_n, \\ \rho_{n+1} &= 4\rho_n + d_{n-1} + \frac{1}{2} \left(\sum_{k=0}^n \rho_k d_{n-k} - 2\rho_{n-1} - \rho_n \right) + \sum_{k=0}^n \rho_k \kappa_{n-k} - \rho_{n-1}, \end{aligned}$$

что после дополнительных преобразований дает:

$$\begin{aligned} \kappa_{n+1} + \kappa_n &= \frac{1}{8}d_{n+1} + \frac{1}{2}d_n + \sum_{k=0}^n d_k \kappa_{n-k}, \\ \rho_{n+1} + 2\rho_{n-1} &= \frac{7}{2}\rho_n + d_{n-1} + \frac{1}{2} \sum_{k=0}^n \rho_k d_{n-k} + \sum_{k=0}^n \rho_k \kappa_{n-k}. \end{aligned}$$

Введем производящие функции последовательностей κ_n и ρ_n , положив $K(z) = \sum_{n=0}^{\infty} \kappa_n z^n$ и $R(z) = \sum_{n=0}^{\infty} \rho_n z^n$. Умножив соотношения выше на z^{n+1}

и просуммировав по n , приходим к равенствам:

$$\begin{aligned} K(z) - z + zK(z) &= \frac{1}{8}(D(z) - 2z - 1) + \frac{1}{2}z(D(z) - 1) + zD(z)K(z), \\ R(z) - 2z^2 + 2z^2R(z) &= \frac{7}{2}zR(z) + z^2(D(z) - 1) + \frac{1}{2}zR(z)D(z) + zR(z)K(z). \end{aligned}$$

Эти равенства можно переписать в виде:

$$\begin{aligned} (1+z)K(z) &= \frac{1}{4}z - \frac{1}{8} + \frac{1}{8}D(z) + \frac{1}{2}zD(z) + zD(z)K(z), \\ (1+2z^2)R(z) &= z^2 + \frac{7}{2}zR(z) + z^2D(z) + \frac{1}{2}zR(z)D(z) + zR(z)K(z). \end{aligned}$$

Из полученных соотношений и явного представления для функции $D(z)$, приведенного ранее, могут быть выведены явные выражения для функций $K(z)$ и $R(z)$, из которых непосредственно вытекает, что у обеих функций, как и у функции $D(z)$ ближайшей к нулю особой точкой является $z_0 = \frac{1}{8}$, и других особых точек на границе круга сходимости нет. Более того, у каждой из этих функций точка $z_0 = \frac{1}{8}$ также как и у функции $D(z)$ является точкой ветвления второго порядка.

Согласно теореме Ньютона—Пуизё (подробнее см. [4]) для функций $D(z)$, $K(z)$ и $R(z)$ в окрестности точки $z_0 = \frac{1}{8}$ имеют место представления:

$$\begin{aligned} D(z) &= \delta_0 + \delta_1\sqrt{1-8z} + o(\sqrt{1-8z}), \\ K(z) &= k_0 + k_1\sqrt{1-8z} + o(\sqrt{1-8z}), \\ R(z) &= r_0 + r_1\sqrt{1-8z} + o(\sqrt{1-8z}), \end{aligned}$$

где $\delta_0 = D\left(\frac{1}{8}\right)$, $k_0 = K\left(\frac{1}{8}\right)$, $r_0 = R\left(\frac{1}{8}\right)$. Эти значения могут быть легко найдены с помощью имеющихся уравнений, путем подстановки в них значения $z = \frac{1}{8}$. В результате получим $\delta_0 = 2$, $k_0 = \frac{9}{28}$, $r_0 = \frac{7}{64}$.

Соотношения между δ_1 , k_1 и r_1 могут быть получены подстановкой разложений функций в уравнения и приравниванием коэффициентов

при $\sqrt{1-8z}$. Продемонстрируем это для функции $K(z)$:

$$\begin{aligned} & \left(1 + \frac{1}{8} - \frac{1}{8}(1-8z)\right) (k_0 + k_1\sqrt{1-8z} + o(\sqrt{1-8z})) = \\ & = \frac{1}{8}(\delta_0 + \delta_1\sqrt{1-8z} + o(\sqrt{1-8z}) - 1) + \\ & + \left(\frac{1}{8} - \frac{1}{8}(1-8z)\right) \left(\frac{1}{4} + \frac{1}{2}\delta_0 + \frac{1}{2}\delta_1\sqrt{1-8z} + o(\sqrt{1-8z}) + \right. \\ & \left. + (\delta_0 + \delta_1\sqrt{1-8z} + o(\sqrt{1-8z}))(k_0 + k_1\sqrt{1-8z} + o(\sqrt{1-8z}))\right). \end{aligned}$$

Тогда соотношение между коэффициентами при $\sqrt{1-8z}$ в правой и левой частях имеет вид:

$$\frac{9}{8}k_1 = \frac{1}{8}\delta_1 + \frac{1}{8}\left(\frac{1}{2}\delta_1 + \delta_0k_1 + \delta_1k_0\right),$$

откуда $7k_1 = \left(\frac{3}{2} + \frac{9}{28}\right)\delta_1$, что влечет $\frac{k_1}{\delta_1} = \frac{51}{196} = \frac{51}{49} \cdot \frac{1}{4} \approx 0,26$.

Выполняя аналогичные преобразования в уравнении, связывающем $R(z)$, приходим к соотношению:

$$\left(1 + 2 \cdot \frac{1}{8^2}\right)r_1 = \frac{7}{2} \cdot \frac{1}{8}r_1 + \frac{1}{8^2}\delta_1 + \frac{1}{2} \cdot \frac{1}{8}(r_1\delta_0 + r_0\delta_1) + \frac{1}{8}(r_1k_0 + r_0k_1),$$

из которого получаем, что $\frac{r_1}{\delta_1} = \frac{373}{6144} = \frac{373}{384} \cdot \frac{1}{16} \approx 0,06$.

Согласно теореме Флажолле—Одльжко асимптотика роста значений последовательностей d_n , κ_n и ρ_n совпадает с асимптотикой роста коэффициентов функции $\sqrt{1-8z}$ умноженной, соответственно, на δ_1 , k_1 и r_1 . Как следствие получаем, что выполнены асимптотические соотношения:

$$\frac{\kappa_n}{d_n} \sim \frac{k_1}{\delta_1} = \frac{51}{196}, \quad \frac{\rho_n}{d_n} \sim \frac{r_1}{\delta_1} = \frac{373}{6144}.$$

Поскольку для последовательности d_n имеется явное выражение через числа Каталана, для величин $q(n)$ и $r(n)$ в силу определений последовательностей κ_n и ρ_n получаем следующие асимптотические (при $n \rightarrow \infty$) оценки:

$$q(n) \gtrsim \frac{51}{196}2^n c_n, \quad r(n) \gtrsim \frac{373}{6144}2^n c_n.$$

С учетом равенства $q(n)+r(n) = \frac{1}{2}2^n c_n$, можно дополнить нижние оценки верхними.

Теорема 3. При $n \rightarrow \infty$ имеют место асимптотические неравенства:

$$\frac{51}{196} \lesssim \frac{q(n)}{2^n c_n} \lesssim \frac{2699}{6144}, \quad \frac{373}{6144} \lesssim \frac{r(n)}{2^n c_n} \lesssim \frac{37}{196}.$$

Полученные оценки очевидно не являются окончательными, однако даже они позволяют сделать некоторые выводы о поведении величин $f(l, n)$. В частности, гипотеза о приближении с ростом n распределения значений $f(l, n)$ к какому-либо «равномерному», явно опровергается вытекающей из теоремы 3 оценкой $q(n) \gtrsim \frac{51}{196} > \frac{1}{4}$.

Дальнейшее уточнение оценок теоремы 3, по-видимому, возможно путем более детального рассмотрения способов представления двоичных дробей в виде произведений. Продвижение на этом пути, возможно, позволит применить аналогичные методы для оценки при растущем n сумм вида $\sum_{\frac{t_1}{2^m} 2^n < l < \frac{t_2}{2^m} 2^n} f(l, n)$, где $m > 2$ — фиксированное число.

Список литературы

- [1] Golomb M. C., Gurvich V. A., *Boolean Functions: Theory, Algorithms and Applications*, eds. Crama Y., Hammer P.L., Cambridge University Press, Cambridge, 2011.
- [2] Схиртладзе Р. Л., “О синтезе р-схемы из контактов со случайными дискретными состояниями”, *Сообщ. АН ГрузССР*, **26:2** (1961), 181–186.
- [3] Яшунский А. Д., “Об асимптотике вероятности значений случайных булевых выражений”, *Дискретн. анализ и исслед. опер., сер. 1*, **13:2** (2006), 59–99.
- [4] Flajolet Ph., Sedgewick R., *Analytic combinatorics*, Cambridge University Press, New York, NY, USA, 2009.
- [5] Flajolet Ph., Odlyzko A. M., “Singularity analysis of generating functions”, *SIAM Journal on Algebraic and Discrete Methods*, **3:2** (1990), 216–240.

On the weight of functions, defined by read-once AND/OR formulas

Eremenko A.R., Yashunsky A.D.

We consider the set of functions defined by read-once formulas with binary conjunction (logical AND) and disjunction (logical OR) operations. For the functions defined by formulas with a fixed number of operations we investigate the weights of functions, i.e. the number of tuples on which the function has value 1. We establish asymptotic

bounds on the number of read-once formulas that define functions with specific weights, in particular on the number of formulas, that define functions with no more than a quarter of ones among their values.

Keywords: Boolean function, read-once formula, function weight, asymptotic bound.

Коды, определяющие изображения с точностью до аффинных преобразований

В.Н. Козлов

В работе представлены коды, задающие изображения с точностью до аффинных преобразований, в том числе некоторый новый код.

Ключевые слова: распознавание образов, изображения, коды изображения.

Изображением называем конечное (непустое) множество точек в евклидовых пространствах разной размерности. В частности, двумерное изображение – конечное множество точек на плоскости. Считаем, что любую фигуру можно «аппроксимировать» конечным множеством точек, которые уже сами по себе делают фигуру вполне узнаваемой. При этом если точек много, то такая совокупность точек практически неотличима от исходной фигуры. Так же можно представлять и полутоновые, черно-бело-серые изображения, при этом разная плотность точек в разных частях изображения дает разные оттенки «серого цвета». Как известно, цветное изображение можно представлять как наложение трех монохроматических (аналогов черно-бело-серых) изображений. Это означает, что совокупностями точек можно представлять и цветные изображения. Трехмерные изображения – точки в трехмерном евклидовом пространстве. Соотнесение между трехмерным изображением и двумерными, являющимися их проекциями, приводит к задачам восстановления тел по плоским проекциям и смежным задачам. Наконец, трехмерный мир в динамике можно рассматривать как четырехмерное изображение (последовательность трехмерных сцен).

Далее рассматриваются двумерные изображения, но сказанное может быть обобщено и на случаи большей размерности.

Перенумеруем некоторым образом точки изображения A так, чтобы номера разных точек были попарно различны. Обозначим через M_A множество этих номеров. Пусть S_{mnu} и S_{kps} – площади треугольников с вершинами в тройках точек с номерами m, n, u и k, p, s и пусть

$\rho_{mnu,kps} = S_{mnu}/S_{kps}$. Полагаем, что порядок номеров в тройках не важен, сами тройки различны и при $S_{kps} = 0$ значение $\rho_{mnu,kps}$ не определено. Множество индексированных чисел $\rho_{mnu,kps}$ для всех таких пар троек обозначим через T_A . Код изображения A – пара $\langle M_A, T_A \rangle$. Изображения A и B с кодами $\langle M_A, T_A \rangle$ и $\langle M_B, T_B \rangle$ назовем эквивалентными, если существует такая биекция $\psi: M_A \rightarrow M_B$, что для любых m, n, u и k, p, s из M_A выполнено $\rho_{mnu,kps} = \rho_{\psi(m)\psi(n)\psi(u),\psi(k)\psi(p)\psi(s)}$. Ясно, что эквивалентность изображений содержательно означает одинаковость их кодов с точностью до перенумерации точек.

Два изображения называем аффинно эквивалентными, если они переводимы друг в друга аффинными преобразованиями. Если все точки изображения не лежат на одной прямой или двух параллельных прямых, то изображение называем плоским.

Теорема 1 [1]. Два плоских изображения эквивалентны точно тогда, когда они аффинно эквивалентны.

Содержательно теорема 1 означает, в частности, что код изображения задает его с точностью до аффинных преобразований.

Назовем изображения A и B пропорциональными, если существует такая биекция $\psi: M_A \rightarrow M_B$, при которой для любых точек с номерами m, n, u из M_A (не лежащих на одной прямой), число $\rho_{mnu,\psi(m)\psi(n)\psi(u)}$ есть константа, не зависящая от выбора точек m, n, u .

Теорема [2]. Два плоских изображения пропорциональны тогда и только тогда, когда они аффинно эквивалентны.

Числа $\rho_{mnu,\psi(m)\psi(n)\psi(u)}$ из определения пропорциональности не являются элементами кода ни изображения A , ни изображения B . Однако они являются элементами кода изображения S , которое трактуется как среда, и включающего изображения A и B как части. Под этим понимается следующее. Изображение A (или B) называется частью среды S , если точки, составляющие A , есть подмножество точек из S . Если код для S есть $\langle M_S, T_S \rangle$, то, очевидно, код $\langle M_A, T_A \rangle$ можно получить, если собрать в M_A номера из M_S всех точек, вошедших в A , и собрав в T_A все те $\rho_{mnu,kps} = S_{mnu}/S_{kps}$ из T_S , для которых m, n, u, k, s, p вошли в M_A . Говорим в этом случае, что код $\langle M_A, T_A \rangle$ есть часть кода $\langle M_S, T_S \rangle$. В этом случае константные $\rho_{mnu,\psi(m)\psi(n)\psi(u)}$ из определения пропорциональности являются элементами кода среды S .

Известны [3,4] результаты о том, что для каждого выпуклого многоугольника (k вершин, $k > 2$) существует и единственен наименьший по площади эллипс, в который этот многоугольник вписывается. Используем это для построения некоторого нового кода изображения.

Лемма 1. Пусть S_t – площадь треугольника с вершинами в точках a, b, c , не лежащих на одной прямой, E – наименьший по площади эллипс, в который вписан треугольник, S_e – площадь эллипса. Тогда отношение площадей S_e и S_t есть константа, не зависящая от треугольника.

Доказательство. Аффинными преобразованиями сделаем треугольник правильным. Эти же преобразования переводят эллипс E в эллипс E' . Поскольку отношения площадей при аффинных преобразованиях сохраняются, то E' – тоже наименьший по площади эллипс, в который вписан преобразованный треугольник, и единственный. Отсюда E' – описанная окружность для правильного треугольника. Действительно, положим, что E' отличен от окружности. Тогда, в силу симметрии треугольника, существуют еще два эллипса E'' и E''' с той же (и значит, минимальной) площадью, в которые вписан треугольник, а это противоречит единственности эллипса. Отношение площадей описанной окружности и правильного треугольника и будут той константой, о которой говорится в формулировке. Лемма доказана.

Пусть теперь A – изображение, M_A^e – множество попарно различных номеров точек в A , S_{mnu}^e и S_{kps}^e – площади наименьших (по площади) эллипсов описанных вокруг треугольников с вершинами в точках соответственно m, n, u и k, p, s , и пусть $\rho_{mnu, kps}^e = S_{mnu}^e / S_{kps}^e$. Полагаем, что порядок номеров в тройках не важен, сами тройки различны и при $S_{kps}^e = 0$ значение $\rho_{mnu, kps}^e$ не определено. Множество индексированных чисел $\rho_{mnu, kps}^e$ для всех таких пар троек обозначим через T_A^e . Эллипс-код изображения A – пара $\langle M_A^e, T_A^e \rangle$. Изображения A и B с кодами $\langle M_A^e, T_A^e \rangle$ и $\langle M_B^e, T_B^e \rangle$ назовем эллипс-эквивалентными, если существует такая биекция $\psi: M_A^e \rightarrow M_B^e$, что для любых m, n, u и k, p, s из M_A^e выполнено $\rho_{mnu, kps}^e = \rho_{\psi(m)\psi(n)\psi(u), \psi(k)\psi(p)\psi(s)}^e$. Ясно, что эллипс-эквивалентность изображений содержательно означает одинаковость их эллипс-кодов с точностью до перенумерации точек.

Из теоремы 1 и леммы 1 с очевидностью проистекает следующее утверждение.

Теорема 3. Два плоских изображения эллипс-эквивалентны точно тогда, когда они аффинно эквивалентны.

Список литературы

- [1] В.Н. Козлов, *Введение в математическую теорию зрительного восприятия*, Издательство Центра прикладных исследований при механико-математическом факультете МГУ, М., 2007.

- [2] В.Н. Козлов, “Алгоритмы формирования системы взаимосвязанных образов”, *Интеллектуальные системы*, **18**, 2014, 99-114.
- [3] Л. Данцер , Б. Грюнбаум , В. Кли, *Теорема Хелли и ее применения*, Издательство «Мир», М., 1968.
- [4] В.Л. Загускин, “Об описанных и вписанных эллипсоидах экстремального объема”, *Успехи математических наук*, **13**, 1958, 89-93.

Codes that define images accurate to affine transformations
V.N. Kozlov

The paper presents codes that define images with an accuracy of affine transformations, including some new code.

Keywords: pattern recognition, images, image codes.

Сложность синтеза многомерных прямоугольных схем

Сытдыков Т. Р.

В данной статье рассматривается модель прямоугольных многомерных схем. Элементы схем расположены в ячейках d -мерной прямоугольной решетки. Каждая пара соседних ячеек решетки соединена шиной, в которой может быть до k проводов. Доказана верхняя оценка функции Шеннона для сложности данного вида схем $\frac{2^n}{\min(n, d \log k)}$.

Ключевые слова: многомерные схемы, многослойные схемы, асимптотика функции Шеннона, сложность схем.

1. Введение

Задача синтеза схем, вычисляющих булевы функции и обладающих в некотором смысле оптимальными или субоптимальными характеристиками, возникла в середине XX века в связи с бурным развитием вычислительной техники. С 1950-х гг. одной из наиболее интенсивно исследуемых моделей схем являются схемы из функциональных элементов (СФЭ). Одной из естественных характеристик оптимальности СФЭ является сложность — количество функциональных элементов в схеме. Соответственно, сложность булевой функции можно определить как минимальную сложность схемы, реализующей данную функцию. Маллер в [16] показал, что для любой булевой функции от n переменных порядок ее сложности не превосходит $\frac{2^n}{n}$. Лупанов в [13] доказал, что для почти всех булевых функций от n переменных сложность в стандартном базисе $\{\vee, \&, \neg\}$ асимптотически равна $\frac{2^n}{n}$. Также Лупанов получил асимптотические оценки сложности булевых функций для произвольного конечного базиса.

На практике, однако, при синтезе схем необходимо учитывать такие моменты, как расположение функциональных элементов в пространстве, разводку проводов и др. В 1960-х гг. появились работы, в которых рассматривались модели схем, в той или иной степени учитывающие эти

факторы. Коршунов в [11] получил оценки сложности для случая СФЭ, размещенных в трехмерном пространстве с ограниченными снизу расстояниями между элементами и проводами, а также ограниченными сверху длинами проводов. Кравцов в [10] рассматривал плоские схемы, элементы которых определенным образом размещены в клетках прямоугольной решетки, и получил порядок функции Шеннона 2^n . Модели клеточных схем, аналогичные или идентичные модели Кравцова, рассматривались в ряде более поздних работ. Так, Альбрехт в [1] показал, что асимптотика функции Шеннона для клеточных схем имеет вид $c \cdot 2^n$, где c — некоторая константа, зависящая от базиса. Грибок в [3] получил асимптотику функции Шеннона 2^n для определенного базиса клеточных элементов. Калачев в [5, 6, 7, 8, 9] исследовал одновременную минимизацию сложности и других характеристик плоских схем (мощность и глубина). Ефимов в [2] изучал энергопотребление объемных схем.

Оценки порядка и асимптотики сложности, полученные для перечисленных выше моделей плоских или объемных схем, превосходят по порядку оценку Лупанова $\frac{2^n}{n}$ сложности для СФЭ. В связи с этим интерес представляет задача обобщения модели плоских либо пространственных схем определенным образом так, чтобы, с одной стороны, уменьшить порядок функции Шеннона, с другой стороны, оставить модель в некотором смысле естественной, приближенной к реально существующим схемам.

В данной статье исследуется один из вариантов подобного обобщения модели клеточных схем. Рассматриваются СФЭ над базисом $P_2(2)$, элементы которых размещены в ячейках d -мерной целочисленной решетки, где $d \geq 2$. При этом в каждой ячейке может быть расположено не более одного функционального элемента СФЭ, реализующего нетождественную функцию. Кроме того, каждая пара соседних ячеек соединена шиной, состоящей из не более чем k проводов. Таким образом, прямоугольные многомерные схемы представляют собой семейство моделей схем с двумя параметрами — d и k .

В [14] была получена асимптотика функции Шеннона сложности для случая $d = 2$, а также доказана нижняя оценка для более общей модели k -слойных схем с планарным носителем. В данной статье для $d \geq 2$ будет получена верхняя оценка функции Шеннона сложности прямоугольных многомерных схем при $k \rightarrow \infty$.

Автор выражает благодарность к.ф.-м.н. Г.В.Калачеву за научное руководство, постановку задачи и ценные замечания, а также д.ф.-м.н. профессору Э.Э.Гасанову за помощь в работе.

2. Основные определения, постановка задачи и результаты

2.1. Схемы, их укладки и технологические ограничения

Согласно [15, с. 148], схема из функциональных элементов (далее СФЭ) в базисе $B \subseteq P_2$ представляет собой размеченный ациклический ориентированный граф. Разметка вершин определяет, какие вершины являются входными или выходными, и всем вершинам, не являющимся входными, сопоставляет булевы функции из базиса B . Ребра СФЭ помечены натуральными числами, и разметка входных ребер вершины определяет порядок аргументов в функции, реализуемой данной вершиной.

Для СФЭ S через $G(S)$ обозначим граф, полученный из СФЭ удалением разметки, а через $V(S)$ и $E(S)$ обозначим соответственно множества вершин и ребер СФЭ.

Носителем будем называть произвольный непустой граф с конечным или счетным числом вершин.

Для удобства будем считать, что

- все вершины всех СФЭ принадлежат некоторому множеству \mathcal{V}_S , а ребра — множеству \mathcal{E}_S ;
- все вершины всех носителей принадлежат некоторому множеству \mathcal{V}_T , а ребра — множеству \mathcal{E}_T ;
- разметка вершин и ребер СФЭ обозначается через $\ell(x)$, где x — вершина или ребро СФЭ.

Укладкой СФЭ S на носитель T будем называть произвольный гомоморфизм $h: G(S) \rightarrow T$.

Схемой с носителем T будем называть пару $K = (S, h)$, где S — схема из функциональных элементов, а h — ее укладка на T . Множество схем с носителем T обозначим через $\mathcal{C}(T)$. Элементами (вершинами) схемы будем называть элементы образа $h(V(S))$. Множество элементов будем обозначать через $V(K)$, а также через $V(S, h)$. Для краткости будем говорить «схема» вместо «схема с носителем» в тех случаях, когда это не приведет к разночтениям.

Будем говорить, что схема $K = (S, h)$ *реализует* булеву функцию или булев оператор f , если соответствующая СФЭ S реализует f .

Обычно в задачах синтеза схем имеются те или иные ограничения на укладку. Такие ограничения задают подмножество допустимых укла-

док. Ограничения могут формулироваться как для конкретного носителя, так и для класса носителей. Для упрощения определения операций над ограничениями формально можно считать, что ограничения всегда относятся ко всем носителям, но для некоторых носителей множество укладок пусто.

Итак, ограничение (глобальное) на укладку представляет собой функцию U , которая паре (S, T) ставит в соответствие некоторое множество $U(S, T) \subseteq \text{Hom}(G(S), T)$ допустимых укладок S в T , где S — СФЭ, T — носитель.

Важным классом ограничений являются технологические (локальные) ограничения. Ограничение на укладку называется *технологическим (локальным)*, если оно может быть описано в терминах ограничения на прообраз вершин и ребер носителя. Формально, локальное ограничение задается парой предикатов (p_V, p_E) , где $p_V : 2^{V_S} \rightarrow \{0, 1\}$, $p_E : 2^{E_S} \rightarrow \{0, 1\}$. Локальное ограничение $U = (p_V, p_E)$ задает глобальное ограничение U' :

$$U'(S, T) = \left\{ h \in \text{Hom}(S, T) \mid \begin{array}{l} \forall v \in h(V(S)) \ p_V(h^{-1}(v)), \\ \forall e \in h(E(S)) \ p_E(h^{-1}(e)) \end{array} \right\}.$$

Введем несколько базовых локальных ограничений.

- Ограничение на базис:

$$bs(B) = (p_B, \top), \quad p_B(s) \Leftrightarrow \forall v \in s \ (\ell(v) \in B),$$

которое выражает свойство «любая вершина из прообраза реализует функцию из множества B ». Здесь и далее \top означает тождественно истинный предикат.

- Ограничение на число проводов, идущих по одному ребру:

$$wt_e(k) = (\top, p_E), \quad p_E(s) \Leftrightarrow |s| \leq k,$$

которое выражает свойство «в каждое ребро носителя может отображаться не более k ребер СФЭ».

- Аналогичное ограничение на число нетождественных элементов в вершине:

$$wt_f(k) = (p_V, \top), \quad p_V(s) \Leftrightarrow |\{v \in s \mid \ell(v) \neq I_1^1\}| \leq k.$$

Здесь I_1^1 — тождественная булева функция.

Для локальных ограничений можно покомпонентно определить булевы операции. Например,

$$(p_V^1, p_E^1) \& (p_E^2, p_E^2) := (p_V^1 \& p_V^2, p_E^1 \& p_E^2);$$

2.2. Модели схем

Моделью схем будем называть пару $M = (T, U)$, где T — носитель, U — ограничение на укладку.

Будем говорить, что схема (S, h) *соответствует модели схем* $M = (T, U)$, если T является носителем схемы и $h \in U(S, T)$. Множество схем, соответствующих модели M , будем обозначать через $\mathcal{C}(M)$; также будем использовать словосочетание «схема в модели M » для любой схемы из $\mathcal{C}(M)$.

Основная часть данной работы будет главным образом посвящена изучению некоторых свойств модели схем, определенной ниже — прямоугольных многомерных схем.

Прямоугольные многомерные схемы. Пусть $d \geq 2$ — целое положительное число. Рассмотрим граф d -мерной целочисленной решетки \mathbb{Z}^d , в котором вершины смежны тогда и только тогда, когда расстояние между ними равно 1 (для краткости будем обозначать данный граф также через \mathbb{Z}^d). Определим модель прямоугольным многомерных схем $M_k^d = (\mathbb{Z}^d, U_k)$, где

$$U_k = wt_e(k)bs(P_2(2))wt_f(1).$$

Здесь базис $P_2(2)$ есть множество всех булевых функций от двух переменных. Для простоты в качестве функций базиса мы будем использовать и булевы функции от одной переменной, подразумевая при этом, что используется соответствующая функция от двух переменных с отождествленными входами.

Таким образом, в каждое ребро прямоугольной многомерной схемы может быть отображено не более k ребер исходной СФЭ, а в каждую вершину — не более одного элемента СФЭ, реализующего нетождественную функцию.

Далее мы будем использовать сокращение *схемы* для прямоугольных многомерных схем в тех случаях, когда это не вызовет разночтений.

2.3. Сложность схем

Для схемы $K = (S, h)$ подмножество носителя $h(V(S))$ будем называть *образом* схемы K .

Под *сложностью* схемы будем понимать количество вершин ее образа. Для сложности схемы K будем использовать обозначение $L(K)$.

Множество всех схем в модели M , реализующих булеву функцию или оператор f , обозначим через $\mathcal{C}(M, f)$.

Пусть f — булева функция, M — модель схем. Определим сложность функции f в модели M :

$$L(M, f) := \min_{K \in \mathcal{C}(M, f)} L(K).$$

В случае, если не существует схемы в модели M , реализующей f , будем формально считать, что $L(M, f) = \infty$.

Введем функцию Шеннона сложности реализации булевых функций в модели M :

$$L(M, n) := \max_{f \in P_2(n)} L(M, f),$$

где $P_2(n)$ — множество булевых функций от n переменных.

2.4. Соглашения при изображении схем

В процессе доказательства будет необходимо изображать укладки схем и другие конструкции.

В двумерном случае будем стараться рисовать укладки максимально приближенно к изображениям клеточных схем, принятым в литературе, например в [10, 6]. Границы между клетками схем будем изображать пунктирными линиями, соединения между элементами — сплошными линиями с, возможно, стрелками, поясняющими ориентацию соответствующих ребер СФЭ.

Как и принято в литературе, будем называть линии соединений проводами, их параллельную группу — шиной, число проводов в шине — ее толщиной. Для простоты будем опускать элемент тождественной функции, соединяя его вход и выход в один непрерывный провод. Таким образом, провода в изображениях схем могут соединять элементы, расположенные в удаленных друг от друга ячейках решетки. Для удобства будем изображать шину одной толстой линией вместо группы из нескольких тонких.

2.5. Прочие обозначения и соглашения

Выражение $\log a$ всюду будет обозначать двоичный логарифм a вместо десятичного.

2.6. Полученные результаты

В данной статье для прямоугольных многомерных схем будет доказана верхняя оценка функции Шеннона $L(M_k^d, n)$.

$$L(M_k^d, n) \lesssim \frac{2^n}{\min(n, d \log k)} \quad \text{при } k \rightarrow \infty, n \rightarrow \infty.$$

3. Верхняя оценка функции Шеннона

В данном разделе будет получена верхняя оценка функции Шеннона для модели прямоугольных d -мерных схем:

$$L(M_k^d, n) \lesssim \frac{2^n}{\min(n, d \log k)} \quad \text{при } k \rightarrow \infty, n \rightarrow \infty.$$

Во всех утверждениях этого раздела в отсутствии каких-либо ограничений на d будем считать, что $d \geq 2$. Для различения вершин графа носителя, графа СФЭ и вспомогательных графов, которые будут использованы при доказательствах, вершины графа d -мерной решетки будем также называть *ячейками*.

Будем использовать несколько вспомогательных лемм. Предварительно введем следующее определение.

Пусть T — некоторый носитель, G — некоторый мультиграф, такой, что $V(G) \subseteq V(T)$. Пусть $Path(T)$ — множество путей в T . Под *разводкой проводов графа G в модели M_k^T* будем понимать отображение $h: E(G) \rightarrow Path(T)$, удовлетворяющее следующим условиям:

- Если $e_g = \{a, b\} \in E(G)$, то $h(e_g)$ — некоторый путь, соединяющий вершины a и b .
- Если $e_t \in E(T)$, то количество путей, являющихся образами ребер графа G и проходящих через e_t (с учетом кратности), не превосходит k .

Для краткости мы будем говорить о *разводке проводов* без упоминания графа и модели схем, если из контекста ясно, о каких графе и модели схем речь.

Неформально, для укладки СФЭ S на носитель T разводка проводов в модели M_k^T соответствует некоторому способу провести провода схемы без ветвлений при фиксированном размещении функциональных элементов в вершинах носителя. Таким образом, для обоснования корректности разводки в общем случае ключевым моментом будет доказательство соответствия разводки локальному ограничению $wt_e(k)$. Как будет показано при доказательстве следующей леммы, с помощью введенного определения будет удобно строить разводки проводов более общих, чем СФЭ, конструкций.

Лемма 1. Пусть k — целое положительное число, T — граф d -мерного куба со стороной l , G — граф с вершинами куба T , степени вершин которого ограничены константой $a \geq 5$. Пусть выполнено соотношение

$$l \leq \frac{k}{a \cdot 1.6^{d-2}}. \quad (1)$$

Тогда существует разводка проводов графа G в модели M_k^T .

Доказательство. Будем строить требуемую разводку индукцией по размерности куба.

База индукции. Пусть $d = 2$. Построим разводку в квадрате так, как показано на рис. 1. Черными кружками в каждой ячейке символически показаны концы ребер графа G .

Ориентируем ребра графа G произвольным образом. Объединим провода, соответствующие началам ребер, по строкам квадрата в горизонтальные шины. Аналогично объединим провода, соответствующие концам ребер, по столбцам квадрата в вертикальные шины. Соединим соответствующие провода из горизонтальных и вертикальных шин (на рисунке это показано соединяющими шины проводами в левой верхней части ячеек), получим искомую разводку.

Ясно, что в такой конструкции в каждое ребро куба будет уложено не более $a \cdot l$ проводов. Согласно (1), $l \leq \frac{k}{a \cdot 1.6^{d-2}}$, что при $d = 2$ дает $a \cdot l \leq k$. Таким образом, локальное ограничение $wt_e(k)$ будет соблюдено.

Шаг индукции. Пусть $d > 2$. Основная идея построения разводки для куба размерности d — сведение исходной задачи к нескольким подзадачам для куба размерности $d - 1$. Для этого сгруппируем в шины провода, которые должны быть проведены в ячейках куба, лежащих в одном «столбике» (т. е. ячейках куба, у которых значения всех координат, кроме одной выделенной, совпадают — см. рис. 2). Тогда, если мы сможем развести провода между построенными шинами в l кубах размерности

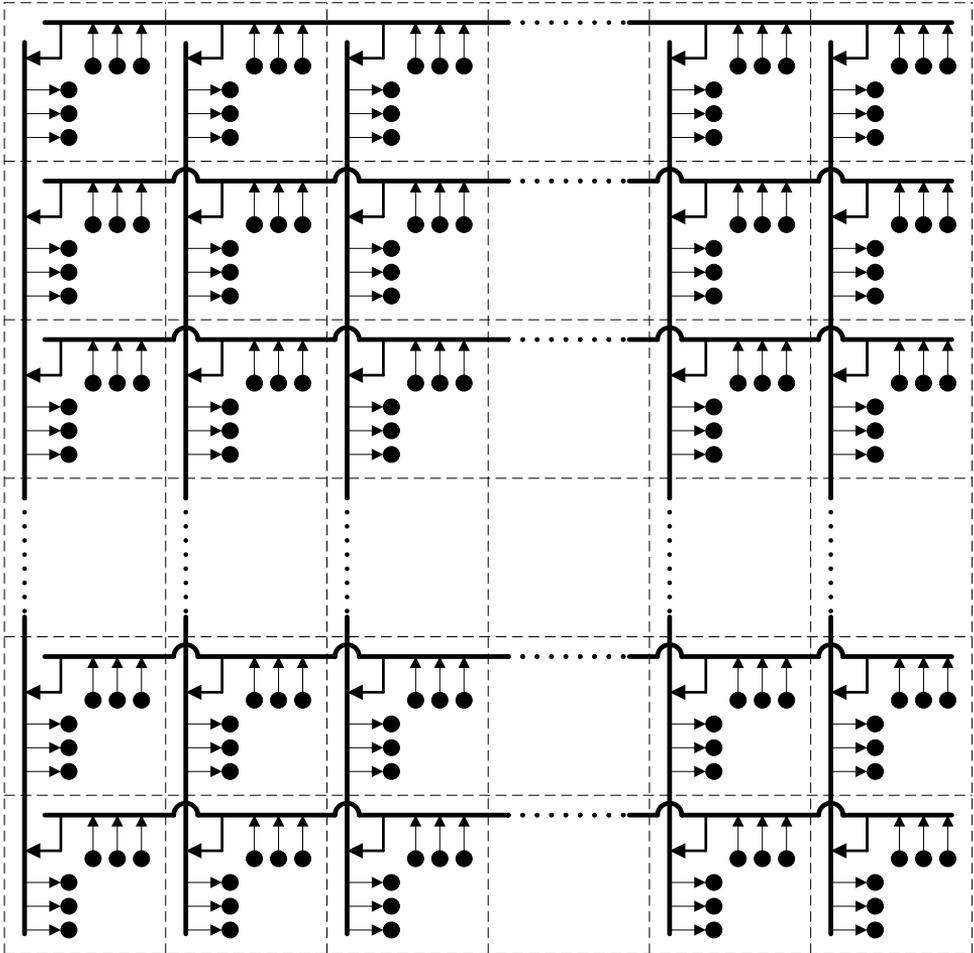


Рис. 1. Разводка проводов в двумерном случае.

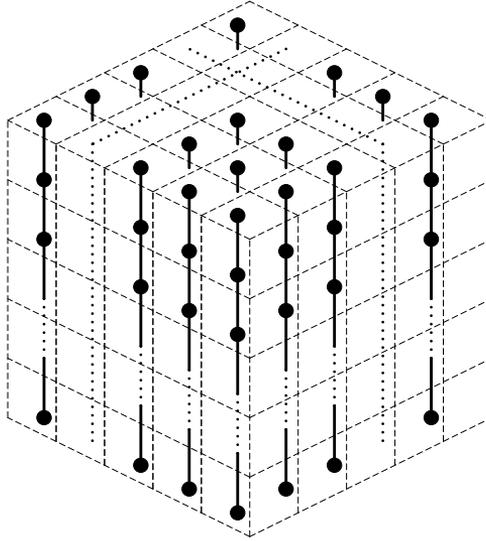


Рис. 2. Группирование проводов в шины вдоль одной из размерностей d -мерного куба.

$d - 1$, соответствующих «слоям» исходного куба вдоль выделенной координатной оси (рис. 3), то получим разводку проводов для d -мерного куба.

Рассмотрим граф $d - 1$ -мерного куба G' , получающийся из графа куба G путем слияния вершин, у которых совпадают все координаты, кроме одной выделенной (например, первой), и отбрасывания возникших при слиянии петель. Ясно, что в G' степень каждой вершины не будет превосходить $a \cdot l$.

Физически такое слияние будет соответствовать описанному выше объединению в одну шину всех проводов, соответствующих l ячейкам куба, которые были объединены при слиянии. Очевидно, что петли, возникшие при слиянии вершин, соответствуют случаю, когда провод соединил нужные две вершины через шину. Ясно, что эти провода можно не рассматривать дальше, поэтому при переходе от G к G' петли были отброшены. В силу (1) получим $a \cdot l \leq k$. Поскольку в каждой шине будет не более $a \cdot l \leq k$ проводов, локальное ограничение $wt_e(k)$ не будет нарушено.

Покажем, как перейти к подзадачам меньшей размерности. Согласно теореме Шеннона о реберной раскраске [17], любой мультиграф, степени

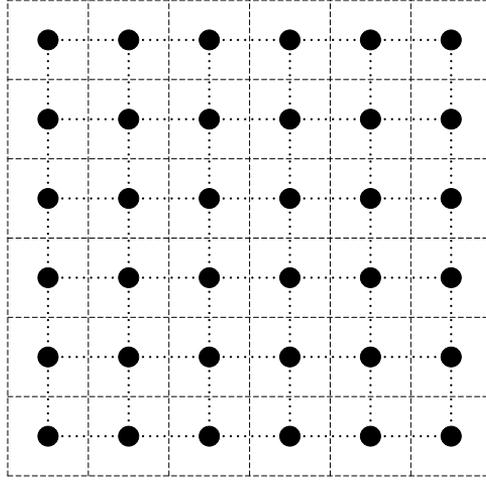


Рис. 3. Разводка проводов в кубе меньшей размерности.

вершин которого не превосходят некоторого числа q , имеет правильную реберную раскраску не более чем в $\frac{3}{2}q$ цветов. В частности, поскольку у мультиграфа G' степень вершин ограничена числом $a \cdot l$, то существует правильная реберная раскраска G' не более чем в $\frac{3}{2}a \cdot l$ цветов. Будем укладывать в каждый из l кубов размерности $d - 1$ ребра в соответствии с раскраской — не более чем по $\lceil \frac{3}{2}a \rceil$ цветов на каждый из l кубов.

Итак, получены подзадачи, где куб имеет размерность $d - 1$ и степень каждой вершины ограничена числом $a' = \lceil \frac{3}{2}a \rceil$. По условию леммы, $a \geq 5$, откуда $a' \leq 1.6a$. Согласно (1), $l \leq \frac{k}{a \cdot 1.6^{d-2}}$, откуда $l \leq \frac{k}{a' \cdot 1.6^{d-3}}$. Следовательно, по предположению индукции существует разводка проводов в кубе размерности $d - 1$ и стороной l , степени вершин которого ограничены числом a' . Конструируя такую разводку в каждой из подзадач, получаем разводку проводов для d -мерного куба. \square

Следующая важная лемма впервые была доказана Лупановым [12]. Мы будем использовать ее формулировку из [15]. В качестве базиса СФЭ используются все булевы функции от не более чем двух переменных. Следуя обозначениям из [15], для произвольной булевой функции f примем за $L(f)$ число элементов в минимальной по числу функциональных элементов СФЭ, вычисляющей f .

Лемма 2 ([15], теорема 11.2). Пусть $n \rightarrow \infty$. Тогда для каждой булевой функции, зависящей от n переменных,

$$L(f) \leq \frac{2^n}{n} \left(1 + O\left(\frac{\log_2 n}{n}\right) \right).$$

Метод синтеза СФЭ, использованный в доказательстве леммы 2, известен как метод Лупанова.

Лемма 3. Пусть $d \geq 2$, $m \rightarrow \infty$, $m \leq d \lfloor \log_{5 \cdot 1.6^{d-2}} k \rfloor$. Тогда для каждой булевой функции f , зависящей от m переменных, существует схема $K(f)$, реализующая f , такая, что ее образ целиком лежит в d -мерном кубе со стороной $l = \sqrt[d]{\frac{2^m}{m}(1 + o(1))}$.

Доказательство. Имеем $m \rightarrow \infty$. По лемме 2 для произвольной функции f от m переменных существует СФЭ S , реализующая f и содержащая не более $N = \frac{2^m}{m}(1 + o(1))$ функциональных элементов. Обозначим

$$l = \left\lceil \sqrt[d]{N} \right\rceil,$$

получим

$$l = \left\lceil \sqrt[d]{N} \right\rceil = \sqrt[d]{\frac{2^m}{m}(1 + o(1))} \leq \sqrt[d]{\frac{2^{d \lfloor \log_{5 \cdot 1.6^{d-2}} k \rfloor}}{m}(1 + o(1))},$$

откуда

$$l \leq \frac{k}{5 \cdot 1.6^{d-2}} \sqrt[d]{\frac{1 + o(1)}{m}} \leq \frac{k}{5 \cdot 1.6^{d-2}} \cdot \frac{1}{2} = \frac{k'}{5 \cdot 1.6^{d-2}}, \quad (2)$$

где $k' = \lceil \frac{1}{2}k \rceil$. Покажем, что при таком l можно уложить СФЭ S в d -мерный куб со стороной l .

Разместим функциональные элементы S в ячейки куба произвольным образом. Ясно, что, если мы сумеем провести провода ко входам всех элементов от входов схемы и соответствующих выходов элементов, укладывая не более k проводов в ребра графа d -мерного куба, то будет получена корректная схема в модели M_k^d . Покажем, как это сделать.

Для упрощения задачи подведем провода от всех входов схемы ко всем ячейкам куба, подключив их к входам соответствующих функциональных элементов. Сами входы схемы будем вести от произвольных граничных ячеек куба (для удобного подключения проводов извне схемы). Также проведем провод выхода схемы от выходного элемента к

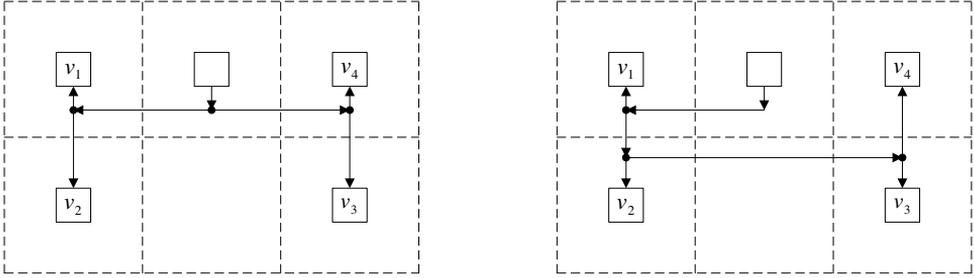


Рис. 4. Преобразование ветвлений провода. Слева — изначальное (произвольное) ветвление, справа — полученное последовательное ветвление провода в целевых ячейках.

произвольной граничной ячейке куба (также для удобного подключения вовне схемы). Легко видеть, что в результате в каждое ребро графа куба будет уложено не более $m + 1$ проводов. По условию леммы, $m \rightarrow \infty$ и $m \leq d \lfloor \log \frac{k}{5 \cdot 1.6^{d-2}} \rfloor$, откуда $m + 1 \leq \lfloor \frac{k}{2} \rfloor = k - k'$. Поэтому для получения корректной укладки S в куб достаточно провести остальные провода (между функциональными элементами S) с соблюдением ограничения $wt_e(k')$.

Для применения леммы 1 о разводке проводов необходимо видоизменить задачу о проведении проводов между функциональными элементами S так, чтобы не было ветвлений проводов и чтобы степени вершин были ограничены. Покажем, как это сделать.

Ясно, что ветвиться будут провода, которые должны быть поданы на вход по крайней мере двум функциональным элементам. Пусть некоторый провод должен быть подключен на входы элементов v_1, v_2, \dots, v_r . Тогда последовательно проведем провод к ячейкам, содержащим элементы v_1, v_2, \dots, v_r , производя ветвления во всех ячейках, кроме последней (пример для $r = 4$ на рис. 4). Поскольку все функциональные элементы реализуют функции не более чем от двух переменных, то в такой конструкции в каждой ячейке куба будет не более двух ветвлений проводов.

Таким образом, исходная задача сводится к следующей: развести провода, соблюдая ограничение $wt_e(k')$, при условии, что в каждой ячейке исходно было не более двух входящих проводов и не более трех исходящих (один провод для выхода функционального элемента и не более двух проводов для ветвлений входов того же элемента). При этом ветвления в середине провода не допускаются, т. е. каждый провод соединяет две заданные ячейки. Фактически требуется построить разводку прово-

дов для графа с вершинами из d -мерного куба со стороной l , степень вершин которого ограничена числом $2 + 3 = 5$.

Поскольку, согласно (2), $l \leq \frac{k'}{5 \cdot 1.6^{d-2}}$, по лемме 1 для $a = 5$ такая разводка проводов будет существовать. Используя ее для соединения проводов функциональных элементов S , получим корректную схему в модели M_k^d , образ которой есть d -мерный куб со стороной l . \square

Лемма 4. Пусть $k \geq 2$. Тогда для любого целого положительного n существует схема K_n , реализующая все конъюнкции от n переменных, образ которой есть прямоугольник длины $2^n + 1$ и высоты n .

Доказательство. Для изображения функциональных элементов схем будем использовать следующие стандартные обозначения (рис. 5).



Рис. 5. Графические обозначения функциональных элементов.

Схема, реализующая все конъюнкции от n переменных, изображена на рис. 6.

Нетрудно видеть, что ограничение $wt_f(1)$ соблюдено, поскольку в каждую клетку схемы уложено не более одного функционального элемента. Ограничение на базис также не нарушается, поскольку все функциональные элементы реализуют либо конъюнкцию, либо отрицание. Наконец, поскольку максимальное количество проводов, пересекающих границу между смежными клетками, равно 2, ограничение $wt_e(k)$ будет выполнено для любого $k \geq 2$.

Высота схемы, очевидно, равна числу входов, т.е. равна n , а длина — количеству выходов плюс 1, что составит $2^n + 1$. \square

Лемма 5. Пусть $k \rightarrow \infty$ и $n \geq d \lceil \log \frac{k}{5 \cdot 1.6^{d-2}} \rceil$. Тогда

$$L(M_k^d, n) \lesssim \frac{2^n}{d \log k}.$$

Доказательство. Достаточно показать, что при указанных в теореме условиях для произвольной функции f от n переменных существует реализующая схема в модели M_k^d со сложностью, асимптотически не превышающей $\frac{2^n}{d \log k}$.

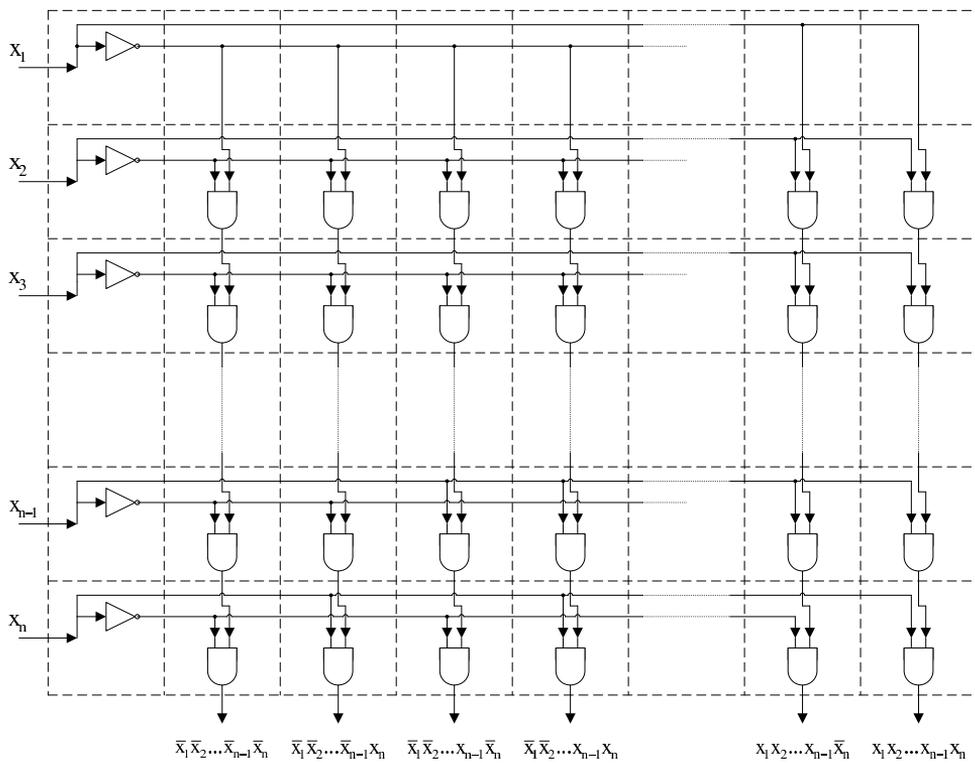


Рис. 6. Схема, реализующая все конъюнкции от n переменных.

Пусть f — произвольная булева функция, зависящая от n переменных. Выделим $m = d \lceil \log_{5.16^{d-2}} k \rceil$ переменных x_1, x_2, \dots, x_m . Оставшиеся $n - m$ переменных разобьем на две примерно одинаковые группы (при малых $n - m$, возможно, пустые) с $a = \lfloor \frac{n-m}{2} \rfloor$ и $b = \lceil \frac{n-m}{2} \rceil$ переменными соответственно. Разложим функцию по этим $n - m$ переменным:

$$f = \bigcup x_{n-m+1}^{\sigma_{n-m+1}} \dots x_n^{\sigma_n} f_i(x_1, \dots, x_m) \quad (3)$$

Согласно лемме 4, существуют схемы K_A и K_B , реализующие все конъюнкции от a и b переменных соответственно. Рассмотрим, например, схему K_B — ее высота должны составить b , а длина — $2^b + 1$. Легко видеть, что данную схему можно преобразовать, вставив в нее пустые столбцы в произвольные места, получив таким образом схему большей длины с нужными интервалами между выходами.

Согласно лемме 3, произвольная функция от m переменных реализуется схемой, образ которой помещается в d -мерный куб со стороной $l \sim \sqrt[d]{\frac{2^m}{m}}$.

Построенная схема будет размещена в d -мерном параллелепипеде с двумя основными размерностями. Конструктивно она будет состоять из 2^{n-m} d -мерных кубических блоков размера l , реализующих функции f_i из разложения (3), и соединяющих их функциональных блоков, расположенных в двумерной плоскости, соответствующей основным размерностям параллелепипеда. Будем называть эту плоскость *соединяющей*. На рис. 7 показано прямоугольное сечение схемы соединяющей плоскостью.

Покажем, как расположить элементы схемы в указанном прямоугольном сечении. Разместим преобразованные схемы K_A и K_B у левого и верхнего краев прямоугольника. Составим 2^{n-m} схем, реализующих функции f_i из разложения (3), и разместим их в d -мерные кубы так, что их двумерные сечения соединяющей плоскостью будут расположены напротив соответствующих выходов K_A и K_B . Для каждого выхода K_A добавим вспомогательную строку, в которой будем вести два провода — один от выхода K_A , второй для аккумуляции дизъюнктов по строке. Для каждого выхода K_B добавим вспомогательный столбец, в котором будем вести шину с проводами для x_1, \dots, x_m (эту шину будем передавать на входы подсхем, реализующим f_i), а также провод, соответствующий выходу K_B . Добавим дополнительную строку сверху для подведения шины от входов схемы к столбцам. Также добавим один столбец слева для проведения шины к самым левым подсхемам. Наконец, добавим один вспомогательный столбец справа для аккумуляции дизъ-

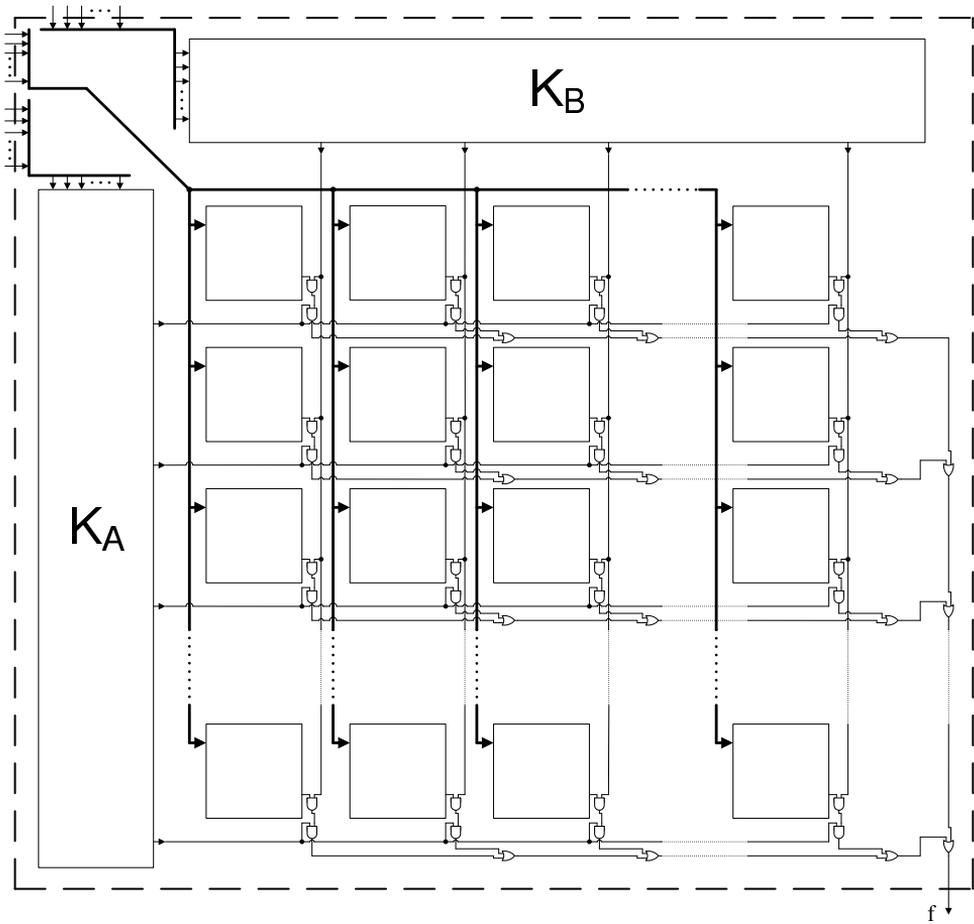


Рис. 7. Схема, реализующая функцию f .

юнктов — на выходе в нижней строке в данном столбце будет получено значение функции f .

Покажем, что при таком построении соблюдены все ограничения модели M_k^d . Внутри подсхем K_A и K_B , а также подсхем, реализующих функции f_i , эти ограничения выполняются в силу лемм 3 и 4. Далее, в верхнем левом углу схемы изображены три шины, собирающие входы схемы в группы — легко видеть, что их можно уложить, не нарушив ограничения $wt_e(k)$ (другие ограничения не будут нарушены в силу отсутствия в той части схемы функциональных элементов). Наконец, в дополнительных строках и столбцах ограничения также соблюдены — для аккумуляции дизъюнктов от каждой подсхемы потребуется три функциональных элемента (две конъюнкции и одна дизъюнкция), которые легко уместить в трех соседних клетках схемы; количество проводов, соединяющих клетки дополнительных столбцов и строк с любой соседней клеткой, не превосходит величины $m + 2 \leq k$ (число проводов шины с m проводами плюс не более двух дополнительных проводов).

Оценим сложность полученной схемы. Для этого вычислим объем соответствующего параллелепипеда. По построению, прямоугольное сечение соединительной плоскости имеет длину

$$a + 1 + 2^b(l + 1) + 1$$

и высоту

$$b + 1 + 2^a(l + 1).$$

Длины параллелепипеда вдоль остальных $d - 2$ размерностей равны длине кубов, реализующих функции f_i , т. е. равны l . Перемножая, получим

$$L(M_k^d, f) \leq (a+1+2^b(l+1)+1) \cdot (b+1+2^a(l+1)) \cdot l^{d-2} \lesssim (a+2^b l) \cdot (b+2^a l) \cdot l^{d-2}.$$

Так как a и b различаются не более чем на 1, то

$$L(M_k^d, f) \lesssim 2^{a+b} \cdot l^d.$$

Подставляя значения a, b, l и учитывая, что $a + b = n - m$, получим

$$L(M_k^d, f) \lesssim 2^{n-m} \cdot \frac{2^m}{m} = \frac{2^n}{m}.$$

Наконец, подставляя значение m , получим

$$L(M_k^d, f) \lesssim \frac{2^n}{d \log k},$$

что и требовалось доказать. \square

Теорема 1.

$$L(M_k^d, n) \lesssim \frac{2^n}{\min(n, d \log k)} \quad \text{при } k \rightarrow \infty, n \rightarrow \infty.$$

Доказательство. Рассмотрим два случая.

1) $n \geq d \lfloor \log \frac{k}{5 \cdot 1.6^{d-2}} \rfloor$. В этом случае, используя лемму 5, получим

$$L(M_k^d, n) \lesssim \frac{2^n}{d \log k} \sim \frac{2^n}{\min(n, d \log k)}.$$

2) $n < d \lfloor \log \frac{k}{5 \cdot 1.6^{d-2}} \rfloor$. В этом случае для $m = n$ выполнены условия леммы 3. По той же лемме 3 получим

$$L(M_k^d, n) \leq \left(\sqrt[d]{\frac{2^n}{n} (1 + o(1))} \right)^d = \frac{2^n}{n} (1 + o(1)) \sim \frac{2^n}{\min(n, d \log k)}.$$

Объединяя результаты рассмотренных случаев, получаем утверждение теоремы. \square

Список литературы

- [1] Альбрехт А., “О схемах из клеточных элементов”, *Проблемы кибернетики*, **33** (1977), 209–214.
- [2] Ефимов А. А., “Верхняя оценка энергопотребления в классе объемных схем”, *Интеллектуальные системы*, **23**:1 (2019), 117–132.
- [3] Грибок С. В., “Об одном базисе для схем из клеточных элементов”, *Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика*, **4** (1999), 36–39.
- [4] Жуков Д. А., “О вычислении частичных булевых функций клеточными схемами”, *Дискретный анализ и исследование операций*, **1**:11 2 (2004), 32–40.
- [5] Калачев Г. В., “Порядок мощности плоских схем, реализующих булевы функции”, *Дискретная математика*, **26**:1 (2014), 49–74.
- [6] Калачев Г. В., “Об одновременной минимизации площади, мощности и глубины плоских схем, реализующих частичные булевы операторы”, *Интеллектуальные системы*, **20**:2 (2016), 203–266.
- [7] Калачев Г. В., “Оценки мощности плоских схем, реализующих функции с ограниченным числом единиц”, *Интеллектуальные системы*, **21**:1 (2017), 28–96.

- [8] Калачев Г. В., “Оценки мощности плоских схем, реализующих монотонные функции”, *Интеллектуальные системы*, **21**:2 (2017), 163–192.
- [9] Калачев Г. В., “О нижней оценке максимального потенциала плоских схем с несколькими выходами через площадь”, *Интеллектуальные системы*, **22**:1 (2018), 111–117.
- [10] Кравцов С. С., “О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов”, *Проблемы кибернетики*, **19** (1967), 285–293.
- [11] Коршунов А. Д., “Об оценках сложности схем из объемных функциональных элементов и объемных схем из функциональных элементов”, *Проблемы кибернетики*, **19** (1967), 275–283.
- [12] Лупанов О. Б., “О синтезе некоторых классов управляющих систем”, *Проблемы кибернетики*, **10** (1963), 63–97.
- [13] Лупанов О. Б., “Об одном подходе к синтезу управляющих систем — принципе локального кодирования”, *Проблемы кибернетики*, **14** (1965), 31–110.
- [14] Сытдыков Т. Р., “Сложность синтеза многослойных клеточных схем”, *Дискретная математика*, **В печати**.
- [15] Чашкин А. В., *Дискретная математика*, Академия, Москва, 2012, 352 с.
- [16] Muller D. E., “Complexity in Electronic Switching Circuits”, *IRE Transactions on Electronic Computers*, **EC-5 1** (1956), 15–19
- [17] Shannon, Claude E., “A theorem on coloring the lines of a network”, *Math. Physics*, **28** (1949), 148–151

The complexity of multidimensional rectangular circuits design Sitdikov T. R.

A model of rectangular multidimensional circuits is considered in this paper. Logic gates are placed in cells of d -dimensional mesh. Each pair of adjacent cells is connected by a bus with at most k wires. We establish Shannon function upper bound $\frac{2^n}{\min(n, d \log k)}$ for the complexity of this type of circuits.

Keywords: multidimensional circuits, multilayer circuits, Shannon function asymptotics, circuit complexity.

О числе максимальных надклассов в классе линейных автоматов

Часовских А.А.

Уточнены перечни предполных классов в классах линейных автоматов над конечными полями. Найден критерий конечности числа предполных надклассов для заданного множества линейных автоматов.

Ключевые слова: конечный автомат, линейный автомат, операции композиции, обратная связь, полнота, замкнутый класс, предполный класс, конечное поле.

%beginndocument

Настоящая работа уточняет результат, полученный в [6]. Мы, в основном, используем определения и обозначения из этой работы.

Через E_k мы обозначаем поле, состоящее из k элементов. Как известно [3], при этом для некоторого простого числа p и натурального числа m выполнено: $k = p^m$. Множество многочленов от переменной ξ над полем E_k обозначаем $E_k[\xi]$, а поле частных для $E_k[\xi]$ — через $E_k(\xi)$. Поле $E_k(\xi)$ содержит подкольцо $E'_k(\xi)$, состоящее из дробей, знаменатели которых имеют ненулевой свободный член, изоморфное кольцу периодических (с предпериодом) рядов переменной ξ над полем E_k . Эти два кольца в дальнейшем мы не различаем. Множество всех формальных степенных рядов от переменной ξ над полем E_k обозначаем R_k .

Множество всех конечных автоматов, построенных из сумматора, задержек и усилителей [1] с использованием операций композиции [2], обозначим \mathfrak{L}_k . Рассуждениями из работы [4] можно показать, что линейный автомат с входными переменными x_1, x_1, \dots, x_n — это отображение $f(x_1, x_2, \dots, x_n)$, из R_k^n в R_k ,

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^n \mu_i x_i + \mu_0, \quad (1)$$

где $\mu_i, \mu_i \in E'_k(\xi)$, $i \in \{0, 1, \dots, n\}$.

Если выполнено равенство (1), то через $U(f)$ будем обозначать множество $\{ \mu_i \mid i \in \{1, 2, \dots, n\} \}$.

Введем следующие подмножества \mathfrak{L}_k .

$$T_a = \{ f \mid f(a, a, \dots, a) - a \in \xi R_k \},$$

$$a \in E_k,$$

$$V_1 = \{ f \mid \text{из (1) следует } |\{ i \mid \mu_i(0) \neq 0 \}| \leq 1 \},$$

$$V_p = \left\{ f \mid \text{из (1) следует } \sum_{i=1}^n \mu_i(0) = 1 \right\},$$

$$M_1 = \{ f \mid \text{из (1) следует } \mu_i - \mu_i(0) \in \xi^2 E'_k(\xi), i \in \{1, 2, \dots, n\} \}.$$

Пусть $E_{k_1}, E_{k_2}, \dots, E_{k_l}$ — все максимальные собственные подполя в E_k . Положим:

$$P_s = \{ f \mid \text{из (1) следует } \mu_i(0) \in E_{k_s}, i \in \{1, 2, \dots, n\} \},$$

$$s \in \{1, 2, \dots, l\}.$$

Через Ω обозначим множество автоморфизмов поля E_k . Если степень числителя дроби μ , $\mu \in E'_k(\xi)$, не превосходит степени его знаменателя, то дробь $\tilde{\mu}$, $\tilde{\mu} = \mu(1/\xi)$, содержится в $E'_k(\xi)$. В этом случае значение $\tilde{\mu}(0)$ обозначим $\Psi_0(\mu)$.

Занумеруем все неприводимые приведенные многочлены из $E_k[\xi]$,

$$p_1, p_2, \dots,$$

так, что $p_1 = \xi$.

Если знаменатель дроби μ , $\mu \in E'_k(\xi)$, не делится на p_i , то для некоторых u и μ' , $u \in E_k[\xi]$, $\mu' \in E'_k(\xi)$ имеем:

$$\mu = u + p_i \mu', \quad \deg u < \deg p_i.$$

Многочлен u в этом случае обозначаем $\Psi_i(\mu)$

Тогда положим:

$$M_{i,\omega} = \{ f \mid \text{из (1) следует } \omega(\mu_j(0)) = \Psi_i(\mu), j \in \{1, 2, \dots, n\} \},$$

$$\omega \in \Omega, \quad i \in \{0, 2, 3, \dots\}.$$

Мы используем множества \tilde{M}_i ,

$$\tilde{M}_i = \{ f \mid \text{из (1) следует, } \exists \Psi_i(\mu_j), j \in \{1, 2, \dots, n\} \},$$

$i \in \{0, 2, 3, \dots\}$.

Через $R_i^{(e)}$ обозначим множество автоматов f из \tilde{M}_i таких, что, если f существенно зависит более чем от одной переменной, то его коэффициенты μ_j в разложении (1) удовлетворяют равенству

$$\Psi_i(\mu_j) = 0, \quad j \in \{1, 2, \dots, n\}, \quad i \in \{0, 2, 3, \dots\}.$$

Через $R_i^{(d)}$ обозначим множество автоматов f из \tilde{M}_i , для которых в разложении (1) не более одного j такого, что $\Psi_i(\mu_j) \neq 0$ и, если такой j найдется, то $\mu_j(0) \neq 0$ и для любого $j', j' \in \{1, 2, \dots, n\} \setminus \{j\}$, выполнено $\mu_{j'}(0) = 0$.

Положим:

$$J_k = \left\{ T_a, V_1, V_p, P_s, M_1, M_{i,\omega}, R_i^{(\rho)} \mid a \in E_k, s \in \{1, 2, \dots, l\}, i \in \{0, 2, 3, \dots\}, \omega \in \Omega, \rho \in \{e, d\} \right\}.$$

Замыкание множества M по операциям композиции обозначаем $K(M)$. Множество M линейных автоматов называется замкнутым классом, если $K(M) = M$. Если $K(M) = \mathfrak{L}_k$, то M полно в \mathfrak{L}_k . Замкнутый класс является максимальным (предполным), если он не совпадает с \mathfrak{L}_k , но, добавляя к нему любой автомат из $\mathfrak{L}_k \setminus M$, получаем полное множество. В работе [5] найдены все максимальные подклассы для случая простого k . В настоящей работе максимальные подклассы построены в общем случае, что уточняет результат работы [6].

Теорема 1. *Множество J_k состоит из максимальных подклассов \mathfrak{L}_k и содержит все его максимальные подклассы.*

Для заданного множества M линейных автоматов из \mathfrak{L}_k элемент Θ множества J_k называется максимальным надклассом для M , если $M \subseteq \Theta$. Анализируя множество J_k , получаем следующие утверждения.

Теорема 2. *Множество M , $M \subseteq \mathfrak{L}_k$, имеет конечное число максимальных надклассов в точности тогда, когда M содержит линейный автомат с не менее чем двумя существенными переменными, и в M найдется f такой, что*

$$U(f) \setminus E_k \neq \emptyset.$$

Теорема 3. *Существует алгоритм, с использованием которого время проверки конечности числа максимальных надклассов для данного множества M , состоящего из r линейных автоматов, каждый из которых зависит не более чем от n переменных, по порядку не превосходит rn .*

Список литературы

- [1] Гилл А., *Линейные последовательностные машины*, пер. с англ., «Наука», Москва, 1974, 288 с.
- [2] Кудрявцев В.Б., Алешин С.В., Подколзин А.С., *Введение в теорию автоматов*, «Наука», Москва, 1985, 320 с.
- [3] Лидл Р., Нидеррайтер Г., *Конечные поля*, пер. с англ., «Мир», Москва, 1988, 430 с.
- [4] Часовских А.А., “О полноте в классе линейных автоматов”, *Математические вопросы кибернетики*, 1991, № 3, 140–166
- [5] Часовских А.А., “Условия полноты линейно-р-автоматных функций”, *Интеллектуальные системы*, **18:3** (2014), 203–252
- [6] Часовских А.А., “Приведенные критериальные системы предполных классов в классах линейных автоматов над конечными полями”, *Интеллектуальные системы*, **22:4** (2018), 115–134

On the number of maximum overclasses in the linear automata class

Chasovskikh A.A.

Updated maximale subclasses lists in linear automata classes over finite fields. A criterion is found for the finiteness of the number of precomplete overclasses for a given set of linear automata.

Keywords: finite automaton, linear automaton, operation of composition, feedback, completeness, closed class, maximum subclass, finite field.

Часть 3.
Математические модели

Автоматы с линейными переходами

Бабин Д.Н.

Рассматривается проблема полноты системы автоматных функций с линейными переходами относительно операции суперпозиции. Эта система не является полной, более того, любая дополняющая ее до базиса система автоматов бесконечна.

Ключевые слова: конечный автомат, полнота, суперпозиция, замкнутый класс.

Теория линейных автоматов с операцией суперпозиции естественным образом использует аппарат линейной алгебры, смотри, например "Линейные последовательные машины" [1] — перевод на русский язык статьи Гилла [2]. Там показано, что линейные автоматы — это замкнутый класс, все полные системы в нем бесконечны, а система состоящая из одноместных функций и сумматора по модулю 2 — полна.

Относительно двух операций: суперпозиции и обратной связи линейные автоматы — это также замкнутый класс, в нем есть конечные полные системы, а также алгоритм проверки конечных систем на полноту, смотри работу Часовских А.А. [3].

Ранее автор показал [4], что линейный автомат может быть разложен в суперпозицию линейных автоматов с двумя состояниями и автомата с безусловными переходами (не обязательно линейного). В настоящей статье приводится явная формула такого разложения, а также доказан факт о бесконечной высоте и глубине класса линейных автоматов в классе всех автоматов.

Системы автоматов, имеющих линейные функции переходов, замкнутого класса не образуют. Эта система автоматов не полна, более того, до полной системы необходимо добавить к ним бесконечно много автоматов. Простое доказательство этих фактов приводится в этой статье.

Полное описание функциональных систем автоматов приведено в [5].

Пусть $E_2 = \{0, 1\}$, $g: E_2^n \rightarrow E_2^m$ булева вектор-функция, их множество обозначается через \mathbf{P}_2 . Пусть

$$E_2^\infty = \{a(1)a(2)\dots | a(j) \in E_2, j = 1, 2, \dots\}$$

— множество всех сверхслов.

$$f: (E_2^\infty)^n \rightarrow (E_2^\infty)^m$$

— автоматная функция (a -функция), т.е. она задается рекуррентно соотношениями

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi(q(t), a_1(t), \dots, a_n(t)), \\ b_j(t) = \psi_j(q(t), a_1(t), \dots, a_n(t)), \quad j = 1, \dots, m. \end{cases}$$

где $q \in Q = \{q_1, \dots, q_r\}$. Параметр q называется состоянием a -функции f , q_1 — ее начальным состоянием, вектор-буквы $\mathbf{a} = (a_1, \dots, a_n)$ и $\mathbf{b} = (b_1, \dots, b_m)$ называются входной и выходной буквами, φ и ψ функцией переходов и выходов, соответственно, а сверхслова $\mathbf{a}(1)\mathbf{a}(2)\dots$ и $\mathbf{b}(1)\mathbf{b}(2)\dots$ — входным и выходным сверхсловами, соответственно. Класс всех a -функций обозначим через \mathbf{P} . Если функции φ и ψ_j линейны, автоматная функция называется линейной. Класс всех линейных a -функций обозначим через \mathbf{L} . Если функция φ линейна, то автоматная функция называется функцией с линейными переходами. Множество a -функций с линейными переходами обозначим через \mathbf{L} . Если функция φ при фиксированных $a_1(t), \dots, a_n(t)$, является взаимно-однозначным отображением Q в Q , то автоматная функция называется групповой. Класс всех групповых a -функций обозначим через \mathbf{G} . Автоматная функция, выдающая одно и то же выходное слово на всех входных словах, называется константной. Класс всех константных a -функций обозначим через \mathbf{K} .

Пусть $\nu \subseteq \mathbf{P}$, обозначим через $[\nu]$ множество всех a -функций, получающихся из ν с помощью операций суперпозиции. Множество ν называется полным, если $[\nu] = \mathbf{P}$. Проблема полноты для P состоит в описании всех полных множеств ν .

Функция

$$\mathbf{f}_{\mathbf{Sh}}(x, y) = \min(x, y) \oplus 1$$

называется функцией Шеффера. Известно, что $\mathbf{P}_2 = [\{\mathbf{f}_{\mathbf{Sh}}\}]$, т.е. функция $\mathbf{f}_{\mathbf{Sh}}$ образует полную систему в классе булевых функций. Здесь \oplus — сложение по модулю 2.

Линейная автоматная функция $d_0: E_2^\infty \rightarrow E_2^\infty$, задаваемая уравнениями

$$\begin{cases} q(1) = 0, \\ q(t+1) = x(t), \\ b(t) = q(t), \end{cases}$$

называется a -функцией задержки с нулевым начальным состоянием. Если в этих уравнениях $q(1) = 1$, то это задержка $d_1: E_2^\infty \rightarrow E_2^\infty$ с единичным начальным состоянием.

Линейная автоматная функция $w_0: E_2^\infty \rightarrow E_2^\infty$, задаваемая уравнениями

$$\begin{cases} q(1) = 0, \\ q(t+1) = q(t) + x(t), \\ b(t) = q(t), \end{cases}$$

называется a -функцией переключатель с нулевым начальным состоянием. Если в этих уравнениях $q(1) = 1$, то это переключатель $w_1: E_2^\infty \rightarrow E_2^\infty$ с единичным начальным состоянием.

Перепишем уравнения автоматной функции f в виде

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi(q(t), \mathbf{a}(t)), \\ \mathbf{b}(t) = \psi(q(t), \mathbf{a}(t)) \end{cases}$$

Запишем уравнения автоматной функции с линейными переходами в виде

$$\begin{cases} q(1) = q_0, \\ q(t+1) = A(q(t)) + B(x(t)) + c, \\ \mathbf{b}(t) = \psi(q(t), \mathbf{a}(t)), \end{cases}$$

где A, B линейные операторы, а c вектор подходящей размерности. Матрица A называется основной матрицей автомата. Известно [1], что линейной заменой переменных матрица A приводится к клеточно-диагональному виду (Жордановой нормальной форме).

$$\begin{pmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_k \end{pmatrix}$$

Здесь Жорданова клетка J_i - это матрица вида

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 \\ a_0 & a_1 & a_2 & \dots & a_{n-1} \end{pmatrix}$$

ассоциированная с многочленом

$$\lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_1\lambda + a_0,$$

который является степенью некоторого неприводимого многочлена над полем Z_2 .

Получилась

Лемма 1.

Автомат с линейными переходами получается суперпозицией булевых функций и автоматов с линейными переходами, основные матрицы которых — Жордановы клетки.

Лемма 2.

Если $\det(J) = 0$, то автомат с основной матрицей жордановой клеткой J выразим суперпозициями автоматов $\mathbf{f}_{\mathbf{sh}}, d_0, d_1$.

Доказательство: В самом деле: разложением по последней строке определителя получаем, что $\det(J_i) = a_0$, но если многочлен

$$\lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_1\lambda + a_0,$$

это степень неприводимого многочлена и $a_0 = 0$, то многочлен делится на λ , а значит этот многочлен λ^n , и ассоциированная с ним матрица это J_0 .

$$J_0 = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Тогда канонические уравнения такого автомата имеют вид

$$\left\{ \begin{array}{l} q_1(1) = q_{1,0}, \\ q_2(1) = q_{2,0}, \\ \dots \\ q_n(1) = q_{n,0}, \\ q_1(t+1) = q_2(t) + B_1(\mathbf{a}(t)) + c_1, \\ q_2(t+1) = q_3(t) + B_2(\mathbf{a}(t)) + c_2, \\ \dots \\ q_{n-1}(t+1) = q_n(t) + B_{n-1}(\mathbf{a}(t)) + c_n, \\ q_n(t+1) = B_n(\mathbf{a}(t)) + c_n, \\ \mathbf{b}(t) = \psi(q_1(t), q_2(t), \dots, q_n(t), \mathbf{a}(t)), \end{array} \right.$$

$$\begin{aligned} q_n(t) &= d_{q_n,0}(B_n(\mathbf{a}(t)) + c_n), \\ q_{n-1}(t) &= d_{q_{n-1},0}(q_n(t) + B_{n-1}(\mathbf{a}(t)) + c_{n-1}) \\ &\dots \\ q_1(t) &= d_{q_1,0}(q_2(t) + B_1(\mathbf{a}(t)) + c_1) \\ \mathbf{b}(t) &= \psi(q_1(t), q_2(t), \dots, q_n(t), \mathbf{a}(t)). \end{aligned}$$

Таким образом, выходная буква при всех t вычисляется по выходам задержек и булевых функций при тех же t . •

Лемма 3.

Если $\det(A) \neq 0$, то автомат с линейными переходами и основной матрицей A выразим суперпозициями автоматов из $K, \mathbf{f}_{Sh}, w_0, w_1$.

Доказательство: Пусть линейный автомат имеет уравнения

$$\left\{ \begin{array}{l} q(1) = q_0, \\ q(t+1) = Aq(t) + Bx(t) + c, \\ \mathbf{b}(t) = q(t), \end{array} \right.$$

где $c = 0$. Пусть n порядок матрицы A , т.е. $A^n = E$, где E единичная матрица. Рассмотрим уравнения функции $\mathbf{b}(x)$,

$$\left\{ \begin{array}{l} p(1) = 1 \\ z(1) = 00 \dots 0 \\ p(t+1) = p(t) + 1 \pmod n \\ W = A^{-p-1}Bx \\ z(t+1) = z(t) + W \\ \mathbf{b}(t) = Wz, \end{array} \right. .$$

Это суперпозиция автоматной функции $W(x)$ с безусловными переходами, имеющей уравнения

$$\begin{cases} p(1) = 1 \\ p(t+1) = p(t) + 1 \mid \text{mod } n \\ W = A^{-p-1}Bx \end{cases}$$

и линейной автоматной функции $b(W)$ с уравнениями

$$\begin{cases} z(1) = 00 \dots 0 \\ z(t+1) = z(t) + W \\ \mathbf{b}(t) = Wz, \end{cases}$$

которая является суперпозицией (параллельным соединением) нескольких автоматных функций w_0 , здесь вектор z имеет ту же размерность, что и q . Автоматная функция $W(x)$ получается суперпозицией константной функции

$$\begin{cases} p(1) = 1 \\ p(t+1) = p(t) + 1 \mid \text{mod } n \\ y = p \end{cases}$$

и булевых функций.

Уравнения для $\mathbf{b}(x)$ в первом и втором случае, это одни и те же рекуррентные соотношения. В самом деле:

$$\begin{aligned} q(t+1) &= A^{p(t+1)}z(t+1) = A^{p(t)+1}(z(t) + A^{-p(t)-1}Bx(t)) = \\ &= A(A^{p(t)}z(t)) + Bx(t) = A(q(t)) + Bx(t) \end{aligned}$$

Автоматная функция с линейными переходами

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi(q(t), \mathbf{a}(t)), \\ \mathbf{b}(t) = \psi(q(t), \mathbf{a}(t)) \end{cases}$$

получается из линейной автоматной функции

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi(q(t), \mathbf{a}(t)), \\ \mathbf{b}(t) = q(t) \end{cases}$$

и булевых функций.

Случай $c \neq 0$ сводится к случаю $c = 0$ заменой переменных состояний.
В самом деле: уравнения

$$\begin{cases} q(1) = q_0, \\ q(t+1) = Aq(t) + Bx(t) + c, \end{cases}$$

равносильны уравнениям

$$\begin{cases} r(1) = c, \\ q(1) = q_0, \\ r(t+1) = r(t), \\ q(t+1) = Aq(t) + r(t) + Bx(t), \end{cases}$$

Лемма 3 доказана •

Для функции f

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi(q(t), \mathbf{a}(t)), \\ \mathbf{b}(t) = \psi(q(t), \mathbf{a}(t)) \end{cases}$$

рассмотрим другую автоматную функцию f^s с уравнениями

$$\begin{cases} \tilde{q}(1) = q_1, \\ \tilde{q}(t+1) = \varphi(\tilde{q}(t), \mathbf{a}((t-1)*s+1)\mathbf{a}((t-1)*s+2)\dots\mathbf{a}(t*s)) \\ \mathbf{b}((t-1)*s+1)\dots\mathbf{b}(t*s) = \psi(\tilde{q}(t), \mathbf{a}((t-1)*s+1)\dots \\ \dots\mathbf{a}(t*s)), \end{cases}$$

которая согласно тем же уравнениям за один такт перерабатывает s входных букв и выдает s выходных букв. Назовем новую автоматную функцию f^s в s раз ускоренной функцией f . Для множества автоматных функций $F = \{f_i\}$ обозначим через $F^s = \{f_i^s\}$. Операция перехода к ускоренной функцией f^s , была рассмотрена автором ранее под названием вербальной операции над автоматами [6]. Имеет место теорема о перестновочности операций ускорения и суперпозиции.

Теорема 1. [6] $[F]^s \subseteq [F^s]$

Имеет место

Утверждение 1.

Пусть для натурального T система всех автоматов μ такова, что число состояний каждого автомата не превосходит T . Тогда найдется автоматная функция f_T , такая что $\mu \subseteq [f_T, \mathbf{f}_{\text{sh}}]$.

Доказательство:

В самом деле: рассмотрим в качестве f_T автоматную функцию с T состояниями, у которой каждая подстановка из полной полугруппы P_T подстановок на T элементах задается одной входной буквой [5]. Пусть входной алфавит f_T это P_T , а множество состояний и выходной алфавит $\{1, 2, \dots, T\}$ в бинарном виде. На выход f_T будет выдавать номер своего состояния.

Для автоматной функции $f \in \mu$ с входным алфавитом A , выходным алфавитом B и T состояниями, определим булеву функцию $\omega : A \rightarrow P_T$, $\omega(a) = \varphi_a$ тогда функция $\psi(f_T(\omega(a)), a) = f \bullet$

Следствие 1.

Для любой автоматной функции f , множество $\{f^s | s \in \mathbf{N}\}$ порождается двумя автомными функциями.

В самом деле, каждая из функций f^s имеет не больше состояний, чем функция f , по утверждению 1 получаем доказательство следствия.

Следствие 2.

$$\mathbf{P}_2^s \subseteq \mathbf{P}_2 \text{ и } \{w_0, w_1\}^s \subseteq [\mathbf{P}_2 \cup \{w_0, w_1\}]$$

Теорема 2.

Пусть Ω конечное множество a -функций, тогда $[\Omega \cup \mathbf{L}] \subsetneq \mathbf{P}$.

Доказательство:

Рассмотрим автоматную функцию $f \in [\Omega \cup \mathbf{L}]$, она получилась конечной схемой операций суперпозиции из функций $\Omega \cup \mathbf{L}$. Каждая автоматная функция $l_i \in \mathbf{L}, i = 1, \dots, t$ участвующая в суперпозиции выражается суперпозицией автоматной функции с безусловными переходами $k_i, i = 1, \dots, t$ и функций $\mathbf{f}_{\mathbf{Sh}}, w_0, w_1, d_1, d_0$ по леммам 2 и 3. Пусть p_i период функции переходов k_i и $s = p_1 \cdot p_2 \cdot \dots \cdot p_t$, тогда

$$l_i^s \in [\mathbf{f}_{\mathbf{Sh}}, w_0, w_1, d_1, d_0],$$

а

$$f_i^s \in [\mathbf{f}_{\mathbf{Sh}}, w_0, w_1, d_1, d_0, f_T],$$

где T максимальное число состояний автоматных функций из Ω .

Значит, для любой автоматной функции из $f \in [\Omega \cup \mathbf{L}]$ найдется натуральное s , такое что f_i^s порождается одним и тем же конечным множеством автоматных функций не зависящим от s

$$[\mathbf{f}_{\mathbf{Sh}}, w_0, w_1, d_1, d_0, f_T].$$

Функция из утверждения 1 $f_n \in [\mathbf{f}_{\mathbf{Sh}}, f_n^s]$ при всех s . Если предположить, что система $[\Omega \cup \mathbf{L}]$ полна, то мы получим, что для любого n , автоматная функция $f_n \in [\mathbf{f}_{\mathbf{Sh}}, w_0, w_1, d_1, d_0, f_T]$. Известно [5], что $\mathbf{P} = [\mathbf{f}_{\mathbf{Sh}}, f_n | n \in \mathbf{N}]$.

Предположение о полноте $[\Omega \cup L]$ приводит к полноте конечного множества

$$[f_{Sh}, w_0, w_1, d_1, d_0, f_T].$$

что противоречиво. •

Полученные результаты верны также для линейных автоматов над другими конечными полями.

Список литературы

- [1] Гилл А., *Линейные последовательные машины*, М. Наука, 1974.
- [2] Gill A., *Linear sequential circuits*, McGraw-Hill, 1966.
- [3] Часовских А.А., “О полноте в классе линейных автоматов”, *Математические вопросы кибернетики*, **3** (1995), 140–166.
- [4] Бабин Д.Н., “Задача выразимости в некоторых классах автоматов”, *Комбинаторно-алгебраические методы в прикладной математике.*, 1985, 21–45.
- [5] Кудрявцев В.Б., Алешин С.В., Подколзин А.С., *Введение в теорию автоматов*, М. Наука, 1985.
- [6] Бабин Д.Н., “Вербальные подавтоматы и задача полноты”, *Вестник московского университета*, **3** (1985), 52–54.

Automata with linear transition functions

Babin D.N.

The problem of completeness of the system of automaton functions with linear transitions with respect to the operation of superposition is considered. This system is not complete; moreover, any system of automata that complements it to the basis is infinite.

Keywords: finite automaton, completeness, superposition, closed class.

Короткие единичные проверяющие тесты для контактных схем при обрывах и замыканиях контактов

Попков К.А.

Рассматривается задача реализации булевых функций избыточными двухполюсными контактными схемами, допускающими короткие единичные проверяющие тесты относительно обрывов и замыканий контактов. Описаны все функции, для которых минимальная длина указанного теста равна 0, 1, 2 и 3. Доказано, что для почти всех булевых функций от n переменных эта длина равна 4.

Ключевые слова: контактная схема, булева функция, обрыв контакта, замыкание контакта, единичный проверяющий тест.

1. Введение

В работе рассматривается задача синтеза легкотестируемых двухполюсных контактных схем [1], реализующих заданные булевы функции. (Слово «двухполюсная» в дальнейшем будем опускать.) Логический подход к тестированию контактных схем предложен С. В. Яблонским и И. А. Чегис в [2]. Представим, что имеется контактная схема S , реализующая булеву функцию $f(\tilde{x}^n)$, где $\tilde{x}^n = (x_1, \dots, x_n)$. Под воздействием некоторого источника неисправностей один или несколько контактов схемы S могут перейти в неисправное состояние. В качестве неисправностей контактов обычно рассматриваются их обрывы и замыкания. При обрыве контакта проводимость между его концами становится тождественно нулевой, а при замыкании — тождественно единичной. В результате схема S вместо исходной функции $f(\tilde{x}^n)$ будет реализовывать некоторую булеву функцию $g(\tilde{x}^n)$, вообще говоря, отличную от f . Все такие функции $g(\tilde{x}^n)$, получающиеся при всевозможных допустимых для рассматриваемой задачи неисправностях контактов схемы S , называются *функциями неисправности* данной схемы.

Введём следующие определения [3, 4, 5]. *Проверяющим тестом* для схемы S называется такое множество T наборов значений переменных x_1, \dots, x_n , что для любой отличной от $f(\tilde{x}^n)$ функции неисправности $g(\tilde{x}^n)$ схемы S в T найдётся набор $\tilde{\sigma}$, на котором $f(\tilde{\sigma}) \neq g(\tilde{\sigma})$. *Диагностическим тестом* для схемы S называется такое множество T наборов значений переменных x_1, \dots, x_n , что T является проверяющим тестом и, кроме того, для любых двух различных функций неисправности $g_1(\tilde{x}^n)$ и $g_2(\tilde{x}^n)$ схемы S в T найдётся набор $\tilde{\sigma}$, на котором $g_1(\tilde{\sigma}) \neq g_2(\tilde{\sigma})$. Число наборов в T называется *длиной* теста. В качестве тривиального диагностического (и проверяющего) теста длины 2^n для схемы S всегда можно взять множество, состоящее из всех двоичных наборов длины n . Тест называется *полным*, если в схеме могут быть неисправны сколько угодно контактов, и *единичным*, если в схеме может быть неисправен только один контакт. Единичные тесты обычно рассматривают для *неизбыточных схем* [5], т. е. для таких схем, в которых любая допустимая неисправность любого одного контакта приводит к функции неисправности, отличной от исходной функции, реализуемой данной схемой.

В дальнейшем будем считать, что в схемах могут происходить как обрывы, так и замыкания контактов независимо друг от друга.

Пусть множество T является единичным проверяющим тестом (ЕПТ) для некоторой контактной схемы S . Введём следующие обозначения: $D_{\text{ЕП}}(T)$ — длина теста T ; $D_{\text{ЕП}}(S) = \min D_{\text{ЕП}}(T)$, где минимум берётся по всем ЕПТ T для контактной схемы S ; $D_{\text{ЕП}}(f) = \min D_{\text{ЕП}}(S)$, где минимум берётся по всем избыточным контактным схемам S , реализующим функцию f ; $D_{\text{ЕП}}(n) = \max D_{\text{ЕП}}(f)$, где максимум берётся по всем булевым функциям f от n переменных. Функция $D_{\text{ЕП}}(n)$ называется *функцией Шеннона* длины ЕПТ. По аналогии с функциями $D_{\text{ЕП}}$ можно ввести функции $D_{\text{ЕД}}$, $D_{\text{ПП}}$ и $D_{\text{ПД}}$ для соответственно единичного диагностического, полного проверяющего и полного диагностического тестов, зависящие от T , от S , от f и от n (в определениях функций $D_{\text{ПП}}(f)$ и $D_{\text{ПД}}(f)$ не предполагается избыточности схем). Так, например, $D_{\text{ПД}}(n)$ — функция Шеннона длины полного диагностического теста.

Перечислим основные результаты, касающиеся задачи синтеза легкотестируемых контактных схем при рассматриваемых неисправностях. В [5, с. 113, теорема 9] с использованием идей С. В. Яблонского установлено, что функция $D_{\text{ЕД}}(n)$ асимптотически не превосходит $\frac{2^{n+1}}{n}$. Х. А. Мадатян в [6] доказал равенство $D_{\text{ПД}}(n) = 2^n$, а в [7] — соотношение

$D_{\text{ЕП}}(n) = O\left(\frac{2^n}{n\sqrt{n}}\right)$. Н. П. Редькин в [8] получил оценку $D_{\text{ПП}}(n) \leq \frac{15}{16} \cdot 2^n$. Из утверждения 2) теоремы 1 работы [9] следует, что для любой булевой функции $f(\tilde{x}^n)$ вида $\varphi(\tilde{x}^{n-1}) \oplus x^n$, где $\varphi(\tilde{x}^{n-1})$ — произвольная неконстантная булева функция, существует неизбыточная контактная схема, содержащая, помимо переменных из множества $\{x_1, \dots, x_n\}$, дополнительную входную переменную x_0 , допускающая ЕПТ длины $4n + 8$ и реализующая булеву функцию, не зависящую существенно от переменной x_0 и равную функции $f(\tilde{x}^n)$. В работе [10], в частности, доказано (теорема 4), что для любой булевой функции $f(\tilde{x}^n)$ существует неизбыточная контактная схема, содержащая не более пяти дополнительных входных переменных, допускающая ЕПТ длины не более 35 и реализующая такую булеву функцию, что $f(\tilde{x}^n)$ получается из неё подстановкой вместо этих дополнительных переменных некоторых булевых констант. В работах автора [11, 12, 13] рассмотрены задачи синтеза легкотестируемых контактных схем только при замыканиях либо только при обрывах (размыканиях) контактов.

Будем говорить, что некоторое свойство выполняется *для почти всех булевых функций от n переменных*, если отношение числа булевых функций от n переменных, для которых это свойство не выполняется, к числу всех булевых функций от n переменных (т. е. к 2^{2^n}) стремится к нулю при $n \rightarrow \infty$.

Далее будут рассматриваться только ЕПТ. Будут описаны все булевы функции f , для которых величина $D_{\text{ЕП}}(f)$ равна 0, 1, 2 и 3 (теорема 1), а также достаточно обширный класс булевых функций f , для которых она равна 4 (теорема 2); будет показано, что в этом классе содержатся почти все булевы функции от n переменных (теорема 3).

В дальнейшем нижний индекс ЕП у буквы D для краткости будем опускать.

2. Родственные функции

Введём обозначение

$$\alpha^\beta = \begin{cases} \alpha, & \text{если } \beta = 1, \\ \bar{\alpha}, & \text{если } \beta = 0, \end{cases}$$

где $\alpha \in \{0, 1\}$.

Заметим, что

$$\alpha^\beta = \alpha \oplus \beta \oplus 1. \quad (1)$$

Назовём булеву функцию $f_2(\tilde{x}^n)$ родственной булевой функции $f_1(\tilde{x}^n)$, если существуют такие попарно различные индексы i_1, \dots, i_n от 1 до n и такие булевы константы $\sigma_1, \dots, \sigma_n$, что $f_2(\tilde{x}^n) = f_1(x_{i_1}^{\sigma_1}, \dots, x_{i_n}^{\sigma_n})$.

Например, любая из функций $x_1\bar{x}_2, x_1x_3, \bar{x}_2\bar{x}_3, x_3\bar{x}_4$ родственна функции x_1x_2 , если все эти функции рассматриваются как функции от переменных x_1, \dots, x_n , где $n \geq 4$.

Отметим, что если булева функция $f_2(\tilde{x}^n)$ родственна булевой функции $f_1(\tilde{x}^n)$, то $f_1(\tilde{x}^n)$ родственна $f_2(\tilde{x}^n)$. Действительно, пусть попарно различные индексы j_1, \dots, j_n от 1 до n таковы, что $j_{i_1} = 1, \dots, j_{i_n} = n$; тогда

$$f_2(x_{j_1}^{\sigma_1}, \dots, x_{j_n}^{\sigma_n}) = f_1\left(\left(x_{j_{i_1}}^{\sigma_1}\right)^{\sigma_1}, \dots, \left(x_{j_{i_n}}^{\sigma_n}\right)^{\sigma_n}\right) = f_1(\tilde{x}^n),$$

т. е. $f_1(\tilde{x}^n)$ родственна $f_2(\tilde{x}^n)$.

Далее для краткости всюду вместо «закрывающий (размыкающий) контакт, отвечающий переменной x_i », будем говорить «контакт x_i » (соответственно «контакт \bar{x}_i »).

Лемма 1. Пусть булева функция $f_2(\tilde{x}^n)$ родственна булевой функции $f_1(\tilde{x}^n)$. Тогда $D(f_2) = D(f_1)$.

Доказательство. По определению существуют такие попарно различные индексы i_1, \dots, i_n от 1 до n и такие булевы константы $\sigma_1, \dots, \sigma_n$, что $f_2(\tilde{x}^n) = f_1(x_{i_1}^{\sigma_1}, \dots, x_{i_n}^{\sigma_n})$. Пусть S_1 — такая неизбыточная контактная схема, реализующая функцию f_1 , а T_1 — такой ЕПТ для этой схемы, что $D(T_1) = D(S_1) = D(f_1)$. Для любых $j \in \{1, \dots, n\}$, $\beta \in \{0, 1\}$ заменим в схеме S каждый контакт x_j^β на контакт $x_{i_j}^{\beta \oplus \sigma_j \oplus 1}$; указанные два контакта поставим в соответствие друг другу. Полученную схему обозначим через S_2 . На любом двоичном наборе $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ каждый контакт $x_{i_j}^{\beta \oplus \sigma_j \oplus 1}$ схемы S_2 функционирует в точности так же, как соответствующий ему контакт x_j^β схемы S_1 на наборе $(\alpha_{i_1}^{\sigma_1}, \dots, \alpha_{i_n}^{\sigma_n})$, поскольку

$$\alpha_{i_j}^{\beta \oplus \sigma_j \oplus 1} = \alpha_{i_j} \oplus (\beta \oplus \sigma_j \oplus 1) \oplus 1 = (\alpha_{i_j} \oplus \sigma_j \oplus 1) \oplus \beta \oplus 1 = (\alpha_{i_j}^{\sigma_j})^\beta$$

в силу (1). Отсюда следует, что схема S_2 при отсутствии в ней неисправностей выдаёт на наборе $\tilde{\alpha}$ значение $f_1(\alpha_{i_1}^{\sigma_1}, \dots, \alpha_{i_n}^{\sigma_n}) = f_2(\tilde{\alpha})$, т. е. реализует функцию $f_2(\tilde{x}^n)$.

Пусть T_2 — множество двоичных наборов длины n , получающееся из множества T_1 заменой каждого набора $(\pi_{s,i_1}, \dots, \pi_{s,i_n})$ (для удобства

занумеруем его компоненты именно так), принадлежащего T_1 , на набор $(\pi_{s,1}^{\sigma_1}, \dots, \pi_{s,n}^{\sigma_n})$. Докажем, что схема S_2 избыточна и допускает ЕПТ T_2 . Рассмотрим произвольную неисправность любого одного контакта этой схемы. Такую же неисправность соответствующего контакта схемы S_1 можно обнаружить на каком-то наборе $\tilde{\pi}_s = (\pi_{s,i_1}, \dots, \pi_{s,i_n}) \in T_1$, так как T_1 является ЕПТ для избыточной схемы S_1 . Значит, для получающейся функции неисправности $g(\tilde{x}^n)$ справедливо соотношение

$$g(\tilde{\pi}_s) \neq f_1(\tilde{\pi}_s). \quad (2)$$

Каждый контакт $x_{i_j}^{\beta \oplus \sigma_j \oplus 1}$ схемы S_2 на наборе $\tilde{\pi}'_s = (\pi_{s,1}^{\sigma_1}, \dots, \pi_{s,n}^{\sigma_n}) \in T_2$ при рассматриваемых неисправностях контактов в схемах S_1, S_2 функционирует так же, как соответствующий ему контакт x_j^β схемы S_1 на наборе $\tilde{\pi}_s$, поскольку

$$(\pi_{s,i_j}^{\sigma_j})^{\beta \oplus \sigma_j \oplus 1} = (\pi_{s,i_j} \oplus \sigma_j \oplus 1) \oplus (\beta \oplus \sigma_j \oplus 1) \oplus 1 = \pi_{s,i_j} \oplus \beta_i \oplus 1 = \pi_{s,i_j}^\beta$$

в силу (1). Отсюда следует, что схема S_2 выдаёт на наборе $\tilde{\pi}'_s$ значение $g(\tilde{\pi}_s)$, отличное от значения

$$f_1(\tilde{\pi}_s) = f_1((\pi_{s,i_1}^{\sigma_1})^{\sigma_1}, \dots, (\pi_{s,i_n}^{\sigma_n})^{\sigma_n}) = f_2(\tilde{\pi}'_s)$$

в силу (2), т. е. рассматриваемая неисправность схемы S_2 обнаруживается на наборе $\tilde{\pi}'_s \in T_2$. Из приведённых рассуждений вытекает, что схема S_2 избыточна и допускает ЕПТ T_2 , поэтому

$$D(f_2) \leq D(S_2) \leq D(T_2) = D(T_1) = D(f_1).$$

Тем самым доказано, что $D(f_2) \leq D(f_1)$. Аналогично доказывается неравенство $D(f_1) \leq D(f_2)$ (с учётом того, что функция $f_1(\tilde{x}^n)$ родственна функции $f_2(\tilde{x}^n)$). В итоге получаем равенство $D(f_2) = D(f_1)$. Лемма 1 доказана. \square

Двоичный набор $\tilde{\sigma}$ длины n будем называть *единичным (нулевым)* набором булевой функции $f(\tilde{x}^n)$, если $f(\tilde{\sigma}) = 1$ (соответственно, $f(\tilde{\sigma}) = 0$).

3. Схемы, допускающие тесты длины не более 3

Опишем вначале все булевы функции f , для которых $D(f) = 0$, $D(f) = 1$, $D(f) = 2$ и $D(f) = 3$.

Лемма 2. Для любой избыточной контактной схемы S , содержащей не менее трёх контактов, справедливо неравенство $D(S) \geq 4$.

Доказательство. Рассмотрим четыре случая.

1. Полюса схемы S совпадают. Тогда она, очевидно, реализует константу 1 как при отсутствии в ней неисправностей, так и при любой неисправности любого её контакта, поэтому избыточна; противоречие.

2. Все контакты схемы S принадлежат некоторой несамопересекающейся цепи C , соединяющей её полюса. Если в этой цепи присутствуют одновременно замыкающий и размыкающий контакт одной и той же переменной, то схема S , очевидно, реализует константу 0 как при отсутствии в ней неисправностей, так и при обрыве любого из контактов цепи C , поэтому избыточна. Если в цепи C присутствуют два замыкающих или два размыкающих контакта одной и той же переменной, то при замыкании любого одного из них, как нетрудно видеть, функция, реализуемая схемой S , не изменится, поэтому схема избыточна. Далее можно считать, что все контакты схемы S отвечают разным переменным. Пусть это контакты $x_1^{\sigma_1}, \dots, x_n^{\sigma_n}$, где $n \geq 3$. Тогда рассматриваемая схема при отсутствии в ней неисправностей реализует функцию $f = x_1^{\sigma_1} \dots x_n^{\sigma_n}$, при обрыве любого контакта — функцию $g_0 \equiv 0$, а при замыкании контакта $x_i^{\sigma_i}$ — функцию $g_i = x_1^{\sigma_1} \dots x_{i-1}^{\sigma_{i-1}} x_{i+1}^{\sigma_{i+1}} \dots x_n^{\sigma_n}$ для $i = 1, \dots, n$. Функция $f(\tilde{x}^n)$ отличается от функции $g_0(\tilde{x}^n)$ только на наборе $(\sigma_1, \dots, \sigma_n)$, а от функции $g_i(\tilde{x}^n)$ — только на наборе $(\sigma_1, \dots, \sigma_{i-1}, \bar{\sigma}_i, \sigma_{i+1}, \dots, \sigma_n)$, где $i = 1, \dots, n$, поэтому в любой ЕПТ для схемы S должны входить все указанные $n + 1 \geq 4$ наборов, откуда следует неравенство $D(S) \geq 4$.

3. Полюса схемы S не совпадают и каждый контакт в ней соединяет её полюса. Если среди этих контактов присутствуют одновременно замыкающий и размыкающий контакт одной и той же переменной, то схема S , очевидно, реализует константу 1 как при отсутствии в ней неисправностей, так и при замыкании любого из её контактов, поэтому избыточна. Если в ней присутствуют два замыкающих или два размыкающих контакта одной и той же переменной, то при обрыве любого одного из них, как нетрудно видеть, функция, реализуемая схемой S , не изменится, поэтому схема избыточна. Далее можно считать, что все контакты схемы S отвечают разным переменным. Пусть это контакты $x_1^{\sigma_1}, \dots, x_n^{\sigma_n}$, где $n \geq 3$. Тогда рассматриваемая схема при отсутствии в ней неисправностей реализует функцию $f = x_1^{\sigma_1} \vee \dots \vee x_n^{\sigma_n}$, при замыкании любого контакта — функцию $g_0 \equiv 1$, а при обрыве контакта $x_i^{\sigma_i}$ — функцию $g_i = x_1^{\sigma_1} \vee \dots \vee x_{i-1}^{\sigma_{i-1}} \vee x_{i+1}^{\sigma_{i+1}} \vee \dots \vee x_n^{\sigma_n}$ для $i = 1, \dots, n$. Функция $f(\tilde{x}^n)$ отличается от функции $g_0(\tilde{x}^n)$ только на наборе $(\bar{\sigma}_1, \dots, \bar{\sigma}_n)$, а

от функции $g_i(\tilde{x}^n)$ — только на наборе $(\bar{\sigma}_1, \dots, \bar{\sigma}_{i-1}, \sigma_i, \bar{\sigma}_{i+1}, \dots, \bar{\sigma}_n)$, где $i = 1, \dots, n$, поэтому в любой ЕПТ для схемы S должны входить все указанные $n + 1 \geq 4$ наборов, откуда следует неравенство $D(S) \geq 4$.

4. Отрицание объединения случаев 1–3: полюса схемы S не совпадают, не все её контакты принадлежат одной и той же несамопересекающейся цепи и в схеме S есть контакт K , хотя бы один конец которого отличен от полюсов схемы. Пусть схема S при отсутствии в ней неисправностей реализует функцию $f(\tilde{x}^n)$, и пусть T — произвольный ЕПТ для данной схемы. При замыкании любого её контакта функция, реализуемая схемой S , не может уменьшиться, поэтому данная неисправность может обнаруживаться только на нулевых наборах функции f , откуда следует, что в тесте T содержится хотя бы один нулевой набор $\tilde{\sigma}_0$ этой функции. Предположим, что это единственный нулевой набор функции f , содержащийся в T . Тогда ни один контакт схемы S не может проводить на наборе $\tilde{\sigma}_0$, поскольку в противном случае замыкание проводящего на этом наборе контакта нельзя было бы обнаружить на наборах из T . Замыкание контакта K должно обнаруживаться на наборе $\tilde{\sigma}_0$, т. е. в полученной схеме должна быть цепь между полюсами, проводящая на указанном наборе. Но единственным проводящим в этой схеме на наборе $\tilde{\sigma}_0$ контактом является K , следовательно, он соединяет полюса схемы; противоречие. Тем самым доказано, что в T содержатся хотя бы два нулевых набора функции f .

Далее, при обрыве любого контакта схемы S функция, реализуемая этой схемой, не может увеличиться, поэтому данная неисправность может обнаруживаться только на единичных наборах функции f , откуда следует, что в тесте T содержится хотя бы один единичный набор $\tilde{\sigma}_1$ этой функции. Пусть C — произвольная проводящая на этом наборе несамопересекающаяся цепь между полюсами схемы S . По предположению случая 4 в данной схеме присутствует хотя бы один контакт, не принадлежащий цепи C . Тогда при обрыве этого контакта в схеме S цепь C по-прежнему будет проводить на наборе $\tilde{\sigma}_1$ и схема на данном наборе выдаст значение $1 = f(\tilde{\sigma}_1)$. Это означает, что в тесте T должен содержаться ещё какой-то единичный набор функции f , отличный от $\tilde{\sigma}_1$, на котором обнаруживается обрыв указанного контакта. В итоге получаем, что в любой ЕПТ для схемы S должны входить хотя бы четыре набора, откуда следует неравенство $D(S) \geq 4$. Лемма 2 доказана. \square

Теорема 1. Пусть $f(\tilde{x}^n)$ — булева функция. Справедливо равенство

$$D(f) = \begin{cases} 0, & \text{если } f \equiv 0 \text{ или } f \equiv 1, \\ 2, & \text{если } f \text{ родственна функции } x_1, \\ 3, & \text{если } f \text{ родственна одной из функций } x_1x_2, x_1 \vee x_2. \end{cases}$$

В остальных случаях $D(f) \geq 4$.

Следствие 1. Для любого $n \geq 2$ справедливо неравенство $D(n) \geq 4$.

Доказательство теоремы 1. В случаях $f \equiv 0$, $f \equiv 1$ функцию f можно реализовать контактной схемой, не содержащей ни одного контакта. У такой схемы нет ни одной функции неисправности, поэтому пустое множество является для неё ЕПТ, откуда следует равенство $D(f) = 0$. В случае $f = x_1$ функцию f можно реализовать контактной схемой, содержащей ровно один контакт. При обрыве (замыкании) этого контакта схема станет реализовывать константу 0 (соответственно, константу 1), которую можно отличить от функции f на любом наборе, первая компонента которого равна 1 (соответственно, 0), поэтому $D(f) \leq 2$. С другой стороны, в любой избыточной контактной схеме S , реализующей функцию f , должен содержаться хотя бы один контакт; при обрыве (замыкании) этого контакта реализуемая схемой функция не может увеличиться (соответственно, уменьшиться), поэтому для обнаружения указанной неисправности в любом ЕПТ T для схемы S должен содержаться хотя бы один единичный (соответственно, нулевой) набор функции f . Отсюда следует неравенства $D(T) \geq 2$, $D(S) \geq 2$ и $D(f) \geq 2$, а вместе с последним из них равенство $D(f) = 2$, т. е. $D(x_1) = 2$.

Если функция $f(\tilde{x}^n)$ родственна функции x_1 , то $D(f) = 2$ в силу леммы 1.

Пусть $f = x_1x_2$. Докажем равенство $D(f) = 3$. Реализуем функцию f схемой $S_{\&}$, представляющей собой цепь из двух контактов: x_1 и x_2 . Легко видеть, что всевозможными функциями неисправности такой схемы являются функции $g_0 \equiv 0$, $g_1 = x_1$ и $g_2 = x_2$. Функция g_0 (функция g_1 , функция g_2) отличается от функции f в точности на всех таких наборах, первые две компоненты каждого из которых равны 1 и 1 соответственно (1 и 0 соответственно, 0 и 1 соответственно). Указанные три множества наборов попарно не пересекаются, а в любой ЕПТ для схемы $S_{\&}$ должно входить хотя бы по одному набору из каждого из них, поэтому $D(S_{\&}) \geq 3$. С другой стороны, выбрав по произвольному набору из каждого из этих множеств, получим ЕПТ длины 3 для схемы $S_{\&}$. Таким

образом, $D(S_{\&}) = 3$. Далее заметим, что единственной контактной схемой, содержащей не более двух контактов и реализующей функцию f (с точностью до перестановки полюсов), является схема $S_{\&}$, поэтому любая другая избыточная схема S' , реализующая эту функцию, содержит не менее трёх контактов и $D(S') \geq 4$ по лемме 2. В итоге получаем, что $D(f) = D(S_{\&}) = 3$, т. е. $D(x_1x_2) = 3$.

Пусть $f = x_1 \vee x_2$. Реализуем функцию f схемой S_{\vee} , представляющей собой параллельное соединение двух контактов: x_1 и x_2 . Дальнейшие рассуждения проводятся двойственным образом по отношению к рассуждениям из случая $f = x_1x_2$ (принцип двойственности см., например, в [14, с. 24]). В итоге получаем, что $D(x_1 \vee x_2) = 3$.

Если функция $f(\tilde{x}^n)$ родственна одной из функций x_1x_2 , $x_1 \vee x_2$, то $D(f) = 3$ в силу леммы 1.

Нетрудно заметить, что контактные схемы, содержащие не более двух контактов, могут реализовывать только булевы функции f , рассмотренные выше. Любая другая булева функция f может быть реализована только контактными схемами, содержащими не менее трёх контактов, откуда с учётом леммы 2 следует неравенство $D(f) \geq 4$. Теорема 1 доказана. \square

4. Схемы, допускающие тесты длины 4

Пусть $n \geq 2$. Назовём $L_{(n)}$ -блоком четырёхполюсную контактную схему с полюсами A_1 , A_2 , A_3 и A_4 , содержащую четыре контакта: контакт x_{t_1} между полюсами A_1 и A_3 , контакт x_{t_2} между полюсами A_2 и A_4 , контакт \bar{x}_{t_3} между полюсами A_2 и A_3 и контакт \bar{x}_{t_4} между полюсами A_1 и A_4 , где либо $t_1, t_2, t_3, t_4 \in \{1, \dots, n-1\}$, либо $t_1 = t_2 = t_3 = t_4 = n$ (см. рис. 1). Для удобства будем обозначать такой $L_{(n)}$ -блок через $B_{t_3, t_4}^{t_1, t_2}$.

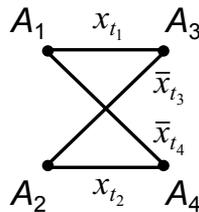


Рис. 1. $L_{(n)}$ -блок

Назовём $L_{(n)}$ -схемой четырёхполосную контактную схему S с полюсами a_0, b_0, a_m и b_m , составленную из произвольных $L_{(n)}$ -блоков B_1, \dots, B_m для произвольного $m \in \mathbb{N}$ следующим образом: полюса a_0 и b_0 схемы S совпадают с полюсами соответственно A_1 и A_2 блока B_1 ; для любого $i \in \{1, \dots, m-1\}$ полюса A_3 и A_4 блока B_i совпадают с полюсами соответственно A_1 и A_2 блока B_{i+1} и для удобства объявляются вершинами соответственно a_i и b_i схемы; полюса a_m и b_m схемы S совпадают с полюсами соответственно A_3 и A_4 блока B_m (см. рис. 2). Наличие буквы L в названии « $L_{(n)}$ -схема» обусловлено тем, что похожее строение имеет известная схема, реализующая линейную булеву функцию $x_1 \oplus \dots \oplus x_n$ и содержащая $4n - 4$ контактов (см., например, [1, с. 44, рис. 21]).

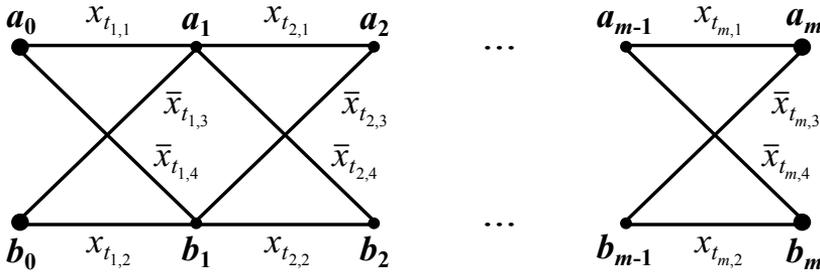


Рис. 2. $L_{(n)}$ -схема

Пусть S — произвольная $L_{(n)}$ -схема, составленная из чётного числа m $L_{(n)}$ -блоков, среди которых число блоков вида $B_{n,n}^{n,n}$ также чётно. Назовём $L'_{(n)}$ -схемой контактную схему с полюсами b_0 и a_m , получающуюся из схемы S добавлением вершины c_1 и соединением её с полюсами b_m и a_0 схемы S контактами x_1 и x_n соответственно, а также добавлением вершины c_2 и соединением её с полюсами b_m и a_0 схемы S контактами \bar{x}_1 и \bar{x}_n соответственно (см. рис. 3).

Введём обозначения $\tilde{0}^l = \underbrace{0, \dots, 0}_l$, $\tilde{1}^l = \underbrace{1, \dots, 1}_l$, где $l \in \mathbb{N} \cup \{0\}$.

(В случае $l = 0$ они обозначают пустую строку: например, $(\tilde{0}^0, 1, \tilde{0}^{n-1}) = (1, \tilde{0}^{n-1})$.)

Лемма 3. Любая $L'_{(n)}$ -схема избыточна и допускает ЕПТ $T = \{(\tilde{0}^n), (\tilde{0}^{n-1}, 1), (\tilde{1}^{n-1}, 0), (\tilde{1}^n)\}$; при этом в случае отсутствия в ней неисправностей она проводит на наборах $(\tilde{0}^n)$ и $(\tilde{1}^n)$ и не проводит на наборах $(\tilde{0}^{n-1}, 1)$ и $(\tilde{1}^{n-1}, 0)$.

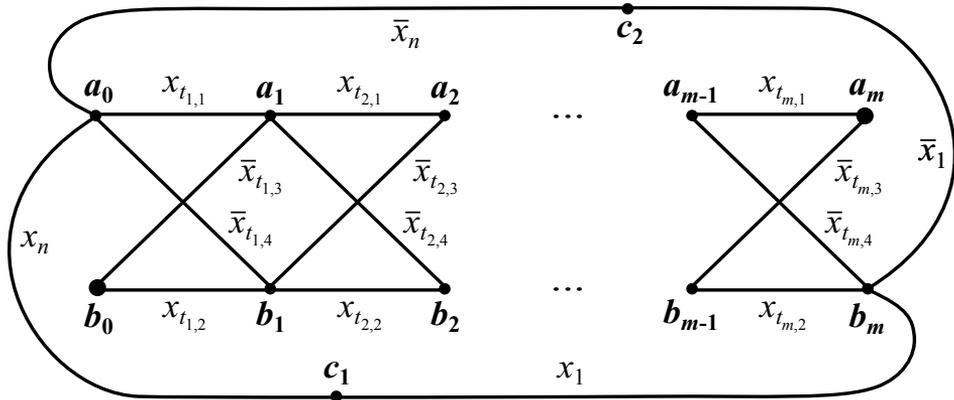


Рис. 3. $L'_{(n)}$ -схема

Доказательство. Пусть S' — произвольная $L'_{(n)}$ -схема, и пусть она при отсутствии неисправностей реализует между своими полюсами булеву функцию $f(\tilde{x}^n)$ и получена из некоторой $L_{(n)}$ -схемы S способом, указанным в определении $L'_{(n)}$ -схемы; в свою очередь, схема S состоит из $L_{(n)}$ -блоков B_1, \dots, B_m для некоторого чётного m , среди которых число μ блоков вида $B_{n,n}^{\mu}$ также чётно; в случае $\mu \geq 2$ обозначим номера этих μ блоков в порядке возрастания через i_1, \dots, i_μ . Докажем, что схема S' неизбыточна и допускает ЕПТ T . Для этого достаточно доказать, что любая неисправность (обрыв или замыкание) любого одного контакта данной схемы обнаруживается на каком-то наборе из множества T . Рассмотрим произвольную такую неисправность. Нетрудно видеть, что все замыкающие (размыкающие) контакты схемы S' принадлежат несамопересекающейся цепи $b_0 - b_1 - \dots - b_m - c_1 - a_0 - a_1 - \dots - a_m$ (соответственно, $b_0 - a_1 - b_2 - \dots - a_{m-1} - b_m - c_2 - a_0 - b_1 - a_2 - \dots - b_{m-1} - a_m$; здесь используется, что m чётно), соединяющей полюса схемы. Поэтому при отсутствии неисправностей схема S' проводит на наборе $(\tilde{1}^n)$ (соответственно, $(\tilde{0}^n)$), а при обрыве произвольного её замыкающего (соответственно, размыкающего) контакта — не проводит на этом наборе. Таким образом, обрыв любого контакта данной схемы обнаруживается на одном из наборов $(\tilde{1}^n), (\tilde{0}^n) \in T$.

Далее, на наборе $(\tilde{1}^{n-1}, 0)$ в схеме S' в случае отсутствия в ней неисправностей проводят все контакты $x_1, \dots, x_{n-1}, \bar{x}_n$ и только они. Ни один блок из множества $\{B_1, \dots, B_m\} \setminus \{B_{i_1}, \dots, B_{i_\mu}\}$ в силу определения $L_{(n)}$ -

блока не содержит контактов переменной x_n (в случае $\mu = 0$ множество $\{B_{i_1}, \dots, B_{i_\mu}\}$ считаем пустым). Поэтому нетрудно видеть, что множество проводящих на наборе $(\tilde{I}^{n-1}, 0)$ контактов схемы S' представляет собой объединение двух непересекающихся и несамопересекающихся цепей: $b_0 - b_1 - \dots - b_{i_1-1} - a_{i_1} - a_{i_1+1} - \dots - a_{i_2-1} - b_{i_2} - b_{i_2+1} - \dots - a_{i_\mu-1} - b_{i_\mu} - b_{i_\mu+1} - \dots - b_m - c_1$ и $c_2 - a_0 - a_1 - \dots - a_{i_1-1} - b_{i_1} - b_{i_1+1} - \dots - b_{i_2-1} - a_{i_2} - a_{i_2+1} - \dots - b_{i_\mu-1} - a_{i_\mu} - a_{i_\mu+1} - \dots - a_m$ (здесь используется, что μ чётно; в случае $\mu = 0$ эти цепи вырождаются в $b_0 - b_1 - \dots - b_m - c_1$ и $c_2 - a_0 - a_1 - \dots - a_m$ соответственно. Везде в случае $i < j$ участок цепи $a_i - \dots - a_j$ или $b_i - \dots - b_j$ считаем пустым), причём полюса b_0 и a_m принадлежат разным цепям, а любой из контактов $\bar{x}_1, \dots, \bar{x}_{n-1}, x_n$ этой схемы соединяет какую-то вершину одной из указанных цепей с какой-то вершиной другой. (Пример строения схемы S' при $m = 6, \mu = 2, i_1 = 3, i_2 = 5$ приведён на рис. 4; сплошными линиями выделены все контакты $x_1, \dots, x_{n-1}, \bar{x}_n$, а пунктирными — все контакты $\bar{x}_1, \dots, \bar{x}_{n-1}, x_n$.) Отсюда следует, что при отсутствии неисправностей схема S' не проводит на наборе $(\tilde{I}^{n-1}, 0)$, а при замыкании любого из её контактов $\bar{x}_1, \dots, \bar{x}_{n-1}, x_n$ — проводит на этом наборе. Таким образом, замыкание любого такого контакта данной схемы обнаруживается на наборе $(\tilde{I}^{n-1}, 0) \in T$.

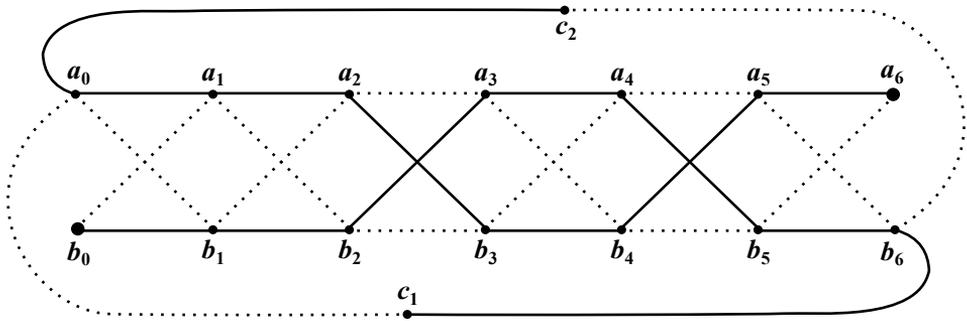


Рис. 4. Строение схемы S'

Осталось рассмотреть замыкание любого из контактов $x_1, \dots, x_{n-1}, \bar{x}_n$ схемы S' . Переобозначим вершины этой схемы — а именно, поменяем местами вершины a_i и b_i для каждого нечётного i от 1 до $m - 1$. Тогда схема S' примет вид, представленный на рис. 5. Дальнейшие рассуждения полностью совпадают с рассуждениями из предыдущего абзаца при замене набора $(\tilde{I}^{n-1}, 0)$ на набор $(\tilde{O}^{n-1}, 1)$, а контактов $x_1, \dots, x_{n-1}, \bar{x}_n$ — на контакты $\bar{x}_1, \dots, \bar{x}_{n-1}, x_n$ и наоборот. Получаем, что рассматриваемая

неисправность обнаруживается на наборе $(\tilde{0}^{n-1}, 1) \in T$, а при отсутствии неисправностей схема S' не проводит на этом наборе. Лемма 3 доказана.

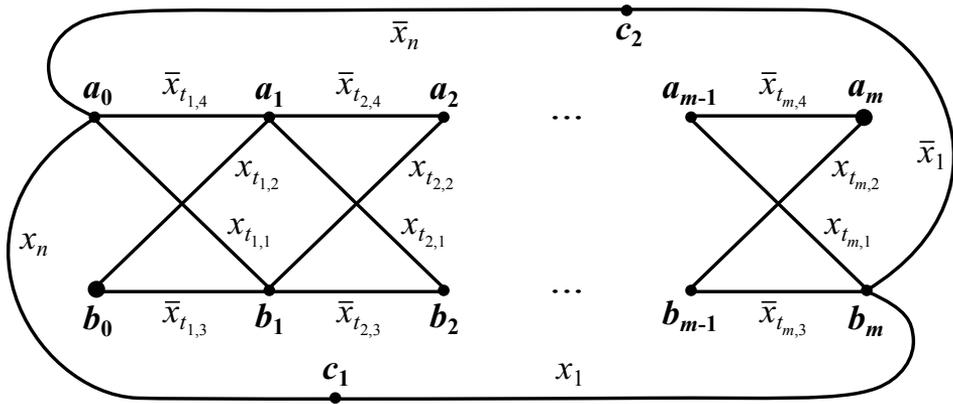


Рис. 5. Схема S' после переобозначения вершин

□

5. Изучение возможностей реализации булевых функций $L'_{(n)}$ -схемами

Дальнейшие рассуждения направлены на поиск булевых функций, которые могут быть реализованы $L'_{(n)}$ -схемами. С учётом леммы 3 для любой такой функции f выполнено соотношение $D(f) \leq 4$. Параллельно будем оценивать сверху сложность каждой из построенных схем, т. е. число контактов в ней, в зависимости от n .

Всюду в данном разделе считаем, что все контакты, содержащиеся в схемах, исправны.

Контакт, соединяющий произвольные две вершины v и v' контактной схемы, будем обозначать через $[v, v']$.

Два контакта будем называть *противоположными*, если один из них имеет вид x_i , а другой — вид \bar{x}_i , где $i \in \mathbb{N}$.

Под *длиной цепи* в контактной схеме будем понимать число содержащихся в этой цепи контактов.

Лемма 4. Для любого двоичного набора $\tilde{\alpha}$ длины $n-1$, $n \geq 3$, отличного от наборов $(\tilde{0}^{n-1})$ и $(\tilde{1}^{n-1})$, существует $L_{(n)}$ -схема $S_{\tilde{\alpha}}$, составленная из

$m = 2n - 5$ $L_{(n)}$ -блоков, содержащая только контакты переменных из множества $\{x_1, \dots, x_{n-1}\}$ и обладающая следующими свойствами:

(i) на наборе $\tilde{\alpha}$ проводимость между полюсами схемы $S_{\tilde{\alpha}}$ из любой из пар (a_0, a_m) , (a_0, b_m) , (b_0, a_m) отсутствует;

(ii) на наборе $\tilde{\alpha}$ есть проводимость между полюсами b_0 и b_m схемы $S_{\tilde{\alpha}}$;

(iii) на любом двоичном наборе $\tilde{\tau}$ длины $n - 1$, отличном от наборов $\tilde{\alpha}$, $(\tilde{0}^{n-1})$ и $(\tilde{1}^{n-1})$, в схеме $S_{\tilde{\alpha}}$ есть проводимости либо между полюсами из каждой из пар (a_0, a_m) , (a_0, b_m) , либо между полюсами из каждой из пар (b_0, a_m) , (b_0, b_m) ,

Доказательство. Пусть $\tilde{\alpha} = (\alpha_1, \dots, \alpha_{n-1})$ и при этом $\alpha_{i_1} = \dots = \alpha_{i_q} = 1$, $\alpha_{i_{q+1}} = \dots = \alpha_{i_{n-1}} = 0$, где $q \in \{1, \dots, n - 2\}$, а i_1, \dots, i_{n-1} — попарно различные индексы от 1 до $n - 1$ (для определённости можно считать, что $i_1 < \dots < i_q$ и $i_{q+1} < \dots < i_{n-1}$). По определению $L_{(n)}$ -схема однозначно задаётся числом $m \in \mathbb{N}$ и $L_{(n)}$ -блоками B_1, \dots, B_m . Положим $m = 2n - 5$, $B_1 = B_{i_1, i_1}^{i_{n-1}, i_1}$; $B_{2j} = B_{i_j, i_{j+1}}^{i_{j+1}, i_j}$, $B_{2j+1} = B_{i_{j+1}, i_j}^{i_{j+1}, i_j}$ для каждого $j = 1, \dots, q - 1$ (при $q \geq 2$); $B_{2j} = B_{i_{j+2}, i_{j+1}}^{i_{j+2}, i_{j+1}}$, $B_{2j+1} = B_{i_{j+2}, i_{j+1}}^{i_{j+2}, i_{j+1}}$ для каждого $j = q, \dots, n - 3$ (при $q \leq n - 3$). Полученную $L_{(n)}$ -схему обозначим через $S_{\tilde{\alpha}}$ (её вид при $n = 5$, $\tilde{\alpha} = (1, 1, 0, 0)$ показан на рис. 6). Проверим выполнение для этой схемы свойств (i)–(iii).

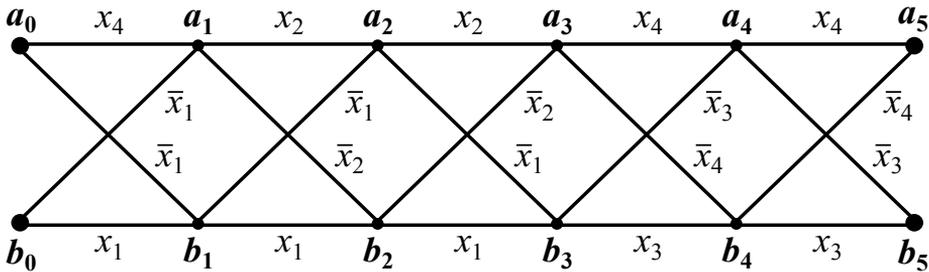


Рис. 6. Схема $S_{\tilde{\alpha}}$

Предположим, что свойство (i) не выполнено, т. е. в схеме $S_{\tilde{\alpha}}$ есть несамопересекающаяся цепь между её полюсами из какой-то из пар (a_0, a_m) , (a_0, b_m) , (b_0, a_m) , проводящая на наборе $\tilde{\alpha}$. Из всех таких цепей выберем цепь C наименьшей длины. Она не может соединять полюса a_0 и a_m , а также полюса a_0 и b_m , так как на наборе $\tilde{\alpha}$ ни один из контактов $[a_0, a_1]$, $[a_0, b_1]$ не проводит (в силу определения блока B_1 это контакты

$x_{i_{n-1}}, \bar{x}_{i_1}$ соответственно). Поэтому цепь C соединяет полюса b_0 и a_m схемы $S_{\tilde{\alpha}}$. Вершины этой цепи при движении от полюса b_0 к полюсу a_m обозначим через v_0, \dots, v_s , тогда $v_0 = b_0$ и $v_s = a_m$. Кроме того, $v_1 = b_1$, поскольку на наборе $\tilde{\alpha}$ контакт $[b_0, a_1]$ не проводит (это контакт \bar{x}_{i_1}). Также

$$v_1, \dots, v_s \notin \{a_0, b_0\} \quad (3)$$

в силу выбора цепи C .

Для удобства будем считать, что вершины a_d и b_d не принадлежат схеме $S_{\tilde{\alpha}}$ для любого $d \geq m + 1$. Докажем, что $v_d \in \{a_d, b_d\}$ для любого $d \in \{0, \dots, s\}$ (в частности, $s \leq m$). Предположим противное. Пусть d — наименьший индекс от 0 до s , для которого $v_d \notin \{a_d, b_d\}$. Тогда $d \geq 2$, $v_{d-2} \in \{a_{d-2}, b_{d-2}\}$ и $v_{d-1} \in \{a_{d-1}, b_{d-1}\}$. Из последнего соотношения вытекает неравенство $d-1 \leq m$. Каждая из вершин a_{d-1}, b_{d-1} в схеме $S_{\tilde{\alpha}}$ соединена контактами с вершинами a_{d-2} и b_{d-2} , а также — в случае $d-1 < m$ — с вершинами a_d и b_d . Поэтому из соотношений $v_{d-1} \in \{a_{d-1}, b_{d-1}\}$ и $v_d \notin \{a_d, b_d\}$ следует, что $v_d \in \{a_{d-2}, b_{d-2}\}$; в частности, $d \geq 3$ в силу (3). Таким образом,

$$2 \leq d-1 \leq m = 2n-5. \quad (4)$$

Далее, из соотношений $v_{d-2} \in \{a_{d-2}, b_{d-2}\}$, $v_d \in \{a_{d-2}, b_{d-2}\}$ и того, что цепь C несамопересекающаяся, следует равенство $\{v_{d-2}, v_d\} = \{a_{d-2}, b_{d-2}\}$. Если $v_{d+1} \in \{a_{d-3}, b_{d-3}\}$, то на участке $v_{d+1} - \dots - v_s$ цепи C обязательно должна содержаться одна из вершин a_{d-2}, b_{d-2} , а значит, одна из вершин v_{d-2}, v_d , однако обе эти вершины уже содержатся на участке $v_0 - \dots - v_d$ данной цепи; противоречие. Поэтому $v_{d+1} \in \{a_{d-1}, b_{d-1}\}$. С учётом ранее установленного соотношения $v_{d-1} \in \{a_{d-1}, b_{d-1}\}$ получаем, что $\{v_{d-1}, v_{d+1}\} = \{a_{d-1}, b_{d-1}\}$. Значит, на участке $v_{d-2} - v_{d-1} - v_d - v_{d+1}$ цепи C чередуются вершины из множеств $\{a_{d-2}, b_{d-2}\}$ и $\{a_{d-1}, b_{d-1}\}$, причём на нём содержатся все вершины $a_{d-2}, b_{d-2}, a_{d-1}, b_{d-1}$, являющиеся полюсами $L_{(n)}$ -блока \mathbf{B}_{d-1} . Из (4) следует неравенство $n \geq 4$ и существование такого $j \in \{1, \dots, n-3\}$, что блок \mathbf{B}_{d-1} имеет один из видов $B_{i_j, i_{j+1}}^{i_{j+1}, i_j}$, $B_{i_{j+1}, i_j}^{i_{j+1}, i_j}$, $B_{i_{j+1}, i_{j+2}}^{i_{j+2}, i_{j+1}}$ или $B_{i_{j+2}, i_{j+1}}^{i_{j+2}, i_{j+1}}$. Заметим, что в блоке каждого из этих видов имеется по одному контакту $x_{i'}$, $x_{i''}$, $\bar{x}_{i'}$ и $\bar{x}_{i''}$ для некоторых $i', i'' \in \{i_j, i_{j+1}, i_{j+2}\}$, $i' \neq i''$. На участке $v_{d-2} - v_{d-1} - v_d - v_{d+1}$ цепи C содержатся три из этих четырёх контактов, поэтому какие-то два из указанных трёх контактов обязательно являются противоположными. Наличие противоположных контактов в данной цепи означает, что она не может проводить на наборе $\tilde{\alpha}$; противо-

речие. Тем самым доказано, что $v_d \in \{a_d, b_d\}$ для любого $d \in \{0, \dots, s\}$; в частности, $s \leq m$. Отсюда и из соотношения $v_s = a_m$ следует, что

$$s = m = 2n - 5,$$

т. е. $v_{2n-5} = a_{2n-5}$. Выше было показано, что $v_1 = b_1$ и $n \geq 4$. Поэтому существует такой индекс $j \in \{1, \dots, n - 3\}$, что $v_{2j-1} = b_{2j-1}$ и $v_{2j+1} = a_{2j+1}$. Рассмотрим четыре случая.

1. Пусть $j \leq q - 1$ и $v_{2j} = a_{2j}$. Тогда участок $v_{2j-1} - v_{2j} - v_{2j+1}$ цепи C имеет вид $b_{2j-1} - a_{2j} - a_{2j+1}$ и содержит контакты \bar{x}_{i_j} и $x_{i_{j+1}}$ из блоков B_{2j} и B_{2j+1} соответственно (см. определения этих блоков в начале доказательства леммы). Но $\alpha_{i_j} = 1$, поскольку $j \leq q$, следовательно, контакт \bar{x}_{i_j} , а вместе с ним и цепь C не могут проводить на наборе $\tilde{\alpha}$. Противоречие.

2. Пусть $j \leq q - 1$ и $v_{2j} = b_{2j}$. Тогда участок $v_{2j-1} - v_{2j} - v_{2j+1}$ цепи C имеет вид $b_{2j-1} - b_{2j} - a_{2j+1}$ и содержит контакты x_{i_j} и $\bar{x}_{i_{j+1}}$ из блоков B_{2j} и B_{2j+1} соответственно. Но $\alpha_{i_{j+1}} = 1$, поскольку $j + 1 \leq q$, следовательно, контакт $\bar{x}_{i_{j+1}}$, а вместе с ним и цепь C не могут проводить на наборе $\tilde{\alpha}$. Противоречие.

3. Пусть $j \geq q$ и $v_{2j} = a_{2j}$. Тогда участок $v_{2j-1} - v_{2j} - v_{2j+1}$ цепи C имеет вид $b_{2j-1} - a_{2j} - a_{2j+1}$ и содержит контакты $\bar{x}_{i_{j+1}}$ и $x_{i_{j+2}}$ из блоков B_{2j} и B_{2j+1} соответственно (см. определения этих блоков в начале доказательства леммы). Но $\alpha_{i_{j+2}} = 0$, поскольку $j + 2 \geq q + 1$, следовательно, контакт $x_{i_{j+2}}$, а вместе с ним и цепь C не могут проводить на наборе $\tilde{\alpha}$. Противоречие.

4. Пусть $j \geq q$ и $v_{2j} = b_{2j}$. Тогда участок $v_{2j-1} - v_{2j} - v_{2j+1}$ цепи C имеет вид $b_{2j-1} - b_{2j} - a_{2j+1}$ и содержит контакты $x_{i_{j+1}}$ и $\bar{x}_{i_{j+2}}$ из блоков B_{2j} и B_{2j+1} соответственно. Но $\alpha_{i_{j+1}} = 0$, поскольку $j + 1 \geq q + 1$, следовательно, контакт $x_{i_{j+1}}$, а вместе с ним и цепь C не могут проводить на наборе $\tilde{\alpha}$. Противоречие.

Во всех случаях получено противоречие, поэтому свойство (i) доказано.

Докажем промежуточное свойство (iv) схемы $S_{\tilde{\alpha}}$, которое будет использоваться при доказательстве свойств (ii), (iii): функции проводимости между вершинами a_{2j-1} и $a_{2j'-1}$, а также между вершинами b_{2j-1} и $b_{2j'-1}$ в этой схеме тождественно равны 1 для любых $j, j' \in \{1, \dots, n - 2\}$.

Достаточно доказать свойство (iv) для случая $j' = j + 1$. Между вершинами a_{2j-1} и a_{2j+1} в схеме $S_{\tilde{\alpha}}$ есть, в частности, цепи $a_{2j-1} - a_{2j} -$

a_{2j+1} и $a_{2j-1} - b_{2j} - a_{2j+1}$. В силу определения блоков B_{2j} и B_{2j+1} первая из этих цепей содержит два контакта x_t , где

$$t = \begin{cases} i_{j+1}, & \text{если } j \leq q - 1, \\ i_{j+2}, & \text{если } j \geq q, \end{cases}$$

а вторая цепь — два контакта \bar{x}_t . Далее, между вершинами b_{2j-1} и b_{2j+1} в схеме $S_{\tilde{\alpha}}$ есть, в частности, цепи $b_{2j-1} - b_{2j} - b_{2j+1}$ и $b_{2j-1} - a_{2j} - b_{2j+1}$. В силу определения блоков B_{2j} и B_{2j+1} первая из этих цепей содержит два контакта $x_{t'}$, где

$$t' = \begin{cases} i_j, & \text{если } j \leq q - 1, \\ i_{j+1}, & \text{если } j \geq q, \end{cases}$$

а вторая цепь — два контакта $\bar{x}_{t'}$. Таким образом, функции проводимости между вершинами a_{2j-1} и $a_{2j'-1}$, а также между вершинами b_{2j-1} и $b_{2j'-1}$ в рассматриваемой схеме не меньше $x_t \vee \bar{x}_t \equiv 1$ и $x_{t'} \vee \bar{x}_{t'} \equiv 1$ соответственно, т. е. тождественно равны 1. Свойство (iv) доказано.

Докажем свойство (ii). В силу свойства (iv) и нечётности m достаточно доказать, что на наборе $\tilde{\alpha}$ есть проводимость между вершинами b_0 и b_1 схемы $S_{\tilde{\alpha}}$, а это утверждение очевидно, так как данные две вершины по определению блока B_1 соединены контактом x_{i_1} , проводящим на указанном наборе.

Докажем свойство (iii). Компоненты набора $\tilde{\tau}$ обозначим через $\tau_1, \dots, \tau_{n-1}$. Рассмотрим три случая.

1. Пусть $q \geq 2$ и $\tau_{i_j} \neq \tau_{i_{j+1}}$ для некоторого $j \in \{1, \dots, q-1\}$. В силу определения блока B_1 вершина b_1 в схеме $S_{\tilde{\alpha}}$ соединена с вершинами a_0 и b_0 контактами \bar{x}_{i_1} и x_{i_1} соответственно, один из которых проводит на наборе $\tilde{\tau}$. Поэтому достаточно доказать, что в этой схеме на указанном наборе есть проводимость между вершиной b_1 и каждой из вершин a_m, b_m . В силу свойства (iv) вершины b_1, a_m и b_m в предыдущем предложении можно заменить на b_{2j-1}, a_{2j+1} и b_{2j+1} соответственно. Проводимость между вершинами b_{2j-1} и b_{2j+1} есть по этому же свойству; исследуем проводимость между вершинами b_{2j-1} и a_{2j+1} . Между ними в схеме $S_{\tilde{\alpha}}$ есть, в частности, цепи $b_{2j-1} - a_{2j} - a_{2j+1}$ и $b_{2j-1} - b_{2j} - a_{2j+1}$. По определению блоков B_{2j} и B_{2j+1} первая из этих цепей содержит по одному контакту \bar{x}_{i_j} и $x_{i_{j+1}}$, а вторая цепь — по одному контакту x_{i_j} и $\bar{x}_{i_{j+1}}$. Одна из них проводит на наборе $\tilde{\tau}$, так как $\tau_{i_j} \neq \tau_{i_{j+1}}$. Случай 1 разобран.

2. Пусть $q \leq n-3$ и $\tau_{i_{j+1}} \neq \tau_{i_{j+2}}$ для некоторого $j \in \{q, \dots, n-3\}$. Так же, как в случае 1, достаточно доказать наличие проводимости между вершинами b_{2j-1} и a_{2j+1} в схеме $S_{\tilde{\alpha}}$ на наборе $\tilde{\tau}$. Между указанными вершинами есть, в частности, цепи $b_{2j-1} - a_{2j} - a_{2j+1}$ и $b_{2j-1} - b_{2j} - a_{2j+1}$. По определению блоков \mathbb{B}_{2j} и \mathbb{B}_{2j+1} первая из этих цепей содержит по одному контакту $\bar{x}_{i_{j+1}}$ и $x_{i_{j+2}}$, а вторая цепь — по одному контакту $x_{i_{j+1}}$ и $\bar{x}_{i_{j+2}}$. Одна из них проводит на наборе $\tilde{\tau}$, так как $\tau_{i_{j+1}} \neq \tau_{i_{j+2}}$. Случай 2 разобран.

3. Отрицание объединения случаев 1 и 2: пусть $\tau_{i_1} = \dots = \tau_{i_q}$ и $\tau_{i_{q+1}} = \dots = \tau_{i_{n-1}}$. Тогда $\tau_{i_1} = \dots = \tau_{i_q} = 0$ и $\tau_{i_{q+1}} = \dots = \tau_{i_{n-1}} = 1$, поскольку $\tilde{\tau} \notin \{\tilde{\alpha}, (\tilde{0}^{n-1}), (\tilde{1}^{n-1})\}$. В силу определения блока \mathbb{B}_1 вершина a_1 в схеме $S_{\tilde{\alpha}}$ соединена с вершинами a_0 и b_0 контактами $x_{i_{n-1}}$ и \bar{x}_{i_1} соответственно, каждый из которых проводит на наборе $\tilde{\tau}$; кроме того, вершина b_1 соединена с вершинами a_0 и b_0 контактами \bar{x}_{i_1} и x_{i_1} соответственно, один из которых проводит на наборе $\tilde{\tau}$. Поэтому на указанном наборе есть проводимость либо между вершинами из каждой из пар (a_0, a_1) , (a_0, b_1) , либо между вершинами из каждой из пар (b_0, a_1) , (b_0, b_1) . Осталось заметить, что по свойству (iv) есть проводимость между вершинами a_1 и a_m , а также между вершинами b_1 и b_m . Случай 3 разобран. Свойство (iii), а вместе с ним лемма 4 доказаны. \square

Сложность построенной схемы $S_{\tilde{\alpha}}$ равна $4(2n-5) = 8n-20$.

Лемма 5. Пусть $n \geq 3$; $\alpha_1, \dots, \alpha_{n-1}$ — произвольные булевы константы, не все из которых равны между собой; $\tilde{\sigma}_0 = (\alpha_1, \dots, \alpha_{n-1}, 0)$, $\tilde{\sigma}_1 = (\alpha_1, \dots, \alpha_{n-1}, 1)$ и M — одно из множеств $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$, $\{\tilde{\sigma}_0\}$, $\{\tilde{\sigma}_1\}$. Тогда существует $L_{(n)}$ -схема S_M , обладающая следующими свойствами:

(v) на любом наборе из множества M проводимость между полюсами схемы S_M из любой из пар (a_0, a_m) , (a_0, b_m) , (b_0, a_m) , (b_0, b_m) отсутствует;

(vi) на любом двоичном наборе $\tilde{\pi}$ длины n , не принадлежащем множеству $M \cup \{(\tilde{0}^n), (\tilde{0}^{n-1}, 1), (\tilde{1}^{n-1}, 0), (\tilde{1}^n)\}$, в схеме S_M есть проводимость либо между полюсами из каждой из пар (a_0, a_m) , (a_0, b_m) , либо между полюсами из каждой из пар (b_0, a_m) , (b_0, b_m) .

Доказательство. Пусть $\tilde{\alpha} = (\alpha_1, \dots, \alpha_{n-1})$, а i и j — такие индексы от 1 до $n-1$, что $\alpha_i = 1$ и $\alpha_j = 0$. По лемме 4 существует $L_{(n)}$ -схема $S_{\tilde{\alpha}}$, составленная из $2n-5$ $L_{(n)}$ -блоков, содержащая только контакты переменных из множества $\{x_1, \dots, x_{n-1}\}$ и обладающая свойствами (i)–(iii). Пусть $\tilde{\pi} = (\tau_1, \dots, \tau_n)$ (в формулировке свойства (vi)) и $\tilde{\tau} = (\tau_1, \dots, \tau_{n-1})$.

Тогда

$$\tilde{\tau} \notin \{(\tilde{0}^{n-1}), (\tilde{1}^{n-1})\}. \quad (5)$$

Рассмотрим два случая.

1. Пусть $M = \{\tilde{\sigma}_0, \tilde{\sigma}_1\}$. Определим $L_{(n)}$ -схему S_M следующим образом: полюса a_0 и b_0 схемы S_M совпадают с полюсами соответственно a_0 и b_0 схемы $S_{\tilde{\alpha}}$; полюса a_{2n-5} и b_{2n-5} схемы $S_{\tilde{\alpha}}$ совпадают с полюсами соответственно A_1 и A_2 $L_{(n)}$ -блока B_m вида $B_{i,j}^{i,j}$, где $m = 2n - 4$; полюса a_m и b_m схемы S_M совпадают с полюсами соответственно A_3 и A_4 блока B_m (см. рис. 7).

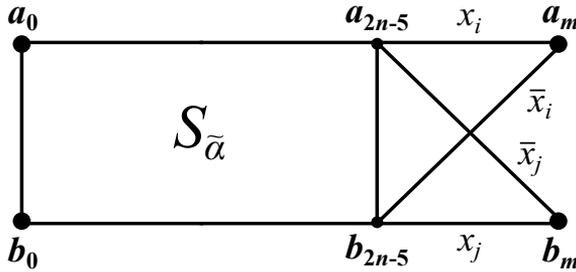


Рис. 7. Схема S_M в случае 1

Предположим, что свойство (v) не выполнено, т. е. в схеме S_M есть несамопересекающаяся цепь C между её полюсами из какой-то из пар (a_0, a_m) , (a_0, b_m) , (b_0, a_m) , (b_0, b_m) , проводящая на наборе $\tilde{\sigma}_\beta$ для некоторого $\beta \in \{0, 1\}$. Пусть $v \in \{a_0, b_0\}$ — один из концов этой цепи. Очевидно, что в ней можно выделить максимальный по длине участок, начинающийся с вершины v , содержащийся целиком в подсхеме $S_{\tilde{\alpha}}$ и проходящий через какую-то вершину $v' \in \{a_{2n-5}, b_{2n-5}\}$. Из свойства (i) схемы $S_{\tilde{\alpha}}$ и того, что первые $n - 1$ компонент наборов $\tilde{\sigma}_\beta$ и $\tilde{\alpha}$ совпадают, вытекает, что обязательно $v = b_0$, $v' = b_{2n-5}$. Вершина v' в силу максимальной выделенного участка инцидентна в цепи C некоторому контакту, не лежащему в подсхеме $S_{\tilde{\alpha}}$, а значит, принадлежащему блоку B_m . Это один из контактов $[b_{2n-5}, a_m]$, $[b_{2n-5}, b_m]$, т. е. один из контактов \bar{x}_i , x_j . Но ни один из них не проводит на наборе $\tilde{\sigma}_\beta$, поскольку $\alpha_i = 1$ и $\alpha_j = 0$; противоречие. Свойство (v) доказано.

Докажем свойство (vi). Заметим, что $\tilde{\tau} \notin \{\tilde{\alpha}, (\tilde{0}^{n-1}), (\tilde{1}^{n-1})\}$ в силу (5) и соотношения $\tilde{\pi} \notin M$. Отсюда, из свойства (iii) схемы $S_{\tilde{\alpha}}$ и того, что первые $n - 1$ компонент наборов $\tilde{\pi}$ и $\tilde{\tau}$ совпадают, следует, что в этой

схеме есть проводимость на наборе $\tilde{\pi}$ между полюсами из каждой из пар $(w, a_{2n-5}), (w, b_{2n-5})$ для некоторого $w \in \{a_0, b_0\}$. В силу определения блока \mathbf{B}_m вершина a_m соединена с вершинами a_{2n-5} и b_{2n-5} контактами x_i и \bar{x}_i соответственно, один из которых проводит на наборе $\tilde{\pi}$; вершина b_m соединена с вершинами a_{2n-5} и b_{2n-5} контактами \bar{x}_j и x_j соответственно, один из которых проводит на наборе $\tilde{\pi}$. Поэтому на указанном наборе есть проводимость между вершиной w и каждой из вершин a_m, b_m . Свойство (vi) доказано.

2. Пусть $M = \{\tilde{\sigma}_\beta\}$ для некоторого $\beta \in \{0, 1\}$. Определим $L_{(n)}$ -схему S_M следующим образом: полюса a_0 и b_0 схемы S_M совпадают с полюсами соответственно a_0 и b_0 схемы $S_{\bar{\alpha}}$; полюса a_{2n-5} и b_{2n-5} схемы $S_{\bar{\alpha}}$ совпадают с полюсами соответственно A_1 и A_2 $L_{(n)}$ -блока \mathbf{B}_{m-1} вида $B_{n,n}^{n,n}$, где $m = 2n - 3$, и объявляются вершинами соответственно a_{m-1} и b_{m-1} схемы S_M ; полюса A_3 и A_4 блока \mathbf{B}_{m-1} совпадают с полюсами соответственно A_1 и A_2 $L_{(n)}$ -блока \mathbf{B}_m вида

$$\begin{cases} B_{i,j}^{i,j}, & \text{если } \beta = 1, \\ B_{j,i}^{j,i}, & \text{если } \beta = 0; \end{cases}$$

полюса a_m и b_m схемы S_M совпадают с полюсами соответственно A_3 и A_4 блока \mathbf{B}_m (вид этой схемы при $\beta = 1$ показан на рис. 8).

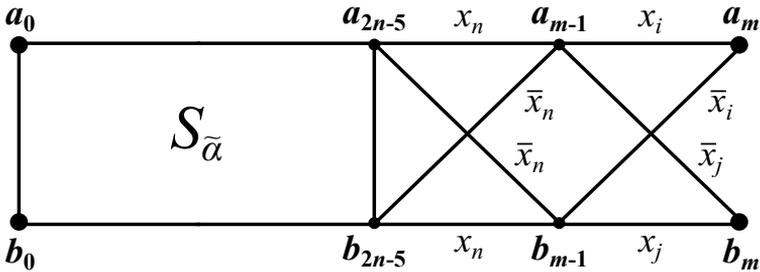


Рис. 8. Схема S_M в случае 2

Предположим, что свойство (v) не выполнено, т. е. в схеме S_M есть несамопересекающаяся цепь C между её полюсами из какой-то из пар $(a_0, a_m), (a_0, b_m), (b_0, a_m), (b_0, b_m)$, проводящая на наборе $\tilde{\sigma}_\beta$. Пусть $v \in \{a_0, b_0\}$ — один из концов этой цепи. Очевидно, что в ней можно выделить максимальный по длине участок, начинающийся с вершины v , содержащийся целиком в подсхеме $S_{\bar{\alpha}}$ и проходящий через какую-то

вершину $v' \in \{a_{2n-5}, b_{2n-5}\}$. Из свойства (i) схемы $S_{\tilde{\alpha}}$ и того, что первые $n - 1$ компонент наборов $\tilde{\sigma}_\beta$ и $\tilde{\alpha}$ совпадают, вытекает, что обязательно $v = b_0$, $v' = b_{2n-5}$. Вершина v' в силу максимальности выделенного участка инцидентна в цепи C некоторому контакту K , не лежащему в подсхеме $S_{\tilde{\alpha}}$. Это один из контактов $[b_{2n-5}, a_{m-1}]$, $[b_{2n-5}, b_{m-1}]$, принадлежащий блоку \mathbf{B}_{m-1} , т. е. один из контактов \bar{x}_n, x_n . Из них на наборе $\tilde{\sigma}_\beta$ проводит только контакт x_n^β ; таким образом, K — это контакт x_n^β . Рассмотрим два подслучая.

2.1. Пусть $\beta = 1$. Тогда контакт K соединяет вершины b_{2n-5} и b_{m-1} цепи C . Вершина b_{m-1} инцидентна в ней ещё одному контакту. В силу строения схемы S_M это один из контактов $[b_{m-1}, a_{2n-5}]$, $[b_{m-1}, a_m]$, $[b_{m-1}, b_m]$, т. е. один из контактов $\bar{x}_n, \bar{x}_i, x_j$ (см. определения блоков \mathbf{B}_{m-1} и \mathbf{B}_m). Но ни один из них не проводит на наборе $\tilde{\sigma}_\beta = (\alpha_1, \dots, \alpha_{n-1}, \beta)$, поскольку $\beta = 1$, $\alpha_i = 1$ и $\alpha_j = 0$; противоречие.

2.2. Пусть $\beta = 0$. Тогда контакт K соединяет вершины b_{2n-5} и a_{m-1} цепи C . Вершина a_{m-1} инцидентна в ней ещё одному контакту. В силу строения схемы S_M это один из контактов $[a_{m-1}, a_{2n-5}]$, $[a_{m-1}, a_m]$, $[a_{m-1}, b_m]$, т. е. один из контактов x_n, x_j, \bar{x}_i (см. определения блоков \mathbf{B}_{m-1} и \mathbf{B}_m). Но ни один из них не проводит на наборе $\tilde{\sigma}_\beta = (\alpha_1, \dots, \alpha_{n-1}, \beta)$, поскольку $\beta = 0$, $\alpha_i = 1$ и $\alpha_j = 0$; противоречие. Свойство (v) доказано.

Докажем свойство (vi). Пусть вначале $\tilde{\pi} \neq \tilde{\sigma}_\beta$. Заметим, что $\tilde{\pi} \neq \tilde{\sigma}_\beta$, так как $\tilde{\pi} \notin M$. Тогда $\tilde{\tau} \notin \{\tilde{\alpha}, (\tilde{0}^{n-1}), (\tilde{1}^{n-1})\}$ в силу (5) и соотношения $\tilde{\pi} \notin \{\tilde{\sigma}_\beta, \tilde{\sigma}_{\bar{\beta}}\}$. Отсюда, из свойства (iii) схемы $S_{\tilde{\alpha}}$ и того, что первые $n - 1$ компонент наборов $\tilde{\pi}$ и $\tilde{\tau}$ совпадают, следует, что в этой схеме есть проводимость на наборе $\tilde{\pi}$ между полюсами из каждой из пар (w, a_{2n-5}) , (w, b_{2n-5}) для некоторого $w \in \{a_0, b_0\}$. По определению блока \mathbf{B}_{m-1} вершина a_{m-1} соединена с вершинами a_{2n-5} и b_{2n-5} контактами x_n и \bar{x}_n соответственно, один из которых проводит на наборе $\tilde{\pi}$; вершина b_{m-1} соединена с вершинами a_{2n-5} и b_{2n-5} контактами \bar{x}_n и x_n соответственно, один из которых проводит на наборе $\tilde{\pi}$. Поэтому на указанном наборе есть проводимость между вершиной w и каждой из вершин a_{m-1}, b_{m-1} . Далее, по определению блока \mathbf{B}_m вершина a_m соединена с вершинами a_{m-1} и b_{m-1} контактами соответственно x_i и \bar{x}_i в случае $\beta = 1$ и контактами соответственно x_j и \bar{x}_j в случае $\beta = 0$, один из которых проводит на наборе $\tilde{\pi}$; вершина b_m соединена с вершинами a_{m-1} и b_{m-1} контактами соответственно \bar{x}_j и x_j в случае $\beta = 1$ и контактами соответственно \bar{x}_i и x_i в случае $\beta = 0$, один из которых проводит на наборе $\tilde{\pi}$. Поэтому на

указанном наборе есть проводимость между вершиной w и каждой из вершин a_m, b_m , что и требовалось доказать.

Пусть теперь $\tilde{\pi} = \tilde{\sigma}_{\tilde{\beta}}$. Из свойства (ii) схемы $S_{\tilde{\alpha}}$ и того, что первые $n - 1$ компонент наборов $\tilde{\pi}$ и $\tilde{\alpha}$ совпадают, вытекает, что на наборе $\tilde{\pi}$ есть проводимость между полюсами b_0 и b_{2n-5} схемы $S_{\tilde{\alpha}}$. Рассмотрим два подслучая.

2.1. Пусть $\beta = 1$. Тогда $\tilde{\pi} = (\alpha_1, \dots, \alpha_{n-1}, 0)$. На наборе $\tilde{\pi}$ каждый из контактов $[b_{2n-5}, a_{m-1}]$, $[a_{m-1}, a_m]$ и $[a_{m-1}, b_m]$ схемы S_M проводит, так как это контакты \bar{x}_n, x_i и \bar{x}_j соответственно (см. определения блоков V_{m-1} и V_m). Следовательно, в данной схеме есть проводимость между полюсом b_0 и каждым из полюсов a_m, b_m , что и требовалось доказать.

2.2. Пусть $\beta = 0$. Тогда $\tilde{\pi} = (\alpha_1, \dots, \alpha_{n-1}, 1)$. На наборе $\tilde{\pi}$ каждый из контактов $[b_{2n-5}, b_{m-1}]$, $[b_{m-1}, a_m]$ и $[b_{m-1}, b_m]$ схемы S_M проводит, так как это контакты x_n, \bar{x}_j и x_i соответственно (см. определения блоков V_{m-1} и V_m). Следовательно, в данной схеме есть проводимость между полюсом b_0 и каждым из полюсов a_m, b_m . Свойство (vi), а вместе с ним лемма 5 доказаны. \square

Сложность построенной схемы S_M , как видно из рис. 7 и 8, не более чем на 8 превышает сложность схемы $S_{\tilde{\alpha}}$, т. е. не превосходит $8n - 12$.

Лемма 6. *Для любой булевой функции $f(\tilde{x}^n)$, $n \geq 3$, существует такая $L_{(n)}$ -схема S , составленная из чётного числа t $L_{(n)}$ -блоков, среди которых число блоков вида $B_{n,n}^{n,n}$ также чётно, что на любом двоичном наборе $\tilde{\tau}$ длины n , не принадлежащем множеству $M_0 = \{(\tilde{0}^n), (\tilde{0}^{n-1}, 1), (\tilde{1}^{n-1}, 0), (\tilde{1}^n)\}$, проводимости между полюсами b_0 и a_0 , b_0 и a_m , b_0 и b_m схемы S равны 0, $f(\tilde{\tau})$, $f(\tilde{\tau})$ соответственно.*

Доказательство. Построим сначала вспомогательную $L_{(n)}$ -схему S_0 . По определению она однозначно задаётся числом $m_0 \in \mathbb{N}$ и $L_{(n)}$ -блоками V_1, \dots, V_{m_0} . Положим $m_0 = 2n - 4$, $V_{2j-1} = B_{j,j}^{j,j}$, $V_{2j} = B_{j+1,j}^{j+1,j}$ для каждого $j = 1, \dots, n - 2$. Вид схемы S_0 показан на рис. 9.

Докажем свойство (vii) этой схемы: функция проводимости между её вершинами b_0 и b_{2j} тождественно равна 1 для любого $j \in \{1, \dots, n - 2\}$. Достаточно доказать, что функция проводимости между вершинами b_{2j-2} и b_{2j} в схеме S_0 тождественно равна 1 для любого $j \in \{1, \dots, n - 2\}$. Между этими вершинами в данной схеме есть, в частности, цепи $b_{2j-2} - b_{2j-1} - b_{2j}$ и $b_{2j-2} - a_{2j-1} - b_{2j}$. В силу определения блоков V_{2j-1} и V_{2j} первая из этих цепей содержит два контакта x_j , а вторая — два контакта \bar{x}_j . Таким образом, функция проводимости между вершинами

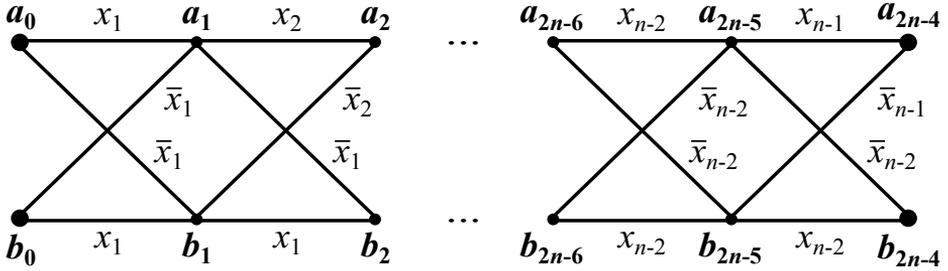


Рис. 9. Схема S_0

b_{2j-2} и b_{2j} в схеме S_0 не меньше $x_j \vee \bar{x}_j \equiv 1$, т. е. тождественно равна 1. Свойство (vii) доказано.

Докажем свойство (viii) схемы S_0 : на любом двоичном наборе $\tilde{\tau} = (\tau_1, \dots, \tau_n)$, не принадлежащем множеству M_0 , в этой схеме есть проводимость между полюсами b_0 и a_{2n-4} . Из соотношения $\tilde{\tau} \notin M_0$ следует, что не все из чисел $\tau_1, \dots, \tau_{n-1}$ равны между собой. Пусть $j \in \{1, \dots, n-2\}$ — максимальной такой индекс, что $\tau_j \neq \tau_{j+1}$. В силу свойства (vii) достаточно доказать, что в схеме S_0 на наборе $\tilde{\tau}$ есть проводимость между вершинами b_{2j-2} и a_{2j} , а также между вершинами a_{2j} и a_{2n-4} . Между вершинами b_{2j-2} и a_{2j} в данной схеме есть, в частности, цепи $b_{2j-2} - a_{2j-1} - a_{2j}$ и $b_{2j-2} - b_{2j-1} - a_{2j}$. В силу определения блоков B_{2j-1} и B_{2j} первая из этих цепей содержит по одному контакту \bar{x}_j и x_{j+1} , а вторая цепь — по одному контакту x_j и \bar{x}_{j+1} . Одна из них проводит на наборе $\tilde{\tau}$, так как $\tau_j \neq \tau_{j+1}$. Между вершинами a_{2j} и a_{2n-4} в схеме S также есть проводимость на наборе $\tilde{\tau}$. Действительно, при $j = n-2$ это очевидно; в случае $j \leq n-3$ в силу выбора числа j выполнено соотношение $\tau_{j+1} = \tau_{j+2} = \dots = \tau_{n-1}$, поэтому либо цепь $a_{2j} - a_{2j+1} - \dots - a_{2n-5} - a_{2n-4}$, состоящая из контактов $x_{j+1}, x_{j+2}, \dots, x_{n-1}$, либо цепь $a_{2j} - b_{2j+1} - a_{2j+2} - \dots - b_{2n-5} - a_{2n-4}$, состоящая из контактов $\bar{x}_{j+1}, \bar{x}_{j+2}, \dots, \bar{x}_{n-1}$, проводит на наборе $\tilde{\tau}$ (некоторые из этих контактов могут входить в одну из рассматриваемых цепей по два раза). Свойство (viii) доказано.

Разобьём все двоичные наборы длины n , кроме наборов из множества M_0 , на $2^{n-1} - 2$ пар наборов, различающихся только в последней компоненте. Пусть d — число таких пар, в каждой из которых хотя бы один набор является нулевым набором функции $f(\tilde{x}^n)$. Если $d = 0$, то положим $\hat{S} = S_0$ и $m = 2n - 4$. В случае же $d \geq 1$ обозначим подмножества

указанных d пар наборов, состоящие из всех нулевых наборов функции f , содержащихся в этих парах, через M_1, \dots, M_d (в произвольном порядке). Тогда $|M_i| \in \{1, 2\}$ для любого $i \in \{1, \dots, d\}$ и множество $M_1 \cup \dots \cup M_d$ совпадает со множеством всех нулевых наборов функции $f(\tilde{x}^n)$, не лежащих в множестве M_0 (при $d = 0$ последнее утверждение также верно, если положить $M_1 \cup \dots \cup M_d = \emptyset$). Для каждого $M \in \{M_1, \dots, M_d\}$ по лемме 5 построим $L_{(n)}$ -схему S_M , обладающую свойствами (v), (vi). Определим $L_{(n)}$ -схему \hat{S} следующим образом: полюса a_0 и b_0 схемы \hat{S} совпадают с полюсами соответственно a_0 и b_0 схемы S_0 ; полюса a_{2n-4} и b_{2n-4} схемы S_0 совпадают с полюсами соответственно a_0 и b_0 схемы S_{M_1} и для удобства объявляются вершинами соответственно a^1 и b^1 схемы \hat{S} ; для любого $i \in \{1, \dots, d-1\}$ (при $d \geq 2$) полюса a_{m_i} и b_{m_i} схемы S_{M_i} , где m_i — некоторое натуральное число, совпадают с полюсами соответственно a_0 и b_0 схемы $S_{M_{i+1}}$ и для удобства объявляются вершинами соответственно a^{i+1} и b^{i+1} схемы \hat{S} ; полюса a_m и b_m схемы \hat{S} совпадают с полюсами соответственно a_{m_d} и b_{m_d} схемы S_{M_d} , где m, m_d — некоторые натуральные числа, и для удобства объявляются вершинами соответственно a^{d+1} и b^{d+1} схемы \hat{S} . Вид схемы \hat{S} показан на рис. 10.

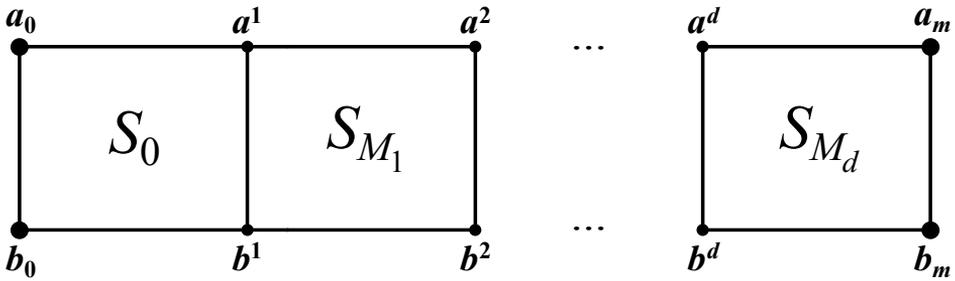


Рис. 10. Схема \hat{S}

Определим теперь $L_{(n)}$ -схему S . Рассмотрим четыре случая.

Случай А. Схема \hat{S} составлена из чётного числа $L_{(n)}$ -блоков, среди которых число блоков вида $B_{n,n}^{n,n}$ также чётно. Тогда положим $S = \hat{S}$.

Случай Б. Схема \hat{S} составлена из нечётного числа $L_{(n)}$ -блоков, среди которых число блоков вида $B_{n,n}^{n,n}$ чётно. Определим схему S следующим образом: полюса a_0 и b_0 схемы S совпадают с полюсами соответственно a_0 и b_0 схемы \hat{S} ; полюса a_m и b_m схемы S совпадают с полюсами соответ-

ственно A_1 и A_2 $L_{(n)}$ -блока \mathbf{B}_{m+1} вида $B_{1,1}^{1,1}$; полюса a_{m+1} и b_{m+1} схемы S совпадают с полюсами соответственно A_3 и A_4 блока \mathbf{B}_{m+1} (см. рис. 11).

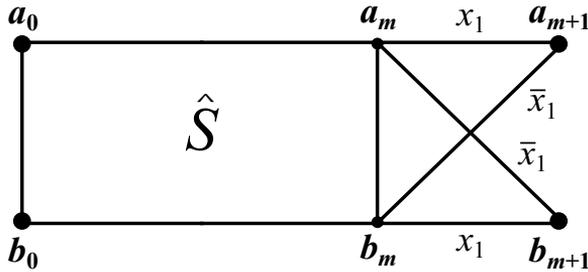


Рис. 11. Схема S в случае Б

Случай В. Схема \hat{S} составлена из нечётного числа $L_{(n)}$ -блоков, среди которых число блоков вида $B_{n,n}^{n,n}$ нечётно. Определим схему S следующим образом: полюса a_0 и b_0 схемы S совпадают с полюсами соответственно a_0 и b_0 схемы \hat{S} ; полюса a_m и b_m схемы \hat{S} совпадают с полюсами соответственно A_1 и A_2 $L_{(n)}$ -блока \mathbf{B}_{m+1} вида $B_{n,n}^{n,n}$; полюса a_{m+1} и b_{m+1} схемы S совпадают с полюсами соответственно A_3 и A_4 блока \mathbf{B}_{m+1} (см. рис. 11; все контакты переменной x_1 в правом блоке надо заменить на соответствующие контакты переменной x_n).

Случай Г. Схема \hat{S} составлена из чётного числа $L_{(n)}$ -блоков, среди которых число блоков вида $B_{n,n}^{n,n}$ нечётно. Определим схему S следующим образом: полюса a_0 и b_0 схемы S совпадают с полюсами соответственно a_0 и b_0 схемы \hat{S} ; полюса a_m и b_m схемы \hat{S} совпадают с полюсами соответственно A_1 и A_2 $L_{(n)}$ -блока \mathbf{B}_{m+1} вида $B_{1,1}^{1,1}$; полюса A_3 и A_4 блока \mathbf{B}_{m+1} совпадают с полюсами соответственно A_1 и A_2 $L_{(n)}$ -блока \mathbf{B}_{m+2} вида $B_{n,n}^{n,n}$ и объявляются вершинами соответственно a_{m+1} и b_{m+1} схемы S ; полюса a_{m+2} и b_{m+2} схемы S совпадают с полюсами соответственно A_3 и A_4 блока \mathbf{B}_{m+2} (см. рис. 12).

Легко видеть, что в каждом из случаев А–Г схема S является $L_{(n)}$ -схемой и составлена из чётного числа $L_{(n)}$ -блоков, среди которых число блоков вида $B_{n,n}^{n,n}$ также чётно.

Далее будем параллельно рассматривать случаи А–Г. Пусть $\tilde{\tau}$ — произвольный двоичный набор длины n , не принадлежащий множеству M_0 . Докажем сначала, что проводимость между полюсами b_0 и a_0 схемы S на этом наборе равна 0, т. е. отсутствует. Обозначим произвольную несамопересекающуюся цепь в схеме S между этими полюсами через C , а вер-

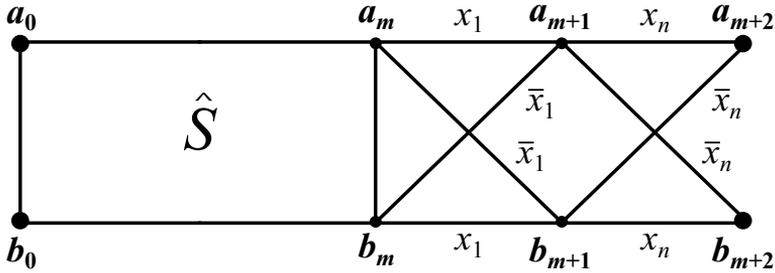


Рис. 12. Схема S в случае Γ

шины этой цепи при движении от a_0 к b_0 — через v_0, \dots, v_s , где $v_0 = a_0$, $v_s = b_0$. Достаточно доказать, что данная цепь не проводит на наборе $\tilde{\tau}$. Рассмотрим два случая.

1. Цепь C целиком содержится в подсхеме S_0 . Пусть $t \in \{0, \dots, 2n - 4\}$ — максимальное такое число, что среди вершин v_0, \dots, v_s есть хотя бы одна вершина $v_{s'}$, принадлежащая множеству $\{a_t, b_t\}$, где a_t, b_t — вершины $L_{(n)}$ -схемы S_0 . Очевидно, что $t \geq 1$, поэтому $0 < s' < s$. Вершина $v_{s'}$ соединена в схеме S_0 контактами с вершинами $a_{t-1}, b_{t-1}, a_{t+1}$ и b_{t+1} , если $t \leq 2n - 5$, и с вершинами a_{t-1} и b_{t-1} , если $t = 2n - 4$. Отсюда и из выбора числа t следует соотношение $v_{s'-1}, v_{s'+1} \in \{a_{t-1}, b_{t-1}\}$; кроме того, $v_{s'-1} \neq v_{s'+1}$. Поэтому в цепи C обязательно одновременно содержатся либо контакты $[a_{t-1}, a_t]$ и $[b_{t-1}, a_t]$, либо контакты $[a_{t-1}, b_t]$ и $[b_{t-1}, b_t]$. В силу определения блоков B_{2j-1} и B_{2j} схемы S_0 , где $j = 1, \dots, n - 2$, это либо контакты x_j и \bar{x}_j , либо контакты x_{j+1} и \bar{x}_{j+1} для некоторого $j \in \{1, \dots, n - 2\}$, т. е. противоположные контакты. Следовательно, данная цепь не может проводить на наборе $\tilde{\tau}$.

2. Цепь C не содержится целиком в подсхеме S_0 . Из вида этой подсхемы легко следует, что цепь C можно разбить на участок C_a , соединяющий вершину a_0 с какой-то вершиной w , не содержащейся в S_0 , и участок C_b , соединяющий вершины w и b_0 ; для любого $t' \in \{0, \dots, 2n - 4\}$ на участке C_a (C_b) обязательно содержится вершина $w_{t'}^a$ (соответственно, $w_{t'}^b$), принадлежащая множеству $\{a_{t'}, b_{t'}\}$; при этом $w_{t'}^a \neq w_{t'}^b$, так как цепь C несамопересекающаяся. Отсюда вытекает, что $s > 2(2n - 3)$, $v_{t'} = w_{t'}^a$ и $v_{s-t'} = w_{t'}^b$ для любого $t' \in \{0, \dots, 2n - 4\}$ (последние два равенства можно доказать индукцией по t'); таким образом, $v_{t'}, v_{s-t'} \in \{a_{t'}, b_{t'}\}$ и $v_{t'} \neq v_{s-t'}$. Рассмотрим пять подслучаев.

2.1. Пусть $v_{t'} = a_{t'}$ для любого $t' \in \{0, \dots, 2n - 4\}$. Тогда в цепи C содержатся контакты $[a_0, a_1], [a_1, a_2], \dots, [a_{2n-5}, a_{2n-4}]$. В силу определения блоков B_{2j-1} и B_{2j} схемы S_0 , где $j = 1, \dots, n - 2$, это контакты x_1, x_2, \dots, x_{n-1} (некоторые из этих контактов при $n \geq 4$ повторяются). Хотя бы одна из первых $n - 1$ компонент набора $\tilde{\tau}$ равна 0, так как $\tilde{\tau} \notin M_0$. Поэтому цепь C не может проводить на данном наборе.

2.2. Пусть $v_{t'} = a_{t'}$ для любого чётного $t' \in \{0, \dots, 2n - 4\}$ и $v_{t'} = b_{t'}$ для любого нечётного $t' \in \{0, \dots, 2n - 4\}$. Тогда в цепи C содержатся контакты $[a_0, b_1], [b_1, a_2], \dots, [b_{2n-5}, a_{2n-4}]$. В силу определения блоков B_{2j-1} и B_{2j} схемы S_0 , где $j = 1, \dots, n - 2$, это контакты $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_{n-1}$ (некоторые из этих контактов при $n \geq 4$ повторяются). Хотя бы одна из первых $n - 1$ компонент набора $\tilde{\tau}$ равна 1, так как $\tilde{\tau} \notin M_0$. Поэтому цепь C не может проводить на данном наборе.

2.3. Пусть существует такое $t' \in \{0, \dots, 2n - 6\}$, что $v_{t'} = a_{t'}$, $v_{t'+1} = a_{t'+1}$ и $v_{t'+2} = b_{t'+2}$. Тогда в цепи C содержатся контакты $[a_{t'}, a_{t'+1}]$ и $[a_{t'+1}, b_{t'+2}]$. В силу определения блоков B_{2j-1} и B_{2j} схемы S_0 , где $j = 1, \dots, n - 2$, это либо контакты x_j и \bar{x}_j соответственно, либо контакты x_{j+1} и \bar{x}_{j+1} соответственно для некоторого $j \in \{1, \dots, n - 2\}$, т. е. противоположные контакты. Поэтому данная цепь не может проводить на наборе $\tilde{\tau}$.

2.4. Пусть существует такое $t' \in \{0, \dots, 2n - 6\}$, что $v_{t'} = a_{t'}$, $v_{t'+1} = b_{t'+1}$ и $v_{t'+2} = b_{t'+2}$. Тогда $v_{s-t'} = b_{t'}$, $v_{s-t'-1} = a_{t'+1}$ и $v_{s-t'-2} = a_{t'+2}$, поэтому в цепи C содержатся контакты $[a_{t'}, b_{t'+1}]$, $[b_{t'+1}, b_{t'+2}]$, $[b_{t'}, a_{t'+1}]$ и $[a_{t'+1}, a_{t'+2}]$. В силу определения блоков B_{2j-1} и B_{2j} схемы S_0 , где $j = 1, \dots, n - 2$, это либо контакты \bar{x}_j , x_j , \bar{x}_j и x_{j+1} соответственно, либо контакты \bar{x}_j , x_{j+1} , \bar{x}_{j+1} и x_{j+1} соответственно для некоторого $j \in \{1, \dots, n - 2\}$. Среди них есть противоположные контакты, поэтому данная цепь не может проводить на наборе $\tilde{\tau}$.

2.5. Пусть существует такое $t' \in \{0, \dots, 2n - 6\}$, что $v_{t'} = b_{t'}$, $v_{t'+1} = a_{t'+1}$ и $v_{t'+2} = a_{t'+2}$. Тогда $v_{s-t'} = a_{t'}$, $v_{s-t'-1} = b_{t'+1}$ и $v_{s-t'-2} = b_{t'+2}$, значит, в цепи C содержатся контакты $[b_{t'}, a_{t'+1}]$, $[a_{t'+1}, a_{t'+2}]$, $[a_{t'}, b_{t'+1}]$ и $[b_{t'+1}, b_{t'+2}]$. Этот подслучай сводится к предыдущему.

Нетрудно заметить, что подслучаи 2.1–2.5 охватывают все возможные подслучаи случая 2. Тем самым доказано, что проводимость между полюсами b_0 и a_0 схемы S на наборе $\tilde{\tau}$ равна 0.

Обозначим через m' число $L_{(n)}$ -блоков в схеме S (в силу построения этой схемы $m' \in \{m, m + 1, m + 2\}$). Докажем, что проводимости между полюсами b_0 и $a_{m'}$, а также между полюсами b_0 и $b_{m'}$ схемы S на наборе $\tilde{\tau}$ равны $f(\tilde{\tau})$. Рассмотрим два случая.

1'. Пусть $f(\tilde{\tau}) = 0$. Тогда $d \geq 1$ и $\tilde{\tau} \in M_i$ для некоторого $i \in \{1, \dots, d\}$. Предположим, что на наборе $\tilde{\tau}$ в схеме S есть несамопересекающаяся проводящая цепь между полюсами b_0 и v для некоторого $v \in \{a_{m'}, b_{m'}\}$. Очевидно, что в указанной цепи можно выбрать участок, соединяющий одну из вершин a^i, b^i с одной из вершин a^{i+1}, b^{i+1} и лежащий целиком внутри подсхемы S_{M_i} , однако это противоречит выполнению свойства (v) для схемы S_{M_i} с учётом того, что вершины a^i, b^i, a^{i+1} и b^{i+1} совпадают с полюсами a_0, b_0, a_{m_i} и b_{m_i} данной схемы соответственно. Поэтому проводимости между полюсами b_0 и $a_{m'}$, а также между полюсами b_0 и $b_{m'}$ схемы S на наборе $\tilde{\tau}$ равны $0 = f(\tilde{\tau})$, что и требовалось доказать.

2'. Пусть $f(\tilde{\tau}) = 1$. Докажем свойство (ix) схемы \hat{S} : в этой схеме на наборе $\tilde{\tau}$ есть проводимость между полюсами b_0 и a_m , а также между полюсами b_0 и b_m . В силу свойств (vii), (viii) в подсхеме S_0 есть проводимость между полюсами b_0 и b_{2n-4} , а также между полюсами b_0 и a_{2n-4} . Если $d = 0$, то $\hat{S} = S_0$ и $m = 2n - 4$, откуда следует требуемое утверждение. В случае $d \geq 1$ имеем $\tilde{\tau} \notin M_1 \cup \dots \cup M_d$. В силу свойства (vi) в подсхеме S_{M_d} есть проводимость между её полюсами v^d и a_m , а также между её полюсами v^d и b_m для некоторого $v^d \in \{a^d, b^d\}$. В случае $d \geq 2$ в силу свойства (vi) в подсхеме $S_{M_{d-1}}$ есть проводимость между её полюсами v^{d-1} и v^d для некоторого $v^{d-1} \in \{a^{d-1}, b^{d-1}\}$. В случае $d \geq 3$ в силу свойства (vi) в подсхеме $S_{M_{d-2}}$ есть проводимость между её полюсами v^{d-2} и v^{d-1} для некоторого $v^{d-2} \in \{a^{d-2}, b^{d-2}\}$, и т. д. В итоге получаем, что в схеме \hat{S} есть проводимость между вершинами v^1 и a_m , а также между вершинами v^1 и b_m для некоторого $v^1 \in \{a^1, b^1\} = \{a_{2n-4}, b_{2n-4}\}$. Выше было показано, что в подсхеме S_0 есть проводимость между полюсами b_0 и v^1 . Таким образом, в схеме \hat{S} есть проводимость между полюсами b_0 и a_m , а также между полюсами b_0 и b_m . Свойство (ix) доказано.

В случае А в силу равенства $S = \hat{S}$ получаем, что проводимости между полюсами b_0 и $a_{m'}$, а также между полюсами b_0 и $b_{m'}$ схемы S на наборе $\tilde{\tau}$ равны $1 = f(\tilde{\tau})$, что и требовалось доказать.

В случае Б в силу определения блока B_{m+1} вершина a_{m+1} соединена в схеме S с вершинами a_m и b_m контактами x_1 и \bar{x}_1 соответственно, один из которых проводит на наборе $\tilde{\tau}$; вершина b_{m+1} соединена с вершинами a_m и b_m контактами \bar{x}_1 и x_1 соответственно, один из которых проводит на наборе $\tilde{\tau}$. С учётом свойства (ix) в схеме S на указанном наборе проводимость между вершиной b_0 и каждым из полюсов a_{m+1}, b_{m+1} равна $1 = f(\tilde{\tau})$, что и требовалось доказать.

В случае В требуемое утверждение доказывается аналогично случаю Б с заменой контактов x_1 и \bar{x}_1 на контакты x_n и \bar{x}_n соответственно.

В случае Γ по аналогии со случаем B устанавливается, что в схеме S на наборе $\tilde{\tau}$ есть проводимость между вершиной b_0 и каждой из вершин a_{m+1}, b_{m+1} . В силу определения блока B_{m+2} вершина a_{m+2} соединена в этой схеме с вершинами a_{m+1} и b_{m+1} контактами x_n и \bar{x}_n соответственно, один из которых проводит на наборе $\tilde{\tau}$; вершина b_{m+2} соединена с вершинами a_{m+1} и b_{m+1} контактами \bar{x}_n и x_n соответственно, один из которых проводит на наборе $\tilde{\tau}$. Поэтому в схеме S на указанном наборе проводимость между вершиной b_0 и каждым из полюсов a_{m+2}, b_{m+2} равна $1 = f(\tilde{\tau})$, что и требовалось доказать.

Во всех случаях доказано, что проводимости между полюсами b_0 и a_m , а также между полюсами b_0 и b_m схемы S на наборе $\tilde{\tau}$ равны $f(\tilde{\tau})$. Лемма 6 доказана. \square

Оценим сверху сложности схем, построенных в ходе доказательства леммы 6. Сложность схемы S_0 равна $4(2n - 4) = 8n - 16$. Сложность каждой из схем S_{M_1}, \dots, S_{M_d} (при $d \geq 1$) не превосходит $8n - 12$. Из определения числа d следует, что $d \leq 2^{n-1} - 2$. Поэтому сложность схемы \hat{S} не превосходит

$$8n - 16 + d(8n - 12) \leq 8n - 16 + (2^{n-1} - 2)(8n - 12) = (4n - 6) \cdot 2^n - 8n + 8$$

(см. рис. 10). Наконец, сложность схемы S не более чем на 8 превышает сложность схемы \hat{S} (см. разбор случаев A – Γ и рис. 11, 12), т. е. не превосходит $(4n - 6) \cdot 2^n - 8n + 16$.

Лемма 7. *Любую булеву функцию $f(\tilde{x}^n)$, $n \geq 3$, удовлетворяющую условиям $f(\tilde{0}^n) = f(\tilde{1}^n) = 1$, $f(\tilde{0}^{n-1}, 1) = f(\tilde{1}^{n-1}, 0) = 0$, можно реализовать $L'_{(n)}$ -схемой.*

Доказательство. В силу леммы 6 существует такая $L_{(n)}$ -схема S , составленная из чётного числа m $L_{(n)}$ -блоков, среди которых число блоков вида $B_{n,n}^{n,n}$ также чётно, что на любом двоичном наборе $\tilde{\tau}$ длины n , не принадлежащем множеству $M_0 = \{(\tilde{0}^n), (\tilde{0}^{n-1}, 1), (\tilde{1}^{n-1}, 0), (\tilde{1}^n)\}$, проводимости между полюсами b_0 и a_0 , b_0 и a_m , b_0 и b_m схемы S равны 0, $f(\tilde{\tau})$, $f(\tilde{\tau})$ соответственно. Пусть S' — контактная схема с полюсами b_0 и a_m , получающаяся из схемы S добавлением вершины c_1 и соединением её с полюсами b_m и a_0 схемы S контактами x_1 и x_n соответственно, а также добавлением вершины c_2 и соединением её с полюсами b_m и a_0 схемы S контактами \bar{x}_1 и \bar{x}_n соответственно (см. рис. 3). Тогда по определению S' является $L'_{(n)}$ -схемой.

Докажем, что схема S' реализует функцию $f(\tilde{x}^n)$. Для этого достаточно доказать, что функция проводимости $h(\tilde{x}^n)$ данной схемы на произвольном двоичном наборе $\tilde{\sigma} = (\sigma_1, \dots, \sigma_n)$ принимает значение $f(\tilde{\sigma})$. Рассмотрим четыре случая.

1. Пусть $f(\tilde{\sigma}) = 1$ и $\tilde{\sigma} \notin M_0$. Тогда проводимость между полюсами b_0 и a_m схемы S на наборе $\tilde{\sigma}$ равна $f(\tilde{\sigma}) = 1$. Следовательно, в подсхеме S , а значит, и в схеме S' есть проводящая на этом наборе цепь между полюсами b_0 и a_m , откуда

$$h(\tilde{\sigma}) = 1 = f(\tilde{\sigma}).$$

2. Пусть $f(\tilde{\sigma}) = 0$ и $\tilde{\sigma} \notin M_0$. Тогда проводимости между полюсами b_0 и a_0 , b_0 и a_m , b_0 и b_m схемы S на наборе $\tilde{\sigma}$ равны 0, $f(\tilde{\sigma}) = 0$, $f(\tilde{\sigma}) = 0$ соответственно, т. е. в подсхеме S нет проводящей на этом наборе цепи ни между какой из пар вершин b_0 и a_0 , b_0 и a_m , b_0 и b_m . Добавление к схеме S контактов $[a_0, c_1]$, $[c_1, b_m]$, $[a_0, c_2]$ и $[c_2, b_m]$ для получения из неё схемы S' никак не повлияет на это свойство. Следовательно, в схеме S' нет ни одной проводящей на наборе $\tilde{\sigma}$ цепи между её полюсами b_0 и a_m , откуда

$$h(\tilde{\sigma}) = 0 = f(\tilde{\sigma}).$$

3. Пусть $f(\tilde{\sigma}) = 1$ и $\tilde{\sigma} \in M_0$. Тогда $\tilde{\sigma} \in \{(\tilde{0}^n), (\tilde{1}^n)\}$ и в силу леммы 3 схема S' проводит на наборе $\tilde{\sigma}$, откуда

$$h(\tilde{\sigma}) = 1 = f(\tilde{\sigma}).$$

4. Пусть $f(\tilde{\sigma}) = 0$ и $\tilde{\sigma} \in M_0$. Тогда $\tilde{\sigma} \in \{(\tilde{0}^{n-1}, 1), (\tilde{1}^{n-1}, 0)\}$ и в силу леммы 3 схема S' не проводит на наборе $\tilde{\sigma}$, откуда

$$h(\tilde{\sigma}) = 0 = f(\tilde{\sigma}).$$

Лемма 7 доказана. □

Сложность построенной схемы S' на 4 превышает сложность схемы S , а значит, не превосходит $(4n - 6) \cdot 2^n - 8n + 20 < 4n \cdot 2^n$ (напомним, что $n \geq 3$).

6. Основные теоремы

В теореме 1 описаны все булевы функции f , для которых $D(f) = 0$, $D(f) = 1$ (таких нет), $D(f) = 2$ и $D(f) = 3$. Теорема 2 даёт описание достаточно обширного класса булевых функций f , для которых $D(f) = 4$.

Теорема 2. Пусть для булевой функции $f(\tilde{x}^n)$, $n \geq 3$, существует такой индекс $i \in \{1, \dots, n\}$ и такие булевы константы $\sigma_1, \dots, \sigma_n$, что

$$f(\sigma_1, \dots, \sigma_n) = f(\bar{\sigma}_1, \dots, \bar{\sigma}_n) = 1, \quad (6)$$

$$f(\sigma_1, \dots, \bar{\sigma}_{i-1}, \bar{\sigma}_i, \sigma_{i+1}, \dots, \sigma_n) = f(\bar{\sigma}_1, \dots, \bar{\sigma}_{i-1}, \sigma_i, \bar{\sigma}_{i+1}, \dots, \bar{\sigma}_n) = 0. \quad (7)$$

Тогда $D(f) = 4$.

Доказательство. Докажем неравенство $D(f) \leq 4$. Рассмотрим функцию $f'(\tilde{x}^n) = f(x_1^{\sigma_1}, \dots, x_n^{\sigma_n})$. Тогда $f(\tilde{x}^n) = f'(x_1^{\sigma_1}, \dots, x_n^{\sigma_n})$ и функция $f(\tilde{x}^n)$ родственна функции $f'(\tilde{x}^n)$. В силу леммы 1 достаточно доказать неравенство $D(f') \leq 4$. Рассмотрим теперь функцию $f''(\tilde{x}^n) = f'(x_1, \dots, x_{i-1}, x_n, x_{i+1}, \dots, x_{n-1}, x_i)$, получающуюся из функции f' перестановкой переменных x_i и x_n (в случае $i = n$ полагаем $f'' = f'$). Тогда $f'(\tilde{x}^n) = f''(x_1, \dots, x_{i-1}, x_n, x_{i+1}, \dots, x_{n-1}, x_i)$ и функция $f'(\tilde{x}^n)$ родственна функции $f''(\tilde{x}^n)$. В силу леммы 1 достаточно доказать неравенство $D(f'') \leq 4$. Заметим, что

$$f''(\tilde{0}^n) = f'(\tilde{0}^n) = f(\bar{\sigma}_1, \dots, \bar{\sigma}_n) = 1,$$

$$f''(\tilde{1}^n) = f'(\tilde{1}^n) = f(\sigma_1, \dots, \sigma_n) = 1,$$

$$f''(\tilde{0}^{n-1}, 1) = f'(0^{i-1}, 1, 0^{n-i}) = f(\bar{\sigma}_1, \dots, \bar{\sigma}_{i-1}, \sigma_i, \bar{\sigma}_{i+1}, \dots, \bar{\sigma}_n) = 0,$$

$$f''(\tilde{1}^{n-1}, 0) = f'(1^{i-1}, 0, 1^{n-i}) = f(\sigma_1, \dots, \sigma_{i-1}, \bar{\sigma}_i, \sigma_{i+1}, \dots, \sigma_n) = 0,$$

а в таком случае требуемое неравенство следует из леммы 7, применяемой для функции $f''(\tilde{x}^n)$, и леммы 3.

Докажем теперь, что $D(f) \geq 4$. Из (6), (7) следуют соотношения

$$f(\sigma_1, \dots, \sigma_n) \neq f(\sigma_1, \dots, \sigma_{i-1}, \bar{\sigma}_i, \sigma_{i+1}, \dots, \sigma_n),$$

$$f(\sigma_1, \dots, \sigma_n) \neq f(\bar{\sigma}_1, \dots, \bar{\sigma}_{i-1}, \sigma_i, \bar{\sigma}_{i+1}, \dots, \bar{\sigma}_n),$$

откуда вытекает, что функция f существенно зависит от переменной x_i и хотя бы от одной из переменных из множества $\{x_1, \dots, x_n\} \setminus \{x_i\}$. Предположим, что $D(f) \leq 3$. Тогда в силу теоремы 1 и предыдущего предложения функция f существенно зависит ровно от двух переменных: x_i и x_j для некоторого $j \in \{1, \dots, n\} \setminus \{i\}$ и родственна одной из функций $x_1 x_2$, $x_1 \vee x_2$. Поэтому существует такая булева функция $\varphi(x, y)$, что $f(\tilde{x}^n) = \varphi(x_i, x_j)$. Тогда из (6), (7) получаем

$$\varphi(\sigma_i, \sigma_j) = \varphi(\bar{\sigma}_i, \bar{\sigma}_j) = 1,$$

$$\varphi(\sigma_i, \bar{\sigma}_j) = \varphi(\bar{\sigma}_i, \sigma_j) = 0.$$

Для любых $\sigma_i, \sigma_j \in \{0, 1\}$ из последних двух соотношений следует, что $\varphi(x, y) \in \{x \oplus y, x \sim y\}$, поэтому $f(\tilde{x}^n) \in \{x_i \oplus x_j, x_i \sim x_j\}$. Но ни одна из функций $x_i \oplus x_j, x_i \sim x_j$ не родственна ни одной из функций $x_1 x_2, x_1 \vee x_2$; противоречие. Таким образом, $D(f) \geq 4$, а с учётом ранее установленного неравенства $D(f) \leq 4$ получаем равенство $D(f) = 4$. Теорема 2 доказана. \square

Из доказательства неравенства $D(f'') \leq 4$ в теореме 2, верхней оценки сложности схемы S' , приведённой в конце предыдущего раздела, и перехода от схемы S_1 к схеме S_2 в доказательстве леммы 1 легко вытекает, что любую булеву функцию $f(\tilde{x}^n)$, удовлетворяющую условиям теоремы 2, можно реализовать неизбыточной контактной схемой сложности менее $4n \cdot 2^n$, допускающей ЕПТ длины 4.

Теорема 3. *Для почти всех булевых функций f от n переменных справедливо равенство $D(f) = 4$.*

Доказательство. Пусть $n \geq 3$. Нетрудно видеть, что множество всех двоичных наборов длины n можно разбить на 2^{n-2} попарно непересекающихся упорядоченных четвёрок наборов

$$U_{\sigma_2, \dots, \sigma_{n-1}} = ((1, \sigma_2, \dots, \sigma_{n-1}, 1), (1, \sigma_2, \dots, \sigma_{n-1}, 0), \\ (0, \bar{\sigma}_2, \dots, \bar{\sigma}_{n-1}, 1), (0, \bar{\sigma}_2, \dots, \bar{\sigma}_{n-1}, 0)),$$

где $\sigma_2, \dots, \sigma_{n-1}$ — булевы константы, образующие все возможные комбинации. Пусть F_n — множество булевых функций от n переменных, не принимающих ни на одной из этих четвёрок наборов ни одну из четвёрок значений $(1, 0, 0, 1), (0, 1, 1, 0)$. Любая булева функция $f(\tilde{x}^n)$, не принадлежащая множеству F_n , удовлетворяет либо соотношениям

$$f(1, \sigma_2, \dots, \sigma_{n-1}, 1) = f(0, \bar{\sigma}_2, \dots, \bar{\sigma}_{n-1}, 0) = 1, \\ f(1, \sigma_2, \dots, \sigma_{n-1}, 0) = f(0, \bar{\sigma}_2, \dots, \bar{\sigma}_{n-1}, 1) = 0,$$

либо соотношениям

$$f(1, \sigma_2, \dots, \sigma_{n-1}, 0) = f(0, \bar{\sigma}_2, \dots, \bar{\sigma}_{n-1}, 1) = 1, \\ f(1, \sigma_2, \dots, \sigma_{n-1}, 1) = f(0, \bar{\sigma}_2, \dots, \bar{\sigma}_{n-1}, 0) = 0$$

для некоторых $\sigma_2, \dots, \sigma_{n-1} \in \{0, 1\}$. Тогда функция $f(\tilde{x}^n)$ удовлетворяет условию теоремы 2 при $i = n$ и $\sigma_1 = 1$ для некоторого $\sigma_n \in \{0, 1\}$, поэтому $D(f) = 4$.

Найдём мощность множества F_n . На каждой из 2^{n-2} четвёрок наборов $U_{\sigma_1, \dots, \sigma_{n-2}}$ любая функция из этого множества может принимать любую из $2^4 - 2 = 14$ четвёрок значений. Следовательно, $|F_n| = 14^{2^{n-2}}$. Тогда

$$\frac{|F_n|}{2^{2^n}} = \frac{14^{2^{n-2}}}{16^{2^{n-2}}} = \left(\frac{7}{8}\right)^{2^{n-2}} \rightarrow 0 \quad (n \rightarrow \infty).$$

Таким образом, отношение числа булевых функций из множества F_n к общему числу булевых функций от n переменных (2^{2^n}) стремится к 0 при $n \rightarrow \infty$. Выше было показано, что для любой булевой функции $f(\tilde{x}^n)$, не принадлежащей множеству F_n , выполнено равенство $D(f) = 4$, откуда следует справедливость теоремы 3. \square

7. Заключение

Описанный в работе для почти всех булевых функций от n переменных метод синтеза реализующих их контактных схем, допускающих единичные проверяющие тесты длины 4 относительно обрывов и замыканий контактов, ввиду малой длины тестов, а значит, малого времени, необходимого для тестирования таких схем, может найти практическое применение. Сложности указанных схем при этом не превосходят $4n \cdot 2^n$, что по порядку в n^2 раз больше нижней оценки сложности реализации почти любой булевой функции от n переменных в классе контактных схем (см., например, [1, с. 60, лемма 8]).

Вместе с тем, пока не удалось получить единой верхней оценки длины минимального единичного проверяющего теста для **любой** булевой функции от n переменных, т. е. верхней оценки величины $D_{\text{ЕП}}(n)$, улучшающей оценку $D_{\text{ЕП}}(n) = O\left(\frac{2^n}{n\sqrt{n}}\right)$ из [7]. Представляет интерес также изучение возможностей реализации всех или почти булевых функций от n переменных контактными схемами, допускающими короткие единичные диагностические тесты, либо контактными схемами, допускающими короткие проверяющие или диагностические тесты относительно обрывов и замыканий не более k контактов, где $k \geq 2$ — заданное натуральное число.

Список литературы

- [1] Лупанов О.Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

- [2] Чегис И. А., Яблонский С. В. Логические способы контроля работы электрических схем // Труды МИАН. — 1958. — **51**. — С. 270–360.
- [3] Яблонский С. В. Надёжность и контроль управляющих систем // Мат-лы Всесоюз. семинара по дискретн. матем. и её прилож. (Москва, 31 января–2 февраля 1984 г.) / Под ред. О. Б. Лупанова. — М.: Изд-во МГУ, 1986. — С. 7–12.
- [4] Яблонский С. В. Некоторые вопросы надёжности и контроля управляющих систем // Матем. вопросы киберн. Вып. 1. — М.: Наука, 1988. — С. 5–25.
- [5] Редькин Н. П. Надёжность и диагностика схем. — М.: Изд-во МГУ, 1992.
- [6] Мадатян Х. А. Полный тест для неповторных контактных схем // Проблемы киберн. Вып. 23. — М.: Наука, 1970. — С. 103–118.
- [7] Мадатян Х. А. Построение единичных тестов для контактных схем // Сборник работ по матем. киберн. — М.: ВЦ АН СССР, 1981. — С. 77–86.
- [8] Редькин Н. П. О полных проверяющих тестах для контактных схем // Методы дискретн. анализа в исслед. экстрем. структур. Вып. 39. — Новосибирск: ИМ СО АН СССР, 1983. — С. 80–87.
- [9] Романов Д. С. О синтезе контактных схем, допускающих короткие проверяющие тесты // Уч. зап. Казан. ун-та. Физ.-матем. науки. — 2014. — **156**, кн. 3. — С. 110–115.
- [10] Романов Д. С., Романова Е. Ю. О единичных проверяющих тестах для схем переключательного типа // Изв. высш. учебн. завед. Поволж. регион. Физ.-матем. науки. — 2015. — № 1 (33). — С. 5–23.
- [11] Попков К. А. О тестах замыкания для контактных схем // Дискретн. матем. — 2016. — **28**, вып. 1. — С. 87–100.
- [12] Попков К. А. О проверяющих тестах размыкания для контактных схем // Дискретн. матем. — 2017. — **29**, вып. 4. — С. 66–86.
- [13] Попков К. А. О диагностических тестах размыкания для контактных схем // Дискретн. матем. — 2019. — **31**, вып. 2. — С. 124–143.
- [14] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

Short single fault detection tests for contact circuits under breaks and closures of contacts

Popkov K.A.

We consider a problem of implementation of Boolean functions by irredundant two-pole contact circuits which allow short single fault detection tests regarding breaks and closures of contacts. We describe all functions which the minimal length of such a test equals 0, 1, 2, and 3 for. We prove that, for almost all Boolean functions on n variables, this length equals 4.

Keywords: contact circuit, Boolean function, contact break, contact closure, fault detection test.

Некорректность интуиционистской теории множеств относительно конструктивной семантики, основанной на гиперарифметических видах.

Коновалов А.Ю.

Исследуется вопрос о корректности аксиом интуиционистской теории множеств относительно семантики реализуемости, основанной на гиперарифметических видах.

Ключевые слова: конструктивная семантика, реализуемость, аксиоматическая теория множеств, гиперарифметические виды.

В интуиционистской математике одним из аналогов понятия множества является *вид* как точно сформулированное условие, которому могут удовлетворять некоторые математические объекты (см. [1]), называемые в этом случае *членами* вида. В работе [2] мы определили семантику типа реализуемости для языка теории множеств, основанную на гиперарифметических видах. В настоящей статье мы продолжим исследование этой семантики.

Отношения на множестве натуральных чисел, принадлежащие классу Π_1^1 аналитической иерархии [3, §16.1], назовем Π_1^1 -предикатами. Из [3, §16.1, теорема V] следует, что найдется такой Π_1^1 -предикат $U(z, x_1, x_2)$, который является универсальным для класса всех 2-местных Π_1^1 -предикатов. Натуральное число z назовем Π_1^1 -индексом отношения $P(x_1, x_2)$, если имеет место $P(x_1, x_2) \iff U(z, x_1, x_2)$. Будем говорить, что отношение $P(x_1, \dots, x_n)$ является гиперарифметическим, если $P(x_1, \dots, x_n)$ и $\neg P(x_1, \dots, x_n)$ суть Π_1^1 -предикаты. Натуральное число z назовем Δ_1^1 -индексом отношения $P(x_1, x_2)$, если $z = c(z_1, z_2)$, где z_1 — Π_1^1 -индекс отношения $\neg P(x_1, x_2)$, а z_2 — Π_1^1 -индекс отношения $P(x_1, x_2)$. Пусть I — множество всех Δ_1^1 -индексов всех 2-местных гиперарифметических отношений, а $D_z(x_1, x_2)$ — гиперарифметическое отношение, Δ_1^1 -индекс которого есть z .

Посредством трансфинитной индукции для каждого ординала α определим множество Δ_α следующим образом:

$$\Delta_\alpha \equiv \{z \in I \mid \neg \exists s \exists x D_z(s, x)\}, \text{ если } \alpha = 0;$$

$$\Delta_\alpha \equiv \{z \in I \mid \forall s, x (D_z(s, x) \rightarrow x \in \Delta_\beta)\}, \text{ если } \alpha = \beta + 1;$$

$$\Delta_\alpha \equiv \bigcup_{\beta < \alpha} \Delta_\beta, \text{ если } \alpha \text{ — предельный ординал.}$$

Через Δ обозначим объединение всех множеств Δ_α , для которых ординал α конечен либо счетен.

Формулы языка теории множеств строятся из предметных переменных, констант элементов множества Δ , двухместных предикатных символов $=$ и \in , логических констант \perp , \top , логических связок \wedge , \vee , \rightarrow , кванторов \forall , \exists и скобок по обычным правилам. При записи формул будем использовать следующие сокращения:

- $\neg\Phi \equiv \Phi \rightarrow \perp$;
- $\exists x \in t \Phi(x) \equiv \exists x (x \in t \wedge \Phi(x))$;
- $\forall x \in t \Phi(x) \equiv \forall x (x \in t \rightarrow \Phi(x))$;
- $\exists! x \Phi(x) \equiv \exists x (\Phi(x) \wedge \forall y (\Phi(y) \rightarrow y = x))$;
- $\forall x_1, \dots, x_n (\Phi \leftrightarrow \Psi) \equiv \forall x_1, \dots, x_n (\Phi \rightarrow \Psi) \wedge \forall x_1, \dots, x_n (\Psi \rightarrow \Phi)$.

Фиксируем примитивно рекурсивную взаимно-однозначную функцию c , кодирующую пары натуральных чисел натуральными числами. Тогда одноместные обратные функции p_1 и p_2 , где $p_1(x)$ и $p_2(x)$ суть первая и вторая компоненты пары c с кодом x , т. е. $c(p_1(x), p_2(x)) = x$, также примитивно рекурсивны. Для каждого натурального числа n фиксируем вычислимую нумерацию всех n -местных частично-рекурсивных функций: $\varphi_1^n, \varphi_2^n, \dots$.

Согласно [2], для всякого натурального числа e и произвольной замкнутой формулы Φ языка теории множеств определим отношение « e реализует Φ » (обозначение: $e \mathbf{r} \Phi$) следующим индуктивным образом:

- $e \mathbf{r} (a = b) \equiv a = b$;
- $e \mathbf{r} (a \in b) \equiv D_b(e, a)$;
- $e \mathbf{r} (\Phi \wedge \Psi) \equiv p_1 e \mathbf{r} \Phi \text{ и } p_2 e \mathbf{r} \Psi$;

- $e \mathbf{r} (\Phi \vee \Psi) \Leftrightarrow (p_1 e = 0 \text{ и } p_2 e \mathbf{r} \Phi) \text{ или } (p_1 e = 1 \text{ и } p_2 e \mathbf{r} \Psi)$;
- $e \mathbf{r} \exists x \Phi(x) \Leftrightarrow p_1 e \in \Delta \text{ и } p_2 e \mathbf{r} \Phi(p_1 e)$;
- $e \mathbf{r} \forall x_1, \dots, x_n (\Phi(x_1, \dots, x_n) \rightarrow \Psi(x_1, \dots, x_n)) \Leftrightarrow$ [для всех¹ натуральных чисел s и $a_1, \dots, a_n \in \Delta$, если $s \mathbf{r} \Phi(a_1, \dots, a_n)$, то определено $\varphi_e^{n+1}(a_1, \dots, a_n, s)$ и верно $\varphi_e^{n+1}(a_1, \dots, a_n, s) \mathbf{r} \Psi(a_1, \dots, a_n)$], при этом список переменных x_1, \dots, x_n может быть пустым;
- $e \mathbf{r} \forall x_1, \dots, x_n \Phi(x_1, \dots, x_n) \Leftrightarrow [e \mathbf{r} \forall x_1, \dots, x_n (\top \rightarrow \Phi(x_1, \dots, x_n))]$, если список переменных x_1, \dots, x_n непуст, формула $\Phi(x_1, \dots, x_n)$ не начинается с квантора \forall , и логическая связка \rightarrow не является главной в $\Phi(x_1, \dots, x_n)$.

Будем говорить, что замкнутая формула Φ языка теории множеств является *реализуемой*, если найдется такое натуральное число e , что имеет место $e \mathbf{r} \Phi$.

Интуиционистская теория множеств имеет следующие аксиомы и схемы аксиом:

$$\begin{aligned}
& \exists z \forall x (x \in z \rightarrow \perp); & (\emptyset) \\
& \forall x \exists z (x \in z \wedge \forall u \in z \exists u' \in z \forall y (y \in u' \leftrightarrow y = u)); & (\text{Inf}) \\
& \forall x, y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y); & (\text{Ext}) \\
& \forall x, y \exists z \forall u (u \in z \leftrightarrow (u = x \vee u = y)); & (\text{Pair}) \\
& \forall x \exists z \forall u (u \in z \leftrightarrow \exists y (y \in x \wedge u \in y)); & (\text{Un}) \\
& \forall y \exists z \forall x (x \in z \leftrightarrow \forall u (u \in x \rightarrow u \in y)); & (\text{Pow}) \\
& \forall x (\forall u \in x \Phi(u) \rightarrow \Phi(x)) \rightarrow \forall x \Phi(x), & (\text{Ind}) \\
& \forall x \exists y \forall u (u \in y \leftrightarrow u \in x \wedge \Phi(u)); & (\text{Sep}) \\
& \forall x [\forall v \in x \exists u \Phi(v, u) \rightarrow \exists y \forall v \in x \exists u \in y \Phi(v, u)]. & (\text{Coll})
\end{aligned}$$

Верны следующие теоремы.

Теорема 1. *Следующие аксиомы интуиционистской теории множеств являются реализуемыми: (\emptyset) , (Inf) , (Pair) , (Un) , (Ind) , (Coll) .*

Теорема 2. *Следующие аксиомы интуиционистской теории множеств не являются реализуемыми: (Ext) , (Pow) .*

¹ Однако, если в списке x_1, \dots, x_n на некоторых позициях i и j стоят одинаковые переменные x_i и x_j , то мы не допускаем рассмотрение тех списков a_1, \dots, a_n , в которых $a_i \neq a_j$.

Список литературы

- [1] А. Гейтинг, *Интуиционизм*, Мир, М., 1965.
- [2] А. Ю. Коновалов, “Семантика реализуемости для конструктивной теории множеств, основанная на гиперарифметический предикатах”, *Вестн. Моск. ун-та. Матем. Механ.*, 2017, № 3, 59–62.
- [3] Х. Роджерс, *Теория рекурсивных функций и эффективная вычислимость*, Мир, М., 1972.

The intuitionistic set theory is not sound with respect to the constructive semantics based on hyperarithmetical sorts.

Kononov A. Yu.

The soundness of axioms of the intuitionistic set theory with respect to the realizability semantics based on hyperarithmetical sorts is studied.

Keywords: constructive semantics, realizability, axiomatic set theory, hyperarithmetical sorts.

О классах передаточных функций линейных автоматов

Часовских А.А.

Для классов передаточных функций линейных автоматов над конечным полем с операциями, индуцированными операциями композиции над этими автоматами, найдены все максимальные подалгебры.

Ключевые слова: конечный автомат, линейный автомат, передаточная функция, операции композиции, обратная связь, полнота, замкнутый класс, предполный класс, конечное поле.

Обозначения, которые не введены в этой работе, можно найти в [6] — [8]. Как и в этих работах, линейный автомат f над конечным полем E_k мы отождествляем с функцией, переменные которой принимают значения из $R_k(\xi)$, и для некоторых дробей μ_i из $E'_k(\xi)$, $i = 0, 1, \dots, n$, выполнено:

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^n \mu_i x_i + \mu_0.$$

В книге [2] коэффициенты μ_i , $i \in \{1, 2, \dots, n\}$, называются передаточными функциями линейного автомата f .

Как следует из [6], операции композиции в классе линейных автоматов индуцируют оператор замыкания K^1 в классе передаточных функций $E'_k(\xi)$, состоящий из операций сложения, умножения и частичной операции «fb», причем для пары дробей μ_i , $i = 1, 2$, значение $\text{fb}(\mu_1, \mu_2)$ определено в точности тогда, когда $\mu_2 \in \xi E'_k(\xi)$, и в этом случае имеем:

$$\text{fb}(\mu_1, \mu_2) = \frac{\mu_1}{1 - \mu_2}.$$

В настоящей работе мы найдем все предполные [3] (максимальные) подклассы в $E'_k(\xi)$, рассматриваемом вместе с оператором замыкания K^1 . Сначала в $E'_k(\xi)$ мы выделим некоторые подмножества. Положим:

$$M_1^{(1)} = \{ \mu \mid \mu \in E'_k(\xi), \mu - \mu(0) \in \xi^2 E'_k(\xi) \},$$

$$R_0^{(1)} = \left\{ \mu \mid \mu \in E'_k(\xi), \mu = \frac{u}{v}, \deg u < \deg v \right\}.$$

Число k является степенью некоторого простого числа p , $k = p^m$. Множество автоморфизмов Ω_k поля E_k содержит $\log_p k = m$ элементов [5]. Для каждого ω , $\omega \in \Omega$, в $E'_k(\xi)$ содержится множество $M_{0,\omega}$,

$$M_{0,\omega}^{(1)} = \left\{ \mu \mid \mu = \frac{u}{v}, \deg u \leq \deg v, \mu(1/\xi)(0) = \omega(\mu(0)) \right\}.$$

Как указано в [6], между множеством W_k максимальных подполей поля E_k и множеством простых делителей числа $\log_p k$ имеется биективное соответствие. Положим:

$$P_{\Delta}^{(1)} = \left\{ \mu \mid \mu \in E'_k(\xi), \mu(0) \in \Delta \right\},$$

$\Delta \in W_k$.

Множество приведенных неприводимых многочленов кольца $E_k[\xi]$, не включающее только многочлен ξ , обозначим I_k . Для заданного p , $p \in I_k$, множество несократимых дробей из $E'_k(\xi)$, числители которых делятся на p , обозначим $R_p^{(1)}$.

Для дроби μ из $E'_k(\xi)$, знаменатель которой не делится на некоторый p , $p \in I_k$, единственным образом определен многочлен u степени меньшей $\deg p$, удовлетворяющий для некоторого μ' , $\mu' \in E'_k(\xi)$, равенству

$$\mu = u + p\mu'.$$

Многочлен u при этом будем обозначать $\text{rest}_p(\mu)$.

Положим:

$$M_{p,\omega}^{(1)} = \left\{ \mu \mid \mu = \frac{u}{v}, (u, v) = 1, \text{rest}_p(\mu) = \omega(\mu(0)) \right\},$$

$p \in I_k$, $\omega \in \Omega$.

Нам понадобится следующее множество:

$$J_k^{(1)} = \left\{ M_1^{(1)}, R_0^{(1)}, M_{0,\omega}^{(1)}, P_{\Delta}^{(1)}, R_p^{(1)}, M_{p,\omega}^{(1)} \mid \omega \in \Omega, \Delta \in W_k, p \in I_k \right\}.$$

Имеет место:

Теорема 1. *Множество $J_k^{(1)}$ состоит из максимальных подклассов $E'_k(\xi)$ и содержит все его максимальные подклассы.*

Тождественный автоморфизм поля E_k обозначим id . Для случая $k = p$, то есть для простого поля, имеем:

$$J_k^{(1)} = \left\{ M_1^{(1)}, R_0^{(1)}, M_{0,\text{id}}^{(1)}, P_1^{(1)}, R_p^{(1)}, M_{p,\text{id}}^{(1)} \mid p \in I_k \right\}.$$

что совпадает с результатами работы [7].

Для доказательства теоремы нам понадобятся вспомогательные утверждения. Пусть F — некоторое подполе в $E_k(\xi)$ и $M \subseteq E_k(\xi)$. Поле, полученное расширением F путем присоединения элементов множества M , обозначаем $F(M)$ [5]. Для одноэлементного множества вместо $F(\{\mu\})$ используем более короткое обозначение $F(\mu)$. Собственное подполе поля F называется максимальным, если оно не содержится в другом собственном подполе этого поля.

Лемма 1. *Если множество M , $M \subseteq E'_k(\xi)$, не содержится ни в одном Θ , $\Theta \in J_k^{(1)}$, то M не содержится ни в одном максимальном подполе поля $E_k(\xi)$.*

Доказательство леммы. Пусть $M \subseteq E'_k(\xi)$ и $\forall \Theta, \Theta \in J_k^{(1)}$, имеет место:

$$M \not\subseteq \Theta.$$

Рассмотрим какое-либо максимальное подполе F поля $E_k(\xi)$. Пусть

$$E_k \subseteq F. \quad (1)$$

Тогда по теореме Люрота [1] для некоторого μ , $\mu \in E_k(\xi)$, имеем: $F = E_k(\mu)$.

Если $\mu \in E_k$, то F не является максимальным подполем поля $E_k(\xi)$, так как

$$F \subsetneq E_k(\xi^2) \subsetneq E_k(\xi).$$

Если $\text{deg } \mu = 1$, то, как не трудно видеть, $F = E_k(\xi)$, и F не является максимальным подполем поля $E_k(\xi)$.

Таким образом, $\text{deg } \mu > 1$, и, не ограничивая общности рассуждений, будем предполагать, что $\mu \in \xi E'_k(\xi)$.

Тогда для некоторых многочленов u и v из $E_k[\xi]$ имеем: $\mu = \xi \frac{u}{v}$, $\max(\text{deg } \xi u, \text{deg } v) > 1$.

Если $\text{deg } u \geq 1$, то для некоторого p , $p \in I_k$, выполнено включение:

$$\{ E_k, \mu \} \subset M_{p,\text{id}}^{(1)}.$$

Поэтому, как не трудно видеть,

$$F \cap E'_k(\xi) \subseteq M_{p,\text{id}}^{(1)},$$

откуда следует, что

$$M \not\subseteq F. \quad (2)$$

Если $\deg u = 0$, то $\deg v > 1$ и

$$F \cap E'_k(\xi) \subseteq M_{0,\text{id}}^{(1)},$$

откуда вытекает (2).

Таким образом, случай (1) рассмотрен.

Пусть включение (1) не имеет места. Известно [5], что в $E_p[z]$ найдется неприводимый многочлен $f(z)$, для корня a которого, имеем:

$$E_p(a) = E_k.$$

Обозначим через $E_{k'}$ поле $E_k \cap F$. Рассмотрим ненулевой приведенный многочлен минимальной степени $g(z)$, $g(z) \in F[z]$, имеющий корень $z = a$. Нетрудно видеть, что $g(z)$ делит $f(z)$. Так как многочлена $f(z)$ имеет в поле E_k ровно m корней $a^{p^0}, a^{p^{-1}}, a^{p^2}, \dots, a^{p^{m-1}}$, то все коэффициенты многочлена $g(z)$ содержатся в $E_{k'}$. Если $E_{k'}$ не является максимальным подполем поля E_k , то найдется такое поле $E_{k''}$, что выполнены соотношения:

$$E_{k'} \subsetneq E_{k''} \subsetneq E_k.$$

В соответствии с [4], степень расширения поля E над его подполем E' называется размерность E как линейного пространства над E' , которая обозначается $[E : E']$. Из приведенных выше рассуждений имеем:

$$[E_k(\xi) : F] = [E_k : E_{k'}]. \quad (3)$$

Расширение поля F элементами из $E_{k''}$ обозначим F' . Отсюда получаем:

$$1 < [F' : F] \leq [E_{k''} : E_{k'}].$$

Из полученного неравенства и равенства (3) следует, что F не является максимальным подполем в $E_k(\xi)$. Полученное противоречие означает, что $E_{k'}$ — максимальное подполе в E_k .

Покажем теперь, что в случае

$$E_k \not\subseteq F \quad (4)$$

максимальное подполе F содержит дробь степени 1. Имеет место равенство:

$$E_{k'}(a) = E_k,$$

и существует неприводимый над $E_{k'}$ многочлен $\hat{f}(z)$, $\hat{f} \in E_{k'}[z]$, для которого a является корнем. Через q обозначим $\deg \hat{f}$.

Из максимальной подполя F и соотношения (4) следует, что множество A ,

$$A = \{ a^i \mid i \in \{0, 1, \dots, q-1\} \}$$

образует базис $E_k(\xi)$ как линейного пространства над F . Поэтому для некоторых μ_i , $\mu_i \in F$, $i = 0, 1, \dots, q-1$, имеет место тождество:

$$\xi = \sum_{i=0}^{q-1} \mu_i a^i.$$

Пусть дроби $\mu_i = \frac{u_i}{v_i}$ представлены в несократимом виде, $i = 0, 1, \dots, q-1$. Так как $\xi \notin E_k$, то найдется i_0 , $i_0 \in \{i = 0, 1, \dots, q-1\}$, такое, что $\deg \mu_{i_0} \geq 1$.

Многочлен $h_1(z)$, $h_1(z) = \mu_{i_0} v_{i_0}(z) - u_{i_0}(z)$, имеет корень $z = \xi$, поэтому он делится на $h_0(z)$, $h_0(z) = z - \sum_{i=0}^{q-1} \mu_i a^i$ в кольце $E_k(\xi)[z]$ без остатка, так как множество A линейно независимо над F . Таким образом, для некоторого многочлена \tilde{f} , $\tilde{f} \in E_k(\xi)[z]$, имеет место равенство:

$$h_1 = \tilde{f} h_0.$$

Можно показать, что \tilde{f} не зависит от переменной ξ , поэтому многочлен $h_0(z) = h_1/\tilde{f}$ степени 1 по z имеет коэффициенты из $E_k(\mu_{i_0})$ и корень $z = \xi$. Таким образом,

$$E_k(\mu_{i_0}) = E_k(\xi),$$

откуда вытекает равенство:

$$F = E_{k'}(\mu_{i_0}).$$

При этом, $\deg \mu_{i_0} = 1$. Не ограничивая общности, можно предположить, что $\mu_{i_0} \in E'_k(\xi)$.

Несложно показать, что для любого максимального подполя $E_{k'}$ поля E_k и любого μ , $\mu \in E'_k(\xi)$, $\deg \mu = 1$, найдется пара p, ω , для которой выполнено включение:

$$E_{k'} \cup \{\mu\} \subset M_{p,\omega}^{(1)}.$$

Из этого включения путем некоторых рассуждений получаем:

$$E_{k'}(\mu) \cap E'_k(\xi) \subseteq M_{\rho, \omega}^{(1)}.$$

Поэтому рассматриваемое множество M не может содержаться в $E_{k'}(\mu)$.

Лемма 1 доказана.

Введем следующие подмножества $E'_k(\xi)$.

$$\tilde{R}_0^{(1)} = \left\{ \mu \mid \mu \in E'_k(\xi), \mu = \frac{u}{v}, \deg u \leq \deg v \right\},$$

$$\tilde{R}_p^{(1)} = \left\{ \mu \mid \mu \in E'_k(\xi), \mu = \frac{u}{v}, (v, p) = 1 \right\},$$

$p \in I_k$.

Лемма 2. Пусть множество дробей M из $E'_k(\xi)$ не содержится ни в одном классе множества $J_k^{(1)}$. Тогда для любого $\rho, \rho \in I_k \cup \{0\}$, выполнено:

$$K^{(1)}(M) \not\subseteq \tilde{R}_\rho^{(1)}.$$

Доказательство леммы.

Пусть $M \subseteq E'_k(\xi)$,

$$\forall \Theta, \Theta \in J_k^{(1)}, M \not\subseteq \Theta. \quad (5)$$

Покажем, что для каждого $\rho, \rho \in I_k \cup \{0\}$, для которого

$$M \subseteq \tilde{R}_\rho^{(1)}, \quad (6)$$

в $K(M)$ содержится дробь μ'_ρ , удовлетворяющая соотношениям $\mu'_\rho(0) = 0$ и $\mu'_\rho \notin R_\rho^{(1)}$.

Пусть для некоторого ρ выполнено (6). Из соотношений (5) для $\Theta \in \{P_\Delta \mid \Delta \in W_k\}$ вытекает, что в $K^1(M)$ содержится дробь μ такая, что $\mu(0)$ является примитивным элементом поля E_k .

Через $\tilde{\mu}$ обозначим элемент множества $M \setminus R_\rho^{(1)}$. Если дробь $\tilde{\mu}$ не является искомой, то $\tilde{\mu}(0) \neq 0$. Поэтому для некоторой степени \tilde{s} имеем: $\tilde{\mu}(0) = \mu^{\tilde{s}}(0)$. Если при этом $\mu \in R_\rho^{(1)}$, то $\tilde{\mu} - \mu^{\tilde{s}}$ — искомый элемент $K^1(M)$.

Рассмотрим случай $\mu \notin R_\rho^{(1)}$. Если для любого $\omega, \omega \in \Omega, \mu \notin M_{\rho, \omega}^{(1)}$, то через f обозначим ненулевой многочлен минимальной степени из $E_p[z]$, имеющий корень $\mu(0)$. Нетрудно видеть, что $f(\mu)$ — искомый.

Осталось рассмотреть случай $\mu \in M_{\rho, \omega}^{(1)}$ для некоторого ω , $\omega \in \Omega$. В M , в соответствии с (5) найдется дробь $\hat{\mu}$, $\hat{\mu} \notin M_{\rho, \omega}^{(1)}$. Если $\hat{\mu}(0) = 0$, то $\hat{\mu}$ — искомая. В противном случае, найдется \hat{s} , что $\hat{\mu} - \mu^{\hat{s}}$ — искомая.

Требуемое свойство множества M доказано. Утверждение леммы следует теперь из лемм 6 и 7 работы [6].

Лемма доказана.

Доказательство теоремы. Замкнутость классов из множества $J_k^{(1)}$ проверяется с использованием определений этих классов.

Если множество M не содержится ни в одном классе из $J_k^{(1)}$, то по лемме 1, с учетом расширяемости каждого множества из $E_k(\xi)$, не порождающего все $E_k(\xi)$, до максимального подполя, получаем равенство:

$$E_p(M) = E_k(\xi).$$

Отсюда, из теоремы 3 работы [6] и леммы 2 следует равенство

$$K^1(M) = E'_k(\xi).$$

Таким образом, $J_k^{(1)}$ является критериальной системой.

Приведенность множества $J_k^{(1)}$, то есть не включение никакого класса Θ этого множества в любой его другой класс Θ' проверяется предъявлением элемента из $\Theta \setminus \Theta'$.

Теорема доказана.

Список литературы

- [1] Ван дер Варден Б. Л., *Алгебра*, пер. с нем., «Наука», Москва, 1976, 648 с.
- [2] Гилл А., *Линейные последовательностные машины*, пер. с англ., «Наука», Москва, 1974, 288 с.
- [3] Кудрявцев В.Б., Алешин С.В., Подколзин А.С., *Введение в теорию автоматов*, «Наука», Москва, 1985, 320 с.
- [4] Ленг С., *Алгебра*, пер. с англ., «Мир», Москва, 1968, 564 с.
- [5] Лидл Р., Нидеррайтер Г., *Конечные поля*, пер. с англ., «Мир», Москва, 1988, 430 с.
- [6] Часовских А.А., “Проблема полноты для класса линейно-автоматных функций”, *Дискретная математика*, **27**:2 (2015), 134–51
- [7] Часовских А.А., “Условия полноты линейно-р-автоматных функций”, *Интеллектуальные системы*, **18**:3 (2014), 203–252
- [8] Часовских А.А., “Приведенные критериальные системы предполных классов в классах линейных автоматов над конечными полями”, *Интеллектуальные системы*, **22**:4 (2018), 115–134

On classes of transfer functions of linear automata
Chasovskikh A.A.

For classes of transfer functions of linear automata over a finite field with operations induced by composition operations on these automata, all maximal subclasses are found.

Keywords: finite automaton, linear automaton, transfer function, operation of composition, feedback, completeness, closed class, maximum subclass, finite field.

Часть 4.
Материалы семинара «Теория
автоматов»

Доклады семинара «Теория автоматов»

В первом и втором кварталах 2019 года на научном семинаре «Теория автоматов» под руководством академика Валерия Борисовича Кудрявцева состоялось 9 докладов.

20 февраля 2019 года

Сложность кванторной задачи удовлетворения ограничениям в зависимости от языка ограничений

с.н.с. Жук Д. Н.

В 2017 году была описана сложность задачи удовлетворения ограничениям в зависимости от языка допустимых ограничений. Одним из обобщений этой задачи является кванторная задача удовлетворения ограничений, где помимо кванторов существования можно использовать также кванторы всеобщности, а именно: на вход подается замкнутая формула первого порядка с единственной связкой конъюнкцией; нужно проверить, верна формула или нет. Нам удалось полностью описать сложность этой задачи для любого языка ограничений на трехэлементном множестве: оказалось, что либо задача решается за полиномиальное время, либо является полной в одном из классов NP , $co - NP$, $PSPACE$. Более того, показано, что уже на четырехэлементном множестве появляются другие классы сложности из булевой иерархии.

27 февраля 2019 года

О сложности доказательства тавтологий

доцент Боков Г. В.

Одной из центральных проблем теории сложности вычислений является вопрос о существовании полиномиальной разрешающей процедуры для классических тавтологий. Её важность обусловлена взаимосвязью с задачей отделимости классов сложности, установленной Куком и Рекхау в 1979 году. Данная взаимосвязь послужила основой программы Кука-Рекхау по получению суперполиномиальных нижних оценок сложности

доказательства тавтологий. В докладе будет рассказано о современном состоянии этой программы, полученных результатах и связанных с ней открытых проблемах.

13 марта 2019 года

Автоматы в лабиринтах. Вычисления на автоматах. Задача преследования

н.с. Волков Н. Ю.

В докладе будет рассказано о задаче преследования системой автоматов («хищников») нескольких независимых друг от друга автоматов («жертв») на плоскости и о том, как автоматы в лабиринтах позволяют моделировать сложные вычисления.

20 марта 2019 года

Об алгебрах, порождаемых линейными автоматами

доцент Часовских А. А.

Для поиска предполных классов в классах линейных автоматов над конечными полями потребовалось решить ряд задач для алгебры одноместных линейных автоматов, сохраняющих нулевую последовательность. В частности, в ней найдены все максимальные подалгебры. При этом использованы результаты о подполях трансцендентных расширений конечных полей. В докладе будут освещены алгебраические аспекты решения задач о полноте в классах линейных автоматов, а также приемы, позволившие выполнить редукцию к алгебре одноместных линейных автоматов, сохраняющих нулевую последовательность.

27 марта 2019 года

О решётке замкнутых классов автоматов с операцией суперпозиции

профессор Бабин Д. Н.

Функциональная система автоматов с операцией суперпозиции не является конечно-порождённой. Кудрявцев В.Б. в 1963 г. показал, что в ней имеется континуум предполных классов. Пример замкнутого класса автоматов, не расширяющегося в этой функциональной системе до предполного, был построен автором. Этот класс Ω является замыканием множества автономных автоматов, автоматов без памяти и автомата-«триггера» (автомата задержки с дополнительной входной буквой пропуска тактов). Очевидно, что все надклассы класса Ω также не расширяются до предполного. Естественно возник вопрос о сохранении свойства не расширяемости в подклассах класса Ω .

Пусть $\sigma \subset \Omega$ – это замыкание множества автоматов без памяти и автомата-«триггера». В настоящей работе автор показал, что всякий замкнутый класс $\sigma \subset \mu \subset \Omega$ до предполного расширяется, и таких классов континуум.

3 апреля 2019 года

О вероятностных и комбинаторно-топологических методах в задаче оценки числа пороговых функций

доцент Ирматов А. А.

В докладе будет рассказано о современных вероятностных и комбинаторно-топологических методах, используемых для получения нижних оценок числа пороговых функций.

17 апреля 2019 года

О фундаментальных проблемах глубокого машинного обучения

с.н.с. Мазуренко И. Л.

В докладе будет рассказано о современном состоянии глубокого машинного обучения. Особое внимание будет уделено способности нейронных сетей выражать любые непрерывные функции с любой наперед заданной точностью. Кроме того, будет рассказано об основных типах нейронных сетей, сходимости обучения, обобщающей способности нейронных сетей, атаках на нейронные сети. Будут сформулированы открытые проблемы в области глубокого машинного обучения.

24 апреля 2019 года

О нелинейной глубине нейронных схем с функцией активации ReLU

н.с. Половников В. С.

В докладе будет рассказано о новых результатах, полученных для нейронных схем из элементов, представляющих собой полную (по операции суперпозиции) систему кусочно-параллельных функций, содержащую все линейные элементы и нелинейную часть — функцию ReLU.

15 мая 2019 года

О классах функций многозначной логики с минимальным логарифмическим темпом роста

аспирант Комков С. А.

Получен критерий минимального логарифмического темпа роста для произвольного конечного множества с заданным множеством операций, а именно, описание всех таких конечных множеств A с заданными на них операциями, чей темп роста отличается не более чем на константу от логарифмического темпа роста по основанию $|A|$.

К сведению авторов публикаций в журнале «Интеллектуальные системы. Теория и приложения»

В соответствии с требованиями ВАК РФ к изданиям, входящим в перечень ведущих рецензируемых научных журналов и изданий, в которых могут быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук, статьи в журнал «Интеллектуальные системы. Теория и приложения» предоставляются авторами в следующей форме:

1. Статьи, набранные в пакете ЛАТ_EX, предоставляются к загрузке через WEB-форму http://intsysjournal.org/generator_form.
2. К статье прилагаются файлы, содержащие название статьи на русском и английском языках, аннотацию на русском и английском языках (не более 50 слов), список ключевых слов на русском и английском языках (не более 20 слов), информация об авторах: Ф.И.О. полностью, место работы, должность, ученая степень и/или звание (если имеется), контактные телефоны (с кодом города и страны), e-mail, почтовый адрес с индексом города (домашний или служебный).
3. Список литературы оформляется в едином формате, установленном системой Российского индекса научного цитирования.
4. За публикацию статей в журнале «Интеллектуальные системы. Теория и приложения» с авторов (в том числе аспирантов высших учебных заведений) статей, рекомендованных к публикации, плата не взимается. Оттиски статей авторам не предоставляются. Журнал распространяется по подписке, экземпляры журнала рассылаются подписчикам наложенным платежом. Условия подписки публикуются в каталоге НТИ «Роспечать», индекс журнала 64559.
5. Доступ к электронной версии последнего вышедшего номера осуществляется через НЭБ «Российский индекс научного цитирования». Номера, вышедшие ранее, размещаются на сайте <http://intsysjournal.org>, и доступ к ним бесплатный. Там же будут размещены аннотации всех публикуемых статей.

Подписано в печать: 20.09.2019

Дата выхода: 27.09.2019

Тираж: 200 экз.

Цена свободная

Свидетельство о регистрации СМИ: ПИ № ФС77-58444 от 25 июня 2014 г.,
выдано Федеральной службой по надзору в сфере связи, информационных
технологий и массовых коммуникаций (Роскомнадзор).