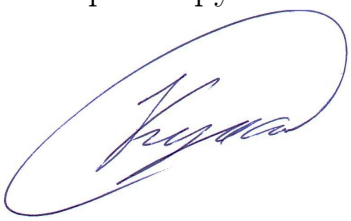
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Сибирский государственный аэрокосмический
университет имени академика М.Ф. Решетнёва»
(СибГАУ)

На правах рукописи



Кукарцев Анатолий Михайлович

ЭФФЕКТИВНЫЕ АЛГОРИТМЫ АНАЛИЗА ДЖЕВОНС-ЭКВИВАЛЕНТНОСТИ ДАННЫХ

Специальность 05.13.17 – Теоретические основы информатики

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
доктор физико-математических наук, доцент
Кузнецов Александр Алексеевич

Красноярск 2016

Оглавление

Введение

Актуальность темы и степень её разработанности. Цифровая информация представляется преимущественно двумя способами: комбинационным и функциональным. Первый рассматривает её в виде комбинации символов некоторого алфавита, а второй – в виде множества значений некоторой дискретной функции. Комбинационные способы представления информации и соответствующие им алгоритмы её обработки начали развиваться с начала XX века. Эти способы представления обычно связывают с работами К. Шеннона [1], Р. В. Хэмминга [2] и многих других исследователей. В конце XX века в связи с развитием информационных технологий и естественной потребностью в качественно новых методах обработки информации начали появляться функциональные способы её представления. Одним из примеров обработки информации в таком представлении является серия алгоритмов сжатия графических данных JPEG [3]. Цифровая информация отображается на некоторую функцию двух аргументов. Далее функция преобразуется и определяющие её параметры (коэффициенты Фурье) округляются, кодируются, и их коды сжимаются комбинационными методами. Такой способ сжатия, как правило, приводит к потерям информации во время преобразования.

Для функционального представления цифровой двоичной информации естественно подходят булевы функции (далее – БФ) [4]. Любому бинарному вектору (далее – БВ), состоящему из нулей и/или единиц, можно инъективно поставить в соответствие БВ длины, кратной степени двойки. Последнему можно взаимно однозначно поставить некоторую БФ. Для этого важно однозначно упорядочить область определения БФ. Это можно выполнить, зафиксировав порядок её аргументов, и в соответствии с ним упорядочить область её определения, например, лексикографически. Сама БФ может быть описана реализующими её функциональными элементами или формулой [5]. Множества отрицаний и перестановок аргументов БФ образуют группу Джевонса [6] и определяют действие над БФ. Указанное действие замечательно тем, что оно

нейтрально, т.к. не затрагивает связей между функциональными элементами и не меняет формулы. Джевонс-эквивалентные БФ будут иметь одинаковые КНФ и ДНФ [7]. Такое действие задаёт естественную эквивалентность БФ и, как следствие, джевонс-эквивалентность соответственных им данным.

Группа Джевонса была определена в конце XIX века С. Джевонсом для описания действия над системой связанных понятий, представленных в виде БФ [6]. Более формальное представление этой группы и другое её название (гипероктаэдральная группа) были предложены А. Янгом [8] в 1930 г. Работы, связанные с группой Джевонса и её приложениями, ведутся с начала XX века, – как за рубежом, так и в России. К ним можно отнести, прежде всего, работы о представлении группы и изучении её свойств исследователей Л. Гейссингера и Д. Кинча [9], М. Баака [10], В. Н. Иванова [11], С. Билли и Т. К. Ламма [12], М. Парвафи, Б. Сивакумара и А. Тамилселви [13], Б. Бьянок [14], Дж. Конда [15], Б. В. Олийныка и В. И. Сущанского [16, 17] и др.; труды, связанные с теорией перечислений исследователей Д. Слепиана [18], П. Константинески [19], Н. Дж. Де Брёйна [20] и др.; практические работы, связанные с кодированием и обработкой информации исследователей О. В. Денисова [21], Д. Г. Видеманна [22] и др.; теоретические и прикладные работы в области криптографии и криптологии исследователей А. В. Тарасова [23], В. Г. Никонова и А. В. Саранцева [24], М. Л. Бурякова и О. А. Логачева [25], Б. А. Погорелова и М. А. Пудовкиной [26, 27], С. П. Горшкова [28], Е. К. Алексеева и Е. К. Карелиной [29] и др.; труды в области генетики исследователей С. Ханненнфлли и П. А. Певзнера [30] и др.; работы в области кристаллографии исследователей Э. Заппа, Э. Дюкмана, и Р. Тварока [31]. К известным нерешенным проблемам, связанным с группой Джевонса, относится также Burnt Pancake problem о сортировке префикс-реверсалами, сформулированная Б. Гейтсом и К. Пападимитроу [32].

Перечислим некоторые важные проблемы в этой предметной области:

– анализ джевонс-эквивалентности данных;

– поиск элементов группы, связывающих джевонс-эквивалентные данные.

Поэтому необходимы эффективные алгоритмы, т.е. такие, которые могут находить решение указанных проблем за разумное время. Как известно, порядок группы Джевонса для БФ n переменных равен $2^n \cdot n!$. Исходя из этого, оценим возможность применения тривиальных алгоритмов, перечисляющих все элементы группы. Время проверки одного элемента составляет $\tau(n) = 10^{-9} \cdot 2^n$, где 2^n – число значений БФ и 10^{-9} с – примерное время вычисления одного значения на ЭВМ (1 ГГц). Тогда полное время работы алгоритма составит $Time(n) = \tau(n) \cdot d_{trivial} = \tau(n) \cdot 2^n \cdot n!$, где $d_{trivial}$ – число действий над БФ тривиальным алгоритмом (порядок группы). В табл. 1 приведены оценки времени работы тривиальных алгоритмов.

Таблица 1. Оценка времени работы тривиальных алгоритмов

n	1–13	14	15	16	17	18	19
$Time(n)$, млн. лет	≈0	0,000742	0,04452	2,8495	193,7679	13951,286	1060297,774

Проанализируем возможность поиска решения тривиальным алгоритмом по табл. 1. Из определения $Time(n)$ можно заключить, что каждое следующее значение времени больше предыдущего в $\frac{10^{-9} \cdot 2^n \cdot 2^n \cdot n!}{10^{-9} \cdot 2^{n-1} \cdot 2^{n-1} \cdot (n-1)!} = 4n$. Начиная с $n = 19$, время, необходимое на вычисление решения указанных задач тривиальным способом, превышает возраст Вселенной [33]. Поэтому требуется эффективный алгоритм решения задач, т.е. такой, который находит решение быстрее тривиального [33].

Указанные проблемы исследуют, начиная с XX века, и относят к задачам классификации. Наиболее известным примером такой классификации является Гарвардский каталог, созданный в 50-х годах XX века [34]. Эти задачи классификации БФ сформулированы в том числе в работах [4, 35]. В работах С. Голомба [36] и Э.А. Якубайтиса [37] предлагались решения указанных проблем, основывающиеся на инвариантах группы, действующей на множестве БФ [4]. Определение инварианта позволяет решить первую проблему. С. Голомб предложил полный инвариант, но сложность его вычисления, так же как и тривиальное решение, носит экспоненциальный характер. Э.А. Якубайтисом также был

предложен инвариант, но он не является полным и дополняется тривиальным алгоритмом. В результате сложность предложенных решений сопоставима со сложностью тривиального алгоритма. По этой причине джевонс-эквивалентные преобразования данных используются в качестве криптографических примитивов [38] в алгоритмах шифрования, основанных на управляемых операциях, где элемент группы является ключом шифрования, а БФ – исходными данными и шифротекстом [39].

Решения указанных задач позволят в перспективе разработать алгоритмы анализа данных, эквивалентных относительно других групп. Задачи, решаемые такими алгоритмами, появляются естественным образом в прикладных областях. Показательным примером является задача решения уравнения действия аддитивной группы кольца вычетов над данными, эквивалентными БФ, при приёме спутникового сигнала ГЛОНАСС. Наибольший интерес представляют разработка и исследование моделей и алгоритмов обработки информации, основывающихся на операциях над классами джевонс-эквивалентных данных. Исследования в этом направлении являются теоретической основой для разработки качественно новых алгоритмов сжатия данных. Исследования операций над джевонс-эквивалентными данными (над джевонс-эквивалентными БФ) позволят также разработать более точные методы распознавая образов. Отдельные направления работ позволят создать методы помехоустойчивого кодирования при условии невозможности добавления избыточности комбинаторными методами (задача восстановления повреждённого спутникового сигнала).

Объект исследования. Джевонс-эквивалентные данные.

Предмет исследования. Анализ джевонс-эквивалентности данных.

Целью диссертационной работы является создание эффективных алгоритмов анализа джевонс-эквивалентности данных и вычисление действующих элементов группы Джевонса.

Поставленная цель достигается путем решения следующих **задач**:

а) найти эффективные представления группы Джевонса, необходимые

для задания её действия на множествах БВ и БФ;

б) исследовать свойства действия группы Джевонса над БВ и БФ;

в) создать алгоритмы решения уравнения действия элемента группы Джевонса над БФ относительно неизвестного действующего элемента;

г) оценить эффективность предложенных алгоритмов и возможность их применения в прикладных задачах.

Соответствие диссертации паспорту специальности. Диссертационная работа соответствует области исследований специальности 05.13.17 – Теоретические основы информатики по п. 5 «Разработка и исследование моделей и алгоритмов анализа данных» и п. 14 «Разработка теоретических основ создания программных систем для новых информационных технологий».

Методы исследования. Основные результаты получены на основе методов теории информации, теории групп, комбинаторного анализа, дискретной математики и высокопроизводительных вычислений.

Научная новизна:

а) найдены два эффективных представления группы Джевонса для задания действия над БВ и БФ, которые позволяют снижать трудозатраты при разработке моделей программных систем, основанных на этом действии;

б) исследованы действия элемента группы Джевонса над БФ, и в результате найдены новые частотные свойства этих действий. Такие свойства позволяют разрабатывать и исследовать алгоритмы анализа данных, основывающиеся на их частотных (энтропийных) характеристиках;

в) найдено новое каноническое представление элемента группы Джевонса, и на его основе создан эффективный алгоритм решения уравнения действия такого элемента над БФ. Он позволяет решить проблему поиска элементов группы, связывающих джевонс-эквивалентные данные;

г) введено новое понятие эквиморфизма групп, доказано эквиморфное вложение группы Джевонса в симметрическую группу степени 2^n. На его основе разработан эквиморфный вычислитель, являющийся моделью архитектуры

процессора, на котором могут создаваться новые программные системы обработки данных. Модель включает в себя эффективные алгоритмы вычисления действия элемента группы Джевонса над БФ.

Теоретическая и практическая значимость работы. Работа носит теоретический характер. Результаты могут быть использованы как непосредственно для определения джевонс-эквивалентности данных, так и для разработки и исследования частотных моделей и алгоритмов обработки информации. Отдельные выводы могут быть использованы для анализа безопасности некоторых криптографических алгоритмов и для генерации специальных данных с одинаковыми частотными (энтропийными) характеристиками **во всех допустимых для них алфавитах**.

Положения, выносимые на защиту диссертационной работы. На защиту выносятся следующие основные результаты:

а) представления группы Джевонса для действия над БВ и БФ;

б) частотные свойства действия элемента группы Джевонса над БФ и метод формирования БВ с одинаковыми частотными (энтропийными) характеристиками **во всех допустимых** для них алфавитах;

в) модель канонического представления элемента группы Джевонса и эффективный алгоритм решения уравнения действия её элемента над БФ;

г) модель эквиморфного вычислителя и его эффективные алгоритмы.

Достоверность результатов работы подтверждается математическими доказательствами основных положений. Эффективность предлагаемых алгоритмов подтверждается результатами, полученными на основе методов спектрального анализа БФ и вычислительных экспериментов.

Апробация результатов работы. Результаты диссертационной работы докладывались автором на следующих международных конференциях:

– Международная конференция, посвящённая памяти В. П. Шункова «Алгебра и логика: теория и приложения» (Красноярск, 2013 г.);

– XVIII Международная конференция «Решетнёвские чтения», посвящён-

ная 90-летию со для рождения генерального конструктора ракетно-космических систем академика М. Ф. Решетнёва (Красноярск, 2014 г.);

– Международная конференция Мальцевские чтения 2014 (Новосибирск, 2014 г.);

– IX Международная конференция «Дискретные модели в теории управляющих систем» (Москва, 2015 г.);

– XX Международная конференция «Решетнёвские чтения» (Красноярск, 2016 г.);

– Международная конференция Мальцевские чтения 2016 (Новосибирск, 2016 г.).

Результаты работы неоднократно обсуждались на семинарах в Сибирском государственном аэрокосмическом университете, Сибирском федеральном университете, а также в Институте математики СО РАН.

Публикации. По результатам диссертационного исследования опубликовано 14 печатных работ, из которых 4 изданы в журналах, рекомендованных ВАК, 8 в тезисах и трудах конференций и 2 свидетельства о регистрации программы, зарегистрированных в Российском реестре программ для ЭВМ. 6 из 14 печатных работ опубликованы в неразделимом соавторстве с научным руководителем А.А. Кузнецовым.

Структура работы. Диссертационная работа состоит из введения, четырёх глав, заключения, списка литературы, списка сокращений и условных обозначений и четырёх приложений.

Во **введении** обоснована актуальность темы диссертационной работы, определены цель и задачи исследования, указаны применяемые в работе методы, представлены основные результаты.

В **главе 1** решается задача выбора конструктивного представления группы Джевонса, необходимого для действий над БВ и БФ, и вводятся основные обозначения. Группа Джевонса, определяемая как внешнее полупрямое произведение своих подгрупп, может быть представлена многими способами, но при

описании действий над БВ и БФ предпочтительнее использовать полупрямое произведение. Такое представление непосредственно отражает целевые задачи, связанные с действием группы Джевонса над булевыми функциями.

Представления группы Джевонса определяется гомоморфизмами внешнего полупрямого произведения, которые различны и могут давать неизоморфные группы (например тождественный гомоморфизм). Для выбора гомоморфизма предлагается вложить группу Джевонса в β_n (подгруппу симметрической группы степени 2^n). Эта подгруппа индуцирует эквивалентное действие на множестве БФ и раскладывается во внутренне полупрямое произведение. Далее из внутреннего автоморфизма определяется внешний для группы Джевонса.

В результате получено два представления группы Джевонса: типа А и типа Б. Типы вычисления А и Б похожи. Преимущество действия типа А заключается в том, что множители не меняют свой порядок при вычислении действия-результата над БВ. При этом сохраняется естественный порядок операций при действии группы подстановок над БВ, но при действии над БФ это нарушается. В свою очередь, тип Б меняет местами множители при вычислении действия-результата над БВ (что нежелательно), но при действии над БФ их перестановки не происходит. В общем случае не определено, что является целевым объектом – БВ или БФ, поэтому несмотря на то, что оба типа выражаются друг через друга, невозможно выбрать какой-то один тип действия как основной, а второй – как сводимый к нему.

Вычисления таких действий трудоёмки, и поэтому предполагается использование инженерно-технических решений (далее – ИТР). Для проверки их корректности приводятся контрольные примеры к основным объектам и операциям. Основные результаты главы 1 опубликованы в [59, 63, 64].

В **главе 2** определяются и исследуются действия группы Джевонса и её подгрупп на множествах БВ и БФ. Выводятся и доказываются правила вычисления композиций таких действий. Вычисление действия группы Джевонса на множестве БФ может быть сведено к действию на множестве эквивалентных

им БВ группой β_n. Вводится новое понятие **эквиморфности групп** – эквивалентности групп, действующих на множестве, относительно их же действия на нём. Доказывается эквиморфизм группы Джевонса и β_n группы.

Исследуются частотные свойства действия группы Джевонса степени n над бинарными векторами длины 2^n, эквивалентными БФ n аргументов. В результате исследования доказано, что эти действия в ряде случаев сохраняют частотные и энтропийные характеристики булевых векторов во **всех допустимых для них алфавитах одновременно**. Такое уникальное свойство действия может использоваться для разработки новых методов анализа алгоритмов обработки информации. Для этого требуется метод генерации БВ с одинаковыми частотными и энтропийными характеристиками. Генерация таких БВ является сложной задачей, поэтому предлагается метод их генерации и приводятся оценки его эффективности. Вычисления действий группы Джевонса над БВ и БФ трудоёмки, и поэтому предполагается использование ИТР. Для проверки их корректности приводятся необходимые контрольные примеры. Основные результаты главы 2 опубликованы в [60, 61, 65, 67].

В **главе 3** приводится формальная постановка основной задачи – решение уравнения действия элемента группы Джевонса над БФ относительно неизвестных действующих элементов. Предлагается эффективный алгоритм решения уравнения, основывающийся на найденном каноническом представлении элемента группы Джевонса. Предлагаемый алгоритм позволяет последовательно находить множители канонического представления неизвестных действующих элементов на основе частотных свойств их действий. Приводятся доказательство корректности алгоритма и способ оценки числа его действий. Для проверки ИТР, реализующих предлагаемый алгоритм, приводятся контрольные примеры, в которых вычисляются решения уравнения для БФ четырёх аргументов и рассматриваемые представления подстановок и элементов группы Джевонса.

Эффективность предлагаемого алгоритма можно существенно повысить с помощью более быстрых методов вычисления действий множителей канони-

ческих представлений искомых решений. Это достигается за счёт архитектуры процессоров и применения эквиморфизмов группы Джевонса и β_n группы. Множители канонического представления элемента группы Джевонса могут содержать отрицание или транспозицию, или отрицание и транспозицию вместе. Для вычисления действий таких элементов разработаны три эффективных алгоритма. Предлагается модель эквиморфного вычислителя, реализующего примитивные операции над БВ: логические умножение и сложение, логические левый и правый сдвиги на число и присвоение. Для алгоритмов выполняется разбиение БВ на подвектора и производится их вычисление так, что каждый подвектор (его значения) обрабатываются одной машинной операцией. Это позволяет повысить эффективность вычислений в сотни раз. Приводятся доказательства корректности алгоритмов эквиморфного вычислителя и расчёт его сложности. Даны методические рекомендации к реализации эквиморфного вычислителя на ИТР. Основные результаты главы 3 опубликованы в [62, 66, 68, 69, 71].

В **главе 4** рассматриваются различные подходы к оценке сложности предлагаемого алгоритма. Приводятся теоретические оценки максимального и минимального числа действий при вычислении решения уравнения. Для практического использования алгоритма этого недостаточно, т.к. опыт показывает, что в подавляющем большинстве случаев число действий составляет n^2+n. Выполнена эмпирическая оценка этого числа для множества конкретных уравнений, отражающих реальные данные. Для более чем $2^{64} \approx 10^{20}$ уравнений были исследованы причины увеличения числа действий выше минимального (n^2+n) и сформулированы предположения о реальной сложности алгоритма, а также о возможности его применения для решения прикладных задач. Исследование проводилось с применением ИТР, основывающихся на специально разработанной библиотеке ***domain object processor*** (или **dop**).

Для БФ с нетривиальной подгруппой инерции в группе Джевонса появление числа действий при решении уравнения больше минимального следует из доказательства корректности алгоритма, но при этом таких БФ подавляю-

щее меньшинство. Поэтому исследование включает в себя: анализ тривиальности подгруппы инерции в группе Джевонса, спектральный анализ всех БФ с тривиальной подгруппой инерции в группе Джевонса для $n = 1, 2, 3, 4, 5$ и статистический анализ числа действий для некоторого количества (миллионов) уравнений при $5 < n < 24$. Для формирования статистики случайные БВ распределены равномерно, потому что реальные данные, в общем случае, также распределены равномерно. В результате исследования выявлено, что число действий при вычислении решения уравнения превосходит n^2+n со статистической вероятностью, не превышающей 10^{-6} . Это позволяет сделать заключение о возможности использования предлагаемых алгоритмов при решении прикладных задач. Основные результаты главы 4 опубликованы в [70, 72].

В **заключении** приведены выводы работы и сформулированы основные результаты.

В **списке сокращений и условных обозначений** содержатся используемые в изложении сокращения и условные обозначения.

В **списке литературы** приведена справочная информация об использованных источниках, а также о публикациях основных результатов.

В **приложении А** содержится справочная подробная статистика классов эквивалентных БФ относительно группы Джевонса и её подгрупп для $n = 1, 2, 3, 4$, включая классы, сдвоенные по отрицанию БФ.

В **приложении Б** приведены справочные каталоги классов эквивалентных БФ относительно группы Джевонса и её подгрупп для $n = 1, 2, 3, 4$, включая классы, сдвоенные по отрицанию БФ. Из-за большого объёма для $n = 4$ не приведены каталоги классов БФ относительно подгрупп группы Джевонса.

В **приложении В** содержатся обязательные сведения о результатах спектрального анализа БФ четырёх и пяти аргументов.

В **приложении Г** приведены обязательные сведения о результатах вычислительных экспериментов. В экспериментах рассчитано число действий при решении уравнения для $5<n<24$ по миллиону экспериментов для каждого n.

Глава 1. Представление группы Джевонса

В главе 1 решается задача выбора конструктивного представления группы Джевонса, необходимого для действий над БВ и БФ, и вводятся основные обозначения. Группа Джевонса, определяемая как внешнее полупрямое произведение своих подгрупп, может быть представлена многими способами, но при описании действий над БВ и БФ предпочтительнее использовать полупрямое произведение. Такое представление непосредственно отражает целевые задачи, связанные с действием группы Джевонса над булевыми функциями.

Представления группы Джевонса определяются гомоморфизмами внешнего полупрямого произведения, которые различны и могут давать неизоморфные группы (например тождественный гомоморфизм). Для выбора гомоморфизма предлагается вложить группу Джевонса в β_n подгруппу симметрической группы степени 2^n. Такая подгруппа индуцирует эквивалентное действие на множестве БФ и раскладывается во внутренне полупрямое произведение. После такого вложения из внутреннего автоморфизма определяется внешний для группы Джевонса. Вычисления таких действий трудоёмки, и поэтому предполагается использование ИТР. Для проверки их корректности приводятся контрольные примеры к основным объектам и операциям.

§ 1.1. Основные обозначения, объекты и операции

Далее по тексту пусть n – целое неотрицательное число, обозначающее количество аргументов БФ и степень группы Джевонса. Мощность множества значений БФ обозначим как $k = 2^n$. Целые неотрицательные индексы обозначим как $i, j \colon i \leqslant n, j < k$. Индексы применяются для описания различных объектов, поэтому иногда их значения могут быть меньше указанных.

Пусть $E = \{0, 1\}$ – множество, состоящее из двух элементов. Декартово произведение этого множества на себя определим как $E^n = \underbrace{E \times \cdots \times E}_{n}$. Например, $E^3 = \{111, 110, 101, 100, 011, 010, 001, 000\}$. Под бинарным вектором длины n будем понимать элемент множества E^n. Для координат множителей

будем использовать классическую числовую нотацию L2R (left to right), т.е. бóльшие координаты находятся левее. Обозначим произвольный элемент такого множества как $x \in E^n, x = \{x_{n-1}, \ldots, x_i, \ldots, x_0\}$. Например, $x \in E^3, x = = \{001\}, x_2 = 0, x_1 = 0, x_0 = 1$.

Зададим операцию над элементами множества E^n как сложение соответственных координат по модулю 2. Пусть $x, y, z \in E_n$ и $z = x \oplus y$ [40], тогда $z = \{x_{n-1} \oplus y_{n-1}, \ldots, x_i \oplus y_i, \ldots, x_0 \oplus y_0\}$. Полученная алгебраическая структура является группой. Во-первых, операция определена так, что всё множество замкнуто относительно применения операции. Во-вторых, из общей ассоциативности сложения следует ассоциативность $\oplus$. В-третьих, нейтральным элементом будет $e = \{0, \ldots, 0, \ldots, 0\}$. В-четвёртых, каждый элемент множества является обратным самому себе, т.к. выполняется сложение по модулю 2. Обозначим множество E^n с операцией $\oplus$ как E_n, это необходимо для семантического разделения сущностей. Будем называть E_n группой инвертирования переменных [4] или группой линейных сдвигов [35]. Дополнительно отметим: $\forall x, y \in E_n$ верно, что $x \oplus y = y \oplus x$, поэтому группа E_n коммутативна или абелева [41, 42].

Подстановкой степени n будем называть объект вида $\pi = \binom{n-1 \ldots 0}{i_{n-1} \ldots i_0}$. Причём в верхней и нижней строках находятся различные числа от 0 до $n-1$. Например, подстановка степени 3: $\pi = \binom{210}{021}$. Подстановка задаёт биективное отображение множества целых неотрицательных чисел от 0 до $n-1$ на себя. В частности, для $\pi = \binom{210}{021}$ будут выполняться следующие отображения: $\pi(2) = 0, \pi(1) = 2, \pi(0) = 1$.

Нотация подстановок выбрана таким образом, чтобы соответствовать индексам БВ. При подготовке исходных данных и интерпретации результатов такой способ не очень удобен для человека, но проведённые несколько тысяч практических вычислений показали эффективность такого представления при решении конкретных задач, связанных с действиями группы Джевонса на множествах БВ и БФ. Под эффективностью понимаются трудозатраты в связке

человек – машина, т.е от формулировки задачи до получения конкретных результатов решений. Был также рассмотрен и традиционный способ задания (записи) подстановок, но практика показала его неэффективность в силу появления путаницы между индексами векторов и значениями подстановки при интерпретации исходных данных и результатов человеком.

Под произведением двух подстановок будем понимать последовательное применение этих подстановок к множеству. Другими словами, результат первой подстановки является исходным значением для второй подстановки. Например, для двух подстановок степени 3: $\pi = \binom{210}{021}$ и $\rho = \binom{210}{201}$ – произведением будет $\nu(2) = \rho(\pi(2)) = \rho(0) = 1, \nu(1) = \rho(\pi(1)) = \rho(2) = 2, \nu(0) = \rho(\pi(0)) = \rho(1) = = 0$ или $\nu = \pi\rho = \binom{210}{120}$.

Подстановка является биективным отображением. Поэтому с каждой подстановкой π можно связать обратную подстановку π^{-1}. Для того, чтобы получить обратную подстановку, нужно поменять строки исходной подстановки местами. Например, для $\pi = \binom{210}{021}$ обратной подстановкой будет $\pi^{-1} = \binom{021}{210} = \binom{210}{102}$. По сути, подстановка является обратимой дискретной функцией на множестве целых неотрицательных чисел от 0 до $n-1$. Результатом произведения подстановки и ей обратной будет нейтральный элемент (или тривиальная подстановка) $e = \binom{n-1n-2\ldots10}{n-1n-2\ldots10}$. Всё множество подстановок степени n с операцией умножения обозначим как S_n и будем называть симметрической группой [43] или группой перестановок переменных [35]. Группа S_n для $n > 2$ не является абелевой, хотя в ней присутствуют конкретные пары π, ρ, для которых верно $\pi\rho = \rho\pi$. Более подробно о групповых свойствах S_n в [43].

Резюме. Задано две группы E_n и S_n, и их порядки равны 2^n и $n!$ соответственно.

Для проверки ИТР предлагаются следующие контрольные примеры. Для группы инвертирования переменных: $x, y \in E_4$, $x = \{0011\}$, $y = \{0010\}$, $x \oplus y = = \{0001\}$. Для группы подстановок: $\pi, \rho \in S_4$, $\pi = \binom{3210}{2103}$, $\rho = \binom{3210}{1023}$, $\pi^{-1} = = \binom{3210}{0321}$, $\rho^{-1} = \binom{3210}{0132}$, $\pi\rho = \binom{3210}{0231}$, $\rho\pi = \binom{3210}{0312}$, $(\pi\rho)^{-1} = \rho^{-1}\pi^{-1} = \binom{3210}{1203}$,

$(\rho\pi)^{-1} = \pi^{-1}\rho^{-1} = \binom{3210}{2013}$.

Подстановки подобраны таким образом, чтобы их порядки, порядки их произведений были больше 2 и результирующие подстановки (правые и левые произведения, отрицания и их правые и левые произведения) не совпадали. Далее по тексту эти подстановки будут использоваться в контрольных примерах.

§ 1.2. Действие группы подстановок на множестве БВ

Группа подстановок S_n может действовать на множестве БВ путём перестановки её координат, но такое действие можно задать по-разному. Как будет показано далее, в зависимости от определения правила действия элемента симметрической группы над БВ будут формироваться различные результаты. Помимо действия над БВ, можно задать действие элемента симметрической группы над БФ [4, 35]. Далее рассмотрим два набора правил вычисления действия группы S_n над БВ. Обозначим их как тип А и тип Б и сопоставим свойства обоих типов.

Действием типа А элемента группы $\pi \in S_n$ над БВ $x \in E^n$ будем называть вычисление результата $x' \in E^n$: $x' = x^\pi$ по следующему правилу: в верхней строке подстановки находятся «старые» индексы, а в нижней – «новые», или в символьном виде:

$$x'_{\pi(i)} = x_i. \qquad (1.1^{\text{А}})$$

Действием типа Б элемента группы $\pi \in S_n$ над БВ $x \in E^n$ будем называть вычисление результата $x' \in E^n$: $x' = x^\pi$ по следующему правилу: в верхней строке подстановки находятся «новые» индексы, а в нижней – «старые», или в символьном виде:

$$x'_i = x_{\pi(i)}. \qquad (1.1^{\text{Б}})$$

Примем за основу следующее суждение: формулируемые правила вывода сохраняют классические математические объекты, в частности произведения (суммы) элементов внутри групп, и **только при действиях симметрической группы и группы Джевонса над БВ и БФ** правила вычисления

могут становиться неестественными. Тогда сформулируем правила композиций действия нескольких подстановок над БВ по типу А и по типу Б.

Лемма 1.1$^{\text{А}}$ (*О действии типа А*). *Если подстановки* $\pi, \rho \in S_n$ *действуют последовательно (*π *и затем* ρ*) над элементом* $x \in E^n$*, то результат действия эквивалентен действию подстановки-произведения* $\pi\rho$*, или в символьном виде* $(x^\pi)^\rho = x^{(\pi\rho)}$.

Доказательство. Определим $x' = x^\pi$ и $x'' = (x')^\rho$, и пусть $i' = \pi(i)$. Тогда по формуле (1.1$^{\text{А}}$) получим $x'_{\pi(i)} = x_i = x'_{i'}$ и подставим в $x''_{\rho(i')} = x'_{i'}$. Последнее соотношение также отражает формулу (1.1$^{\text{А}}$) – независимо от того, какой символ выбран для индекса. Тогда вычислим $x''_{\rho(\pi(i))} = x'_{\pi(i)} = x_i = x''_{(\pi\rho)(i)}$, или при переходе от индексной к векторной форме записи получим $(x^\pi)^\rho = x^{(\pi\rho)}$. Что и требовалось доказать. □

Лемма 1.1$^{\text{Б}}$ (*О действии типа Б*). *Если подстановки* $\pi, \rho \in S_n$ *действуют последовательно (*π *и затем* ρ*) над элементом* $x \in E^n$*, то результат действия эквивалентен действию подстановки-произведения* $\rho\pi$*, или в символьном виде* $(x^\pi)^\rho = x^{(\rho\pi)}$.

Доказательство. Определим $x' = x^\pi$ и $x'' = (x')^\rho$, и пусть $i' = \rho(i)$. Тогда по формуле (1.1$^{\text{Б}}$) получим $x''_i = x'_{\rho(i)} = x'_{i'}$ и подставим в $x'_{i'} = x_{\pi(i')}$. Последнее соотношение так же отражает формулу (1.1$^{\text{Б}}$) – независимо от того, какой символ выбран для индекса. Тогда вычислим $x''_i = x'_{i'} = x_{\pi(i')} = x_{\pi(\rho(i))} = x_{(\rho\pi)(i)}$, или при переходе от индексной к векторной форме записи получим $(x^\pi)^\rho = x^{(\rho\pi)}$. Что и требовалось доказать. □

Типы вычисления А и Б похожи. Преимущество действия типа А заключается в том, что множители не меняют свой порядок при вычислении действия-результата над БВ. При этом сохраняется естественный порядок операций при действии группы подстановок над БВ, но при действии над БФ это нарушается. В свою очередь, тип Б меняет местами множители при вычислении действия-результата над БВ (что нежелательно), но при действии над БФ их перестановки не происходит. В общем случае не определено, что является целевым объ-

ектом – БВ или БФ, поэтому, несмотря на то, что оба типа выражаются друг через друга, невозможно выбрать какой-то один тип действия как основной, а второй как сводимый к нему.

Так как в одном выражении указываются как групповые операции, так и действия, например, $x^{\pi\rho}$, то возникает неоднозначность в приоритете выполнения операций. Для определённости примем, что действие имеет минимальный приоритет, т.е. для $x^{\pi\rho}$ нужно сначала вычислить произведение $\pi\rho$, а только затем действие над x результатом произведения. Если необходим другой порядок выполнения операций, то условимся использовать скобки для изменения приоритета. Например, $(x^{\pi})^{\rho}$ обозначает последовательное применение действий, сначала π над БВ, а затем ρ над результатом первого действия.

Элементы симметрической группы действуют не только на множестве БВ, но и на группе E_n в целом, причём такое действие реализует автоморфное отображение группы E_n.

Теорема 1.1 (*Об автоморфизме*). *Отображение* $E_n^{\pi} \to E_n, \forall\pi \in S_n$ *есть автоморфизм – независимо от типа действия А или Б.*

Доказательство. Сначала докажем гомоморфность, а затем биективность. Пусть $x, y, z \in E_n\colon z = x \oplus y$, тогда если отображение – автоморфизм, то верно $z^{\pi} = x^{\pi} \oplus y^{\pi}$.

Применим действие к компоненту i левой части $(z_i)^{\pi}$. Оно раскроется по типу А как $z_{\pi(i)}$ и по типу Б как $z_{\pi^{-1}(i)}$. Из определения внутригрупповой операции в E_n имеем $z_i = x_i \oplus y_i$, тогда получим для типа А соотношение $x_{\pi(i)} \oplus y_{\pi(i)}$, а для типа Б — $x_{\pi^{-1}(i)} \oplus y_{\pi^{-1}(i)}$. Перейдём к унифицированной форме действия (в виде леммы $1.1^{\text{А}}$ или в виде леммы $1.1^{\text{Б}}$) как $(z_i)^{\pi} = (x_i)^{\pi} \oplus (y_i)^{\pi}$. Для типа А это верно по определению, а для типа Б верно из $\forall\pi\exists!\pi^{-1}\colon \pi\pi^{-1} = \pi^{-1}\pi = e_S$, откуда заключаем, что отображение сохраняет операцию независимо от типа А или Б.

Из общей алгебры верно [41], что любая подстановка порождается транспозициями, и даже транспозициями вида $(0, i)$. Рассмотрим, как действует на

всё множество E^n такая транспозиция. Разобьем всё множество группы E_n на классы по следующему правилу. Значения координат БВ внутри каждого класса совпадают, кроме координат 0 и i. В каждом таком классе будет по четыре вектора, а всего классов 2^{n-2}. Транспозиция переставляет координаты 0 и i, поэтому её действие будет локализовано внутри классов. Значения координат, которыми отличаются вектора внутри класса, являются: 00, 01, 10 и 11. В случае 00 и 11 отображение будет тривиально. В случае 01 и 10 векторы будут отображаться друг в друга, откуда заключаем, что транспозиция отображает E_n биективно на себя. Тогда для типа А по лемме $1.1^{\text{А}}$ заключаем, что $E_n^\pi \to E_n$ биекция. Для типа Б по лемме $1.1^{\text{Б}}$ транспозиции, образующие π, будут действовать в обратном порядке, но будут биекциями, т.е. по типу Б отображение $E_n^\pi \to E_n$ тоже биекция. Следовательно, отображение $E_n^\pi \to E_n, \forall \pi \in S_n$ биекция, сохраняющая операцию независимо от типа действия А или Б. Что и требовалось доказать. □

§ 1.3. Контрольные примеры действия подстановок над БВ

Для демонстрации леммы $1.1^{\text{А}}$ и леммы $1.1^{\text{Б}}$ покажем действие подстановок над БВ $x \in E^4$ в общем виде. Для этого вычислим x^π, x^ρ, $(x^\pi)^\rho$, $(x^\rho)^\pi$, $x^{\pi\rho}$, $x^{\rho\pi}$ и действия отрицательных подстановок $x^{\pi^{-1}}$, $x^{\rho^{-1}}$, $\left(x^{\pi^{-1}}\right)^{\rho^{-1}}$, $\left(x^{\rho^{-1}}\right)^{\pi^{-1}}$, $x^{(\pi\rho)^{-1}}$, $x^{(\rho\pi)^{-1}}$, $x^{\pi^{-1}\rho^{-1}}$, $x^{\rho^{-1}\pi^{-1}}$ для обоих типов.

Для типа А выполним действие над x. Пусть $x^\pi = x'$, откуда по формуле $(1.1^{\text{А}})$ для $\pi = \binom{3210}{2103}$ и $x'_{\pi(i)} = x_i$ получим:

$$x'_{\pi(3)} = x'_2 = x_3,$$
$$x'_{\pi(2)} = x'_1 = x_2,$$
$$x'_{\pi(1)} = x'_0 = x_1,$$
$$x'_{\pi(0)} = x'_3 = x_0.$$

В результате получим $x' = x^\pi = \{x_0, x_3, x_2, x_1\}$. На позициях, соответствующих нижней строке подстановки, находятся координаты, индексы которых соответствуют верхней строке подстановки. Это позволяет использовать «быстрый счёт». Вычислим «быстро» остальные подстановки:

$$\rho = \binom{3210}{1023} : x^{\rho} = \{x_0, x_1, x_3, x_2\},$$
$$\pi^{-1} = \binom{3210}{0321} : x^{\pi^{-1}} = \{x_2, x_1, x_0, x_3\},$$
$$\rho^{-1} = \binom{3210}{0132} : x^{\rho^{-1}} = \{x_1, x_0, x_2, x_3\},$$
$$\pi\rho = \binom{3210}{0231} : x^{\pi\rho} = \{x_1, x_2, x_0, x_3\},$$
$$\rho\pi = \binom{3210}{0312} : x^{\rho\pi} = \{x_2, x_0, x_1, x_3\}.$$

Далее аналогично подействуем отрицательными произведениями. При построении этих действий важно понимать, что лемма 1.1^{A} на них не распространяется, потому что выполняется **только одно** действие над БВ (лемма 1.1^{A} определяет композицию действий, т.е. более чем одно действие), а наличие более чем одной подстановки определяется групповым разложением отрицательного элемента:

$$(\pi\rho)^{-1} = \rho^{-1}\pi^{-1} = \binom{3210}{1203} : x^{(\pi\rho)^{-1}} = x^{\rho^{-1}\pi^{-1}} = \{x_0, x_2, x_3, x_1\},$$
$$(\rho\pi)^{-1} = \pi^{-1}\rho^{-1} = \binom{3210}{2013} : x^{(\rho\pi)^{-1}} = x^{\pi^{-1}\rho^{-1}} = \{x_0, x_3, x_1, x_2\}.$$

При вычислении композиций действий использовать «быстрый счёт» нецелесообразно. Из-за наличия трёх наборов индексов (исходные индексы, индексы промежуточного результата и конечные индексы) возникает путаница. Пусть $(x^{\pi})^{\rho} = x'', x^{\pi} = x'$, тогда формула (1.1^{A}) примет вид $x''_{\rho}(i) = x'_i$, и по ранее вычисленным значениям из $x' = x^{\pi} = \{x_0, x_3, x_2, x_1\}$ и $\rho = \binom{3210}{1023}$ имеем:

$$x''_{\rho(3)} = x''_1 = x'_3 = x_0,$$
$$x''_{\rho(2)} = x''_0 = x'_2 = x_3,$$
$$x''_{\rho(1)} = x''_2 = x'_1 = x_2,$$
$$x''_{\rho(0)} = x''_3 = x'_0 = x_1.$$

В результате получим $x'' = \{x_1, x_2, x_0, x_3\}$. Далее непосредственно заключаем, что $(x^{\pi})^{\rho} = x^{\pi\rho}$, что верно по лемме 1.1^{A}. Для остальных композиций дадим лишь результаты:

$$(x^{\rho})^{\pi} = \{x_2, x_0, x_1, x_3\} = x^{\rho\pi},$$
$$\left(x^{\pi^{-1}}\right)^{\rho^{-1}} = \{x_0, x_3, x_1, x_2\} = x^{\pi^{-1}\rho^{-1}},$$
$$\left(x^{\rho^{-1}}\right)^{\pi^{-1}} = \{x_0, x_2, x_3, x_1\} = x^{\rho^{-1}\pi^{-1}}.$$

При вычислении более чем одного действия рекомендуется использовать

либо лемму 1.1[А] в паре с «быстрым счётом», либо ИТР. Если рекомендацию невозможно выполнить, то целесообразно дописать индексы в промежуточном результате. Такое дополнение помогает избежать ошибок. Например, используя «быстрый счёт», найти $(x^{\pi})^{\rho}$, если $x^{\pi} = \left\{ \overset{3}{x_0}, \overset{2}{x_3}, \overset{1}{x_2}, \overset{0}{x_1} \right\}$ и $\rho = \binom{3210}{1023}$, то $(x^{\pi})^{\rho} = \{x_1, x_2, x_0, x_3\} = x^{\pi\rho}$.

Для типа Б выполним действие над x. Пусть $x^{\pi} = x'$, откуда по формуле (1.1[Б]) для $\pi = \binom{3210}{2103}$ и $x'_i = x_{\pi(i)}$ получим:

$$x'_3 = x_{\pi(3)} = x_2,$$
$$x'_2 = x_{\pi(2)} = x_1,$$
$$x'_1 = x_{\pi(1)} = x_0,$$
$$x'_0 = x_{\pi(0)} = x_3.$$

В результате получим $x' = x^{\pi} = \{x_2, x_1, x_0, x_3\}$. Отметим, что порядок следования компонентов соответствует верхней строке подстановки π. Это позволяет использовать «быстрый счёт». Вычислим «быстро» остальные подстановки:

$$\rho = \tbinom{3210}{1023} : x^{\rho} = \{x_1, x_0, x_2, x_3\},$$
$$\pi^{-1} = \tbinom{3210}{0321} : x^{\pi^{-1}} = \{x_0, x_3, x_2, x_1\},$$
$$\rho^{-1} = \tbinom{3210}{0132} : x^{\rho^{-1}} = \{x_0, x_1, x_3, x_2\},$$
$$\pi\rho = \tbinom{3210}{0231} : x^{\pi\rho} = \{x_0, x_2, x_3, x_1\},$$
$$\rho\pi = \tbinom{3210}{0312} : x^{\rho\pi} = \{x_0, x_3, x_1, x_2\}.$$

Далее аналогично подействуем отрицательными произведениями. При построении этих действий важно понимать, что лемма 1.1[Б] на них не распространяется, потому что выполняется **только одно** действие над БВ (лемма 1.1[Б] определяет композицию действий, т.е. более чем одно действие), а наличие более чем одной подстановки определяется групповым разложением отрицательного элемента:

$$(\pi\rho)^{-1} = \rho^{-1}\pi^{-1} = \tbinom{3210}{1203} : x^{(\pi\rho)^{-1}} = x^{\rho^{-1}\pi^{-1}} = \{x_1, x_2, x_0, x_3\},$$
$$(\rho\pi)^{-1} = \pi^{-1}\rho^{-1} = \tbinom{3210}{2013} : x^{(\rho\pi)^{-1}} = x^{\pi^{-1}\rho^{-1}} = \{x_2, x_0, x_1, x_3\}.$$

При вычислении композиций действий использовать «быстрый счёт» неце-

лесообразно. Из-за наличия трёх наборов индексов (исходные индексы, индексы промежуточного результата и конечные индексы) возникает путаница. Пусть $(x^\pi)^\rho = x'', x^\pi = x'$, тогда формула ($1.1^{\text{Б}}$) примет вид $x''_i = x'_{\pi(i)}$, и по ранее вычисленным значениям из $x' = x^\pi = \{x_2, x_1, x_0, x_3\}$ и $\rho = \binom{3210}{1023}$ имеем:

$$x''_3 = x'_{\rho(3)} = x'_1 = x_0,$$
$$x''_2 = x'_{\rho(2)} = x'_0 = x_3,$$
$$x''_1 = x'_{\rho(1)} = x'_2 = x_1,$$
$$x''_0 = x'_{\rho(0)} = x'_3 = x_2.$$

В результате получим $x'' = \{x_0, x_3, x_1, x_2\}$. Далее непосредственно заключаем, что $(x^\pi)^\rho = x^{\rho\pi}$, что верно по лемме $1.1^{\text{Б}}$. Для остальных композиций дадим лишь результаты:

$$(x^\rho)^\pi = \{x_0, x_2, x_3, x_1\} = x^{\pi\rho},$$
$$\left(x^{\pi^{-1}}\right)^{\rho^{-1}} = \{x_1, x_2, x_0, x_3\} = x^{\rho^{-1}\pi^{-1}},$$
$$\left(x^{\rho^{-1}}\right)^{\pi^{-1}} = \{x_2, x_0, x_1, x_3\} = x^{\pi^{-1}\rho^{-1}}.$$

При вычислении более чем одного действия рекомендуется использовать либо лемму $1.1^{\text{Б}}$ в паре с «быстрым счётом», либо ИТР. Если рекомендацию невозможно выполнить, то целесообразно дописать индексы в промежуточном результате. Такое дополнение помогает избежать ошибок. Например, используя «быстрый счёт», найти $(x^\pi)^\rho$, если $x^\pi = \left\{\overset{3}{x_2}, \overset{2}{x_1}, \overset{1}{x_0}, \overset{0}{x_3}\right\}$ и $\rho = \binom{3210}{1023}$, то $(x^\pi)^\rho = \{x_0, x_3, x_1, x_2\} = x^{\rho\pi}$.

В качестве сравнительной характеристики типов действий А и Б можно отметить следующее. Тип Б более пригоден для «быстрого счёта» при непосредственном вычислении композиций действий. В то же время, в силу специфики леммы $1.1^{\text{Б}}$ (не сохраняет естественный порядок множителей), если требуется аналитический вывод соотношений, более предпочтителен тип действий А. Результаты типов действий А и Б связаны как взаимнообратные и по итоговой подстановке, и по промежуточному результату. Всякое действие, выполненное по типу А, есть действие, выполненное по типу Б, но с обратной подстановкой, – как полностью, так и частично. Например, $(x^\pi)^\rho = x^{\pi\rho} = \{x_1, x_2, x_0, x_3\}$

по типу А эквивалентно действию обратной подстановки по типу Б, т.е. для $(\pi\rho)^{-1} = \rho^{-1}\pi^{-1}$: $x^{\rho^{-1}\pi^{-1}} = \{x_1, x_2, x_0, x_3\} = \left(x^{\pi^{-1}}\right)^{\rho^{-1}}$. Это верно и для промежуточных результатов: $(x^{\pi})^{\rho}$ для типа А эквивалентно действию $\left(x^{\pi^{-1}}\right)^{\rho^{-1}}$ по типу Б.

§ 1.4. Выбор представления группы Джевонса

Группа E_n также может действовать на множестве БВ. Сам БВ длины n является элементом группы E_n. Тогда определим результат действия этой группы на БВ как результат групповой операции исходного вектора и некоторого действующего элемента E_n, а именно положим: $x' = x^z$, где $x, x' \in E^n$ – БВ и $z \in E_n$ – действующий элемент, $x' = x \oplus z$. Действие, записанное в виде показателя, используется прежде всего для семантики объектов, т.е. чтобы разделить исходные значения и действия над ними. Такая форма записи также позволяет использовать единообразное описание действий над БВ. Далее по тексту примем, что если используется латинский алфавит, то речь идёт об элементах E_n, а если греческий – об элементах S_n.

Рассмотрим более детально группы E_n и S_n и то, как элементы этих групп дают способы преобразования БВ. В специальной литературе [4, 35] можно найти упоминания (либо без указания конкретного гомоморфизма, либо с указанием только одного) о том, что эти группы могут быть объединены в более крупную группу – группу Джевонса D_n. Классически группа Джевонса определяется как полупрямое произведение групп $E_n \leftthreetimes S_n$ [4]. Определение группы Джевонса сводится к тому, что элемент группы Джевонса есть совместное действие всех возможных отрицаний БВ (действие элемента E_n, по сути, не что иное, как выполнение операции отрицания над частями вектора) и всех возможных перестановок элементов вектора. В работе [4] дано именно такое определение. Там же группа Джевонса представляется как группа, действующая на множестве БФ. Как будет показано далее, существуют трудности использования такого задания (представления).

Одной из таких трудностей является перестановочность элементов в произведении (аналогично лемме 1.1[Б]). Трудности, возникающие при вычислении произведений в лемме 1.1[Б], могут быть решены переопределением самого действия, но для БФ трудность перестановочности множителей является следствием самой природы БФ, а не описанием. По этой причине определение из [4] не может использоваться в настоящем изложении.

Второй трудностью является сам способ задания группы Джевонса. Она заключается в том, что внешнее полупрямое произведение групп может быть задано многими способами, и в результате давать различные (неизоморфные между собой, например – прямое произведение) группы [41]. Рассмотрим классическое определение внешнего полупрямого произведения некоторых групп N и H. Определим операцию для двух элементов группы-произведения (n_0, h_0) и (n_1, h_1), где $n_0, n_1 \in N$ и $h_0, h_1 \in H$ [41]:

$$(n_0, h_0) \circ (n_1, h_1) = (n_0 \psi_{h_0}(n_1), h_0 h_1). \tag{1.2}$$

Здесь $\psi_{h_0}(n_1)$ – автоморфный образ элемента n_1, причём гомоморфизм зависит от элемента h_0. И в зависимости от выбора гомоморфизма ψ могут быть получены различные группы-произведения, в том числе вырожденный случай – прямое произведение (ψ – тождественно). Полученные различные полупрямые произведения могут называться группой Джевонса, т.к. для внешнего полупрямого произведения выбор конкретного ψ – это вопрос задания. Отсюда заключаем, что нужны основания для выбора конкретного ψ для реализации действий группы Джевонса на множествах БВ и БФ.

Одним из таких оснований является связь двух групп по действию над вектором. Далее покажем на примере, что исключительно действие над вектором не позволяет выбрать гомоморфизм. Рассмотрим уравнение $x^\pi = x'$, где $x, x' \in E^n, \pi \in S_n$. Решить это уравнение относительно π – значит найти все решения или показать, что их нет. Рассмотрим случай, при котором нет решений. Так как x, x' – векторы одинаковой длины, а π меняет местами элементы вектора, то для наличия решений необходимо и достаточно, чтобы они содер-

жали равное число нулей и единиц. Поэтому не имеет смысла рассматривать случаи отсутствия решений. Если же уравнение разрешимо относительно π, то можно построить эквивалентное уравнение $x^z = x'$, где $z \in E_n$, т.к. элементы x, x' множества E^n являются и элементами группы E_n, а потому такие уравнения всегда разрешимы. Другими словами, всякое действие группы S_n сводимо к действию E_n. Поэтому относительно действия групп E_n и S_n на множестве E^n ни одно определение ψ не конструктивно для целевой задачи. Основания выбора ψ для настоящего изложения – действия над БФ.

Из теоремы 1.1 следует, что действие элемента группы S_n по формуле ($1.1^{\text{А}}$) или по формуле ($1.1^{\text{Б}}$) на всю группу E_n есть автоморфизм. Но отображение $E_n^{\pi} \to E_n, \forall \pi \in S_n$ не является автоморфизмом для искомого гомоморфизма ψ в произведении (1.2), т.к. действие группы Джевонса над БФ с таким гомоморфизмом будет некорректно.

Сначала рассмотрим искомый гомоморфизм абстрактно, а после дадим конкретные вычислительные формулы и доказательства. Группа Джевонса индуцирует действие на множестве БФ так, что всё множество БФ разбивается на непересекающиеся классы. Для этого определим некоторую группу β_n, которая индуцирует на множестве БФ действие, эквивалентное действию группы Джевонса, т.е. разбивает всё множество БФ на такие же непересекающиеся классы. Пусть также группа β_n содержит элементы одной природы и раскладывается во внутреннее полупрямое произведение своих подгрупп: $\beta_n = B_n \leftthreetimes T_n$. Произведение указанных групп внутреннее, поэтому гомоморфизм из произведения (1.2) будет тоже внутренним. Он будет задаваться сопряжениями элементов естественно. Тогда пусть существуют биекции (необязательно изоморфизмы) $E_n \to B_n$, $S_n \to T_n$ и $D_n \to \beta_n$. Примем в качестве оснований выбора гомоморфизма, что внешний гомоморфизм группы Джевонса и внутренний группы β_n эквивалентны. Термины «биекция» применяются вместо изоморфизма потому, что, как будет показано далее, наряду с изоморфными вложениями групп появляются и антиизоморфные. Антиизоморфные вложения не нарушают тре-

бование разбиения множества БФ на непересекающиеся классы, эквивалентные разбиению с помощью группы Джевонса, поэтому допустимы.

В результате таких построений получится группа, которая задаётся независимо от БФ и явно с ними не связана, но в то же время индуцирует такое же действие, как и группа Джевонса. Её действия на БВ и БФ будут задаваться независимо от них. Причём правила вычисления действий вполне могут нарушать классические групповые соотношения, так же как в лемме 1.1Б. Перейдём к конкретному описанию группы β_n и к обоснованию вышеописанных требований. Сначала дадим некоторые опорные суждения.

Сопоставим с каждым элементом множества E^n некоторое неотрицательное целое число. Число и вектор будем обозначать одинаковыми символами, т.к. БВ, по сути, есть двоичная форма записи искомого числа [44]:

$$\forall x \in E^n, \exists! x \in \mathbb{Z}_+ : x = \sum_{i=n-1}^{0} x_i \cdot 2^i. \tag{1.3}$$

Так, например, $x \in E^4 : x = \{0011\}$, получим $x = 0{\cdot}2^3{+}0{\cdot}2^2{+}1{\cdot}2^1{+}1{\cdot}2^0 = 3$. Или обратно: $x \in \mathbb{Z}_+ : x = 5$, получим $x{=}4{+}1{=}0{\cdot}8{+}1{\cdot}4{+}0{\cdot}2{+}1{\cdot}1{=}\{0101\}$.

Отображение (1.3) является биекцией и верно $0 \leqslant x < k$. Порядок индексов определяется в единой нотации L2R. Тогда определим действие элементов группы E_n и S_n над элементами множества $\mathbb{Z}_+$ по аналогии с соответствующими им БВ.

Действие элемента группы $z \in E_n$ на $x \in E^n$ в виде (1.3) можно записать следующим образом:

$$x^z = \sum_{i=n-1}^{0} (x_i \oplus z_i) \cdot 2^i. \tag{1.4}$$

При этом нет необходимости перехода к вектору. В свою очередь, для действия элемента группы $\pi \in S_n$ в зависимости от типа действия по формуле (1.1А) или по формуле (1.1Б) в виде (1.3) получим:

$$x^\pi = \sum_{i=n-1}^{0} x_{\pi^{-1}(i)} \cdot 2^i = \sum_{i=n-1}^{0} x_i \cdot 2^{\pi(i)}; \tag{1.5А}$$

$$x^\pi = \sum_{i=n-1}^{0} x_{\pi(i)} \cdot 2^i = \sum_{i=n-1}^{0} x_i \cdot 2^{\pi^{-1}(i)}. \tag{1.5Б}$$

Действие типа A неудобно для «быстрого счёта» и для записи в виде действия на БВ, но правая часть формулы (1.5^{A}) позволяет решать это. Определим:

$$\varphi_z(j) = j^z, \forall z \in E_n; \tag{1.6}$$

$$\varphi_\pi(j) = j^\pi, \forall \pi \in S_n. \tag{1.7}$$

Так как j пробегает все значения от 0 до $k-1$ и j^z – биекция как групповая операция в E_n, а j^π – биекция, согласно теореме 1.1, то отображения φ_z и φ_π сами являются биекциями множества чисел от 0 до $k-1$ на себя. Другими словами, φ_z и φ_π – подстановки симметрической группы S_k. Обозначим множество элементов φ_z как B_n и множество элементов φ_π как T_n. Покажем, что эти отображения – биекции и сохраняют операцию (включая антиизоморфизмы).

Теорема 1.2 (*Об изоморфизме* B_n). *Отображение вида* (1.6) $E_n \to B_n, z \in E_n, \varphi_z \in B_n \colon \varphi_z(j) = j^z$ *есть изоморфизм.*

Доказательство. Сохранение операции показывается непосредственно из произведения подстановок. Пусть $z_0, z_1 \in E_n$, тогда вычислим $\varphi_{z_0}\varphi_{z_1}$. Из правил перемножения подстановок имеем $(\varphi_{z_0}\varphi_{z_1})(j) = \varphi_{z_1}(\varphi_{z_0}(j)) = \varphi_{z_1}(j^{z_0}) = (j^{z_0})^{z_1} = j^{z_0 z_1} = \varphi_{z_0 z_1}(j)$, или $\varphi_{z_0}\varphi_{z_1}{=}\varphi_{z_0 z_1}$. Отсюда заключаем, что операция сохраняется. Из формулы (1.6) следует, что для любого $z{\in}E_n$ найдётся образ. Тогда покажем, что у такого образа будет только один прообраз. Будем вести доказательство от обратного. Пусть $z_0{\neq}z_1$ и $\varphi_{z_0}{=}\varphi_{z_1}$ или $\varphi_{z_0}(j){=}\varphi_{z_1}(j), \forall j{\in}E^n$, откуда перейдём к тождеству $j^{z_0} = j^{z_1} \Rightarrow j \oplus z_0 = j \oplus z_1$, которое будем преобразовывать внутри группы E_n. Тогда верно $j \oplus j \oplus z_0 = j \oplus j \oplus z_1 \Rightarrow z_0 = z_1$, откуда заключаем противоречие. Следовательно, отображение (1.6) – биекция, и сохраняет операцию. Что и требовалось доказать. □

Из теоремы 1.2 заключаем, что $B_n < S_k$ – изоморфное вложение группы E_n в S_k. Полное отображение вектора в подстановку представим как:

$$\varphi_z = \begin{pmatrix} 2^n - 1 & \dots & j & \dots & 0 \\ \sum\limits_{i=n-1}^{0} \overline{z_i} \cdot 2^i & \dots & \sum\limits_{i=n-1}^{0} (j_i \oplus z_i) \cdot 2^i & \dots & \sum\limits_{i=n-1}^{0} z_i \cdot 2^i \end{pmatrix}. \tag{1.8}$$

Первый и последний элементы могут быть заданы явно, остальные рассчитываются через j.

Теорема 1.3 (*Об изоморфизме* T_n). *Отображение вида* (1.7) $S_n \to T_n, \pi \in S_n, \varphi_\pi \in T_n\colon \varphi_\pi(j) = j^\pi$ *есть изоморфизм для типа действия А и антиизоморфизм для типа действия Б.*

Доказательство. Сохранение операции показывается непосредственно из произведения подстановок. Пусть $\pi_0, \pi_1 \in S_n$, тогда вычислим $\varphi_{\pi_0}\varphi_{\pi_1}$. Из правил перемножения подстановок имеем $(\varphi_{\pi_0}\varphi_{\pi_1})(j) = \varphi_{\pi_1}(\varphi_{\pi_0}(j)) = = \varphi_{\pi_1}(j^{\pi_0}) = (j^{\pi_0})^{\pi_1}$. Далее по типу А согласно формуле (1.1$^{\text{А}}$) имеем $(j^{\pi_0})^{\pi_1} = = j^{\pi_0\pi_1} = \varphi_{\pi_0\pi_1}(j)$ или $\varphi_{\pi_0}\varphi_{\pi_1} = \varphi_{\pi_0\pi_1}$, и для типа Б согласно формуле (1.1$^{\text{Б}}$) имеем $(j^{\pi_0})^{\pi_1} = j^{\pi_1\pi_0} = \varphi_{\pi_1\pi_0}(j)$ или $\varphi_{\pi_0}\varphi_{\pi_1} = \varphi_{\pi_1\pi_0}$, откуда заключаем, что операция сохраняется, но для типа Б приводит к перестановке образов. Из формулы (1.7) следует, что для любого $\pi \in S_n$ найдётся образ. Тогда покажем, что у такого образа будет только один прообраз. Будем вести доказательство от обратного. Пусть $\pi_0 \neq \pi_1$ и $\varphi_{\pi_0} = \varphi_{\pi_1}$ или $\varphi_{\pi_0}(j) = \varphi_{\pi_1}(j), \forall j \in E^n$. Отсюда перейдём к тождеству $j^{\pi_0} = j^{\pi_1}$, которое будем преобразовывать внутри группы T_n. Тогда верно $(j^{\pi_0})^{\pi_1^{-1}} = (j^{\pi_1})^{\pi_1^{-1}} \Rightarrow (j^{\pi_0})^{\pi_1^{-1}} = j$. Переходя к компонентам j по формуле (1.1$^{\text{А}}$) или по формуле (1.1$^{\text{Б}}$), получим, что $\left(\pi_0\pi_1^{-1}\right)(i) = i$ или $\left(\pi_1^{-1}\pi_0\right)(i) = i$. То есть независимо от типа действия получаем тривиальную подстановку и, как следствие, $\pi_0 = \pi_1$, откуда заключаем противоречие. Следовательно, отображение (1.7) – биекция, и сохраняет операцию, но по типу Б приводит к перестановке образов. Что и требовалось доказать. □

Из теоремы 1.3 заключаем, что $T_n < S_k$ изоморфное (для типа Б антиизоморфное) вложение группы S_n в S_k. Полное отображение подстановки в подстановку запишем в следующем виде для типов А и Б соответственно:

$$\varphi_\pi = \begin{pmatrix} 2^n-1 & \dots & j & \dots & 0 \\ 2^n-1 & \dots & \sum\limits_{i=n-1}^{0} j_i \cdot 2^{\pi(i)} & \dots & 0 \end{pmatrix}; \qquad (1.9^{\text{А}})$$

$$\varphi_\pi = \begin{pmatrix} 2^n-1 & \dots & j & \dots & 0 \\ 2^n-1 & \dots & \sum\limits_{i=n-1}^{0} j_{\pi(i)} \cdot 2^{i} & \dots & 0 \end{pmatrix}. \qquad (1.9^{\text{Б}})$$

Первый и последний элементы могут быть заданы явно, остальные рассчитываются через j.

Резюме. Определено две группы B_n и T_n, которые являются подгруппами в S_k.

Сконструируем множество β_n как произведения (по групповой операции S_k) всех возможных элементов указанных групп в любых порядках. Для определённости примем, что сначала указывается элемент $b \in B_n$, а затем $t \in T_n$ (далее будет показано, что произведения в обратном порядке сводимы к указанному). Элемент множества β_n запишем как (bt).

Теорема 1.4 (*Об изоморфизме* β_n). *Множество* $\beta_n = B_n \cdot T_n$, *образованное как теоретико-множественное произведение подгрупп* B_n *и* T_n, *есть группа, которая является внутренним полупрямым групповым произведением* $B_n \leftthreetimes T_n$.

Доказательство. Сначала покажем, что $B_n \cap T_n = e$. Рассмотрим отображение (1.8) и отображение ($1.9^{\text{А}}$) или отображение ($1.9^{\text{Б}}$). Сравним в общем виде получаемые подстановки по первому и последнему элементам. Для отображения ($1.9^{\text{А}}$) или для отображения ($1.9^{\text{Б}}$) эти элементы неподвижны. В свою очередь, для отображения (1.8) подвижными будут не только первый и последний элементы, но и все остальные. И только для нейтральных элементов будут получены одинаковые подстановки. Далее покажем, что любое произведение $(t_0 b_0)$ сводимо к $(b_1 t_1)$. Запишем произведение $(t_0 b_0)$ в виде произведения изоморфизмов-прообразов отображения (1.6) и отображения (1.7). Пусть $\pi \in S_n$ соответствует t_0, а $z \in E_n$ – b_0 и $(t_0 b_0) = \varphi_\pi \varphi_z$. Тогда вычислим $(t_0 b_0)(j) = \varphi_z(\varphi_\pi(j)) = \varphi_z(j^\pi) = (j^\pi)^z$ абстрактно без привязки к типу А или типу Б. Пользуясь тем, что $(j^\pi)^z = j^\pi \oplus z = j^\pi \oplus \left(z^{\pi^{-1}}\right)^\pi$, и теоремой 1.1, получим $(j^\pi)^z = \left(j \oplus z^{\pi^{-1}}\right)^\pi = \left(j^{z^{\pi^{-1}}}\right)^\pi = \varphi_\pi\left(j^{z^{\pi^{-1}}}\right) = \varphi_\pi\left(\varphi_{z^{\pi^{-1}}}(j)\right)$, т.е. $(t_0 b_0) = \varphi_{z^{\pi^{-1}}} \varphi_\pi = (b_1 t_1)$. Данное выражение показывает, во-первых, что любой элемент представим в виде произведения элементов исходных групп. Во-вторых, из указанного представления и общей ассоциативности симметрической группы следует замкнутость и наличие обратных элементов. То есть β_n – группа. В-третьих, $t_1 = t_0$ и $z^{\pi^{-1}} \in E_n$. Другими словами, любой элемент из β_n

можно переставить с элементами B_n. Отсюда заключаем, что $B_n \triangleleft \beta_n$. В совокупности полученные выводы являются определением полупрямого произведения с нормальным делителем B_n. Что и требовалось доказать. □

Как будет показано далее, группа Джевонса может быть определена более чем одним способом. В свою очередь, группа β_n, B_n и T_n являются подгруппами S_k и не зависят от типа А или типа Б. Группа β_n **задаётся независимо от типа действия**. Она вообще не зависит от групп E_n и S_n и от понятия действия последней на БВ и БФ. По этой причине в теореме 1.4 доказательство дано абстрактно, т.е. использование изоморфизма (1.6) и изоморфизма (1.7) необходимо только для доказательства утверждений теоремы 1.4, а не для задания самой β_n.

Перейдём к представлению группы Джевонса и вложим её изоморфно в группу β_n. Обозначим элемент группы Джевонса, отражая полупрямое произведение $D_n = E_n \leftthreetimes S_n$ как $(z\pi) \in D_n \colon z \in E_n, \pi \in S_n$. Из свойств полупрямых произведений групп следует $(z\pi) = (ze_S)(e_E\pi)$, где e_S и e_E – нейтральные элементы групп S_n и E_n соответственно. Тогда пусть элемент (ze_S) отображается в S_k согласно отображению (1.6), а элемент $(e_E\pi)$ – согласно отображению (1.7). Весь же элемент группы Джевонса будет отображаться в их произведение, или в символьном виде $(z\pi) = \varphi_z\varphi_\pi$.

Положим $(z_0\pi_0), (z_1\pi_1) \in D_n$, тогда вычислим произведения их образов в β_n или $\varphi_{z_0}\varphi_{\pi_0}\varphi_{z_1}\varphi_{\pi_1}$. Опираясь на доказательство теоремы 1.4, сначала вычислим произведение внутренних элементов $\varphi_{\pi_0}\varphi_{z_1} = \varphi_{z_1^{\pi_0^{-1}}}\varphi_{\pi_0}$. Далее, согласно теореме 1.2 и теореме 1.3, получим $\varphi_{z_0}\varphi_{\pi_0}\varphi_{z_1}\varphi_{\pi_1} = \varphi_{z_0}\varphi_{z_1^{\pi_0^{-1}}}\varphi_{\pi_0}\varphi_{\pi_1} = = \varphi_{z_0 z_1^{\pi_0^{-1}}}\varphi_{\pi_0}\varphi_{\pi_1}$. Произведение двух последних элементов раскроется для типов А и Б неодинаково. Для типа А $\varphi_{z_0}\varphi_{z_1^{\pi_0^{-1}}}\varphi_{\pi_0}\varphi_{\pi_1} = \varphi_{z_0 z_1^{\pi_0^{-1}}}\varphi_{\pi_0\pi_1}$ и для типа Б $\varphi_{z_0}\varphi_{z_1^{\pi_0^{-1}}}\varphi_{\pi_0}\varphi_{\pi_1} = \varphi_{z_0 z_1^{\pi_0^{-1}}}\varphi_{\pi_1\pi_0}$. Итак, получим, что операция в группе Джевонса задана следующим образом для типов А и Б соответственно:

$$(z_0\pi_0)(z_1\pi_1) = \left(z_0 z_1^{\pi_0^{-1}}\pi_0\pi_1\right); \qquad (1.10^{\text{А}})$$

$$(z_0\pi_0)(z_1\pi_1) = \left(z_0 z_1^{\pi_0^{-1}}\pi_1\pi_0\right). \qquad (1.10^{\text{Б}})$$

Получено два представления группы Джевонса типа А и типа Б. Обе группы независимо от типа действия изоморфны группе β_n. Группа Джевонса типа А соответствует определению полупрямого произведения (1.2). В свою очередь, группа Джевонса типа Б отлична от группы, описываемой формулой (1.2), так как множитель симметрической группы вкладывается антиизоморфно. Обе операции задаются таким образом, что гомоморфизм ψ из произведения (1.2) имеет одинаковый абстрактный вид $\psi_{\pi_0}(z_1) = z_1^{\pi_0^{-1}}$. Для каждого типа его необходимо сводить к действию по формуле ($1.1^{\text{А}}$) или по формуле ($1.1^{\text{Б}}$).

Резюме. Задано полупрямое произведение групп E_n и S_n.

Гомоморфизм ψ из произведения (1.2) группы Джевонса можно задать в том числе как $\psi_{\pi_0}(z_1){=}z_1^{\pi_0}$ и для типа А, и для типа Б. Полученные алгебраические структуры будут являться группами с операциями, отличными от операции ($1.10^{\text{А}}$) и операции ($1.10^{\text{Б}}$), и могут также называться группами Джевонса. Более того, сам такой гомоморфизм корректен в том смысле, что элементы S_n действуют естественным образом на группе E_n. Но полученные таким образом группы не будут эквивалентны группе β_n по действию над БФ.

Определим формулы для вычисления обратного и сопряженного элементов. Обратный элемент будет абстрактно одинаков для типа А и типа Б. Согласно правилам вычисления обратного элемента [41] полупрямого произведения, имеем:

$$(z\pi)^{-1} = \left(\psi_{\pi^{-1}}\left(z^{-1}\right)\pi^{-1}\right) = \left(\left(z^{-1}\right)^{\left(\pi^{-1}\right)^{-1}}\pi^{-1}\right) = \left(z^{\pi}\pi^{-1}\right). \tag{1.11}$$

Выражение $z^{-1} = z$ верно, так как порядок элементов группы E_n равен 2. Формула (1.11) абстрактна, т.е. конечные соотношения для типа А и типа Б будут различны (в частности, будут различны части нормального делителя).

Сопряжения элементов в группе Джевонса необходимы для перестановки сомножителей по классическим групповым законам и часто используются в прикладных задачах. Для типов действий А и Б будем вести вывод параллельно. Пусть $(z_0\pi_0), (z_1\pi_1) \in D_n$, тогда вычислим $(z_0\pi_0)^{(z_1\pi_1)}$. Из определения сопряжённого элемента получим $(z_1\pi_1)^{-1}(z_0\pi_0)(z_1\pi_1)$, далее, согласно

но формуле (1.11), будет верно $\left(z_1^{\pi_1}\pi_1^{-1}\right)(z_0\pi_0)(z_1\pi_1)$. Теперь найдём произведение для типа А и типа Б. Для типа А, согласно формуле ($1.10^{\text{А}}$), получим $\left(z_1^{\pi_1}z_0^{\pi_1}\pi_1^{-1}\pi_0\right)(z_1\pi_1)=\left(z_1^{\pi_1}z_0^{\pi_1}z_1^{\left(\pi_1^{-1}\pi_0\right)^{-1}}\pi_1^{-1}\pi_0\pi_1\right)=\left(z_1^{\pi_1}z_0^{\pi_1}z_1^{\pi_0^{-1}\pi_1}\pi_0^{\pi_1}\right)=\left(\left(z_0z_1z_1^{\pi_0^{-1}}\right)^{\pi_1}\pi_0^{\pi_1}\right)$. Для типа Б, согласно формуле ($1.10^{\text{Б}}$) и правилам произведения действий по формуле ($1.1^{\text{Б}}$), вычислим $\left(z_1^{\pi_1}z_0^{\pi_1}\pi_0\pi_1^{-1}\right)(z_1\pi_1)=\left(z_1^{\pi_1}z_0^{\pi_1}z_1^{\left(\pi_0\pi_1^{-1}\right)^{-1}}\pi_1\pi_0\pi_1^{-1}\right)=$ $=\left(z_1^{\pi_1}z_0^{\pi_1}z_1^{\pi_1\pi_0^{-1}}\pi_0^{\pi_1^{-1}}\right)=\left(\left(z_0z_1z_1^{\pi_0^{-1}}\right)^{\pi_1}\pi_0^{\pi_1^{-1}}\right)$. В итоге для типа А и типа Б получим:

$$(z_0\pi_0)^{(z_1\pi_1)}=\left(\left(z_0z_1z_1^{\pi_0^{-1}}\right)^{\pi_1}\pi_0^{\pi_1}\right); \qquad (1.12^{\text{А}})$$

$$(z_0\pi_0)^{(z_1\pi_1)}=\left(\left(z_0z_1z_1^{\pi_0^{-1}}\right)^{\pi_1}\pi_0^{\pi_1^{-1}}\right). \qquad (1.12^{\text{Б}})$$

Элементы нормального делителя $\left(z_0z_1z_1^{\pi_0^{-1}}\right)^{\pi_1}$ в формуле ($1.12^{\text{А}}$) и формуле ($1.12^{\text{Б}}$) совпадают только абстрактно. Их нужно раскрывать по формуле ($1.1^{\text{А}}$) или по формуле ($1.1^{\text{Б}}$) для типов А и Б соответственно.

§ 1.5. Контрольные примеры операций в группе Джевонса

Далее покажем на примере полученные формулы и группы. Выберем пример для E_3 и S_3. Образы элементов групп удобно строить в виде таблицы. Пусть первые три столбца таблицы – это компоненты произвольного элемента $j\in E^3, j=\{j_2,j_1,j_0\}$, а строки таблицы будут заполнены так, что значения j как чисел, согласно формуле (1.3), убывают при обходе таблицы снизу вверх (нотация D2U, down to up). Остальные столбцы будем дописывать по мере действия элементов из E_3. Воспользуемся табличным представлением и вычислим B_3.

Таблица 1.1. Вычисление B_3 (начало)

j_2	j_1	j_0	j	z_{000}			j^z	z_{001}			j^z	z_{010}			j^z	z_{011}			j^z
0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	2	0	1	1	3
0	0	1	1	0	0	1	1	0	0	0	0	0	1	1	3	0	1	0	2
0	1	0	2	0	1	0	2	0	1	1	3	0	0	0	0	0	0	1	1
0	1	1	3	0	1	1	3	0	1	0	2	0	0	1	1	0	0	0	0
1	0	0	4	1	0	0	4	1	0	1	5	1	1	0	6	1	1	1	7
1	0	1	5	1	0	1	5	1	0	0	4	1	1	1	7	1	1	0	6
1	1	0	6	1	1	0	6	1	1	1	7	1	0	0	4	1	0	1	5
1	1	1	7	1	1	1	7	1	1	0	6	1	0	1	5	1	0	0	4

Каждый четвёртый столбец табл. 1.1 есть значение подстановки-образа. Тогда получим следующие подстановки:

$$\varphi_{\{000\}}=\binom{76543210}{76543210}\ \varphi_{\{001\}}=\binom{76543210}{67452301}\ \varphi_{\{010\}}=\binom{76543210}{54761032}\ \varphi_{\{011\}}=\binom{76543210}{45670123}.$$

Таблица 1.2. Вычисление B_3 (конец)

j_2	j_1	j_0	j	z_{100}			j^z	z_{101}			j^z	z_{110}			j^z	z_{111}			j^z
0	0	0	0	1	0	0	4	1	0	1	5	1	1	0	6	1	1	1	7
0	0	1	1	1	0	1	5	1	0	0	4	1	1	1	7	1	1	0	6
0	1	0	2	1	1	0	6	1	1	1	7	1	0	0	4	1	0	1	5
0	1	1	3	1	1	1	7	1	1	0	6	1	0	1	5	1	0	0	4
1	0	0	4	0	0	0	0	0	0	1	1	0	1	0	2	0	1	1	3
1	0	1	5	0	0	1	1	0	0	0	0	0	1	1	3	0	1	0	2
1	1	0	6	0	1	0	2	0	1	1	3	0	0	0	0	0	0	1	1
1	1	1	7	0	1	1	3	0	1	0	2	0	0	1	1	0	0	0	0

Каждый четвёртый столбец табл. 1.2 есть значение подстановки-образа. Тогда получим следующие подстановки:

$$\varphi_{\{100\}} = \binom{76543210}{32107654}\ \varphi_{\{101\}} = \binom{76543210}{23016745}\ \varphi_{\{110\}} = \binom{76543210}{10325476}\ \varphi_{\{111\}} = \binom{76543210}{01234567}.$$

Полученные подстановки составляют группу B_3 порядка 8. Табличное представление позволяет «быстро» строить элементы. Отрицание каждой компоненты j переставляет строки таблицы каждые четыре, каждые две и каждую одну для j_2, j_1 и j_0 соответственно.

Группа S_3 содержит нейтральный элемент, три элемента порядка 2: $(1,0)$, $(2,0)$, и $(2,1)$, и два элемента порядка 3: $(2,1,0)$ и $(2,0,1)$. Согласно формуле (1.7) и формуле ($1.1^{\text{А}}$) и формуле ($1.1^{\text{Б}}$), различаться будут только элементы порядка 3 в образах типа А и типа Б. Аналогично воспользуемся табличным представлением и вычислим T_3.

Таблица 1.3. Вычисление T_3 (начало)

j_2	j_1	j_0	j	π_{e_S}			j^π	$\pi_{(1,0)}$			j^π	$\pi_{(2,0)}$			j^π	$\pi_{(2,1)}$			j^π
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	0	0	1	1	0	1	0	2	1	0	0	4	0	0	1	1
0	1	0	2	0	1	0	2	0	0	1	1	0	1	0	2	1	0	0	4
0	1	1	3	0	1	1	3	0	1	1	3	1	1	0	6	1	0	1	5
1	0	0	4	1	0	0	4	1	0	0	4	0	0	1	1	0	1	0	2
1	0	1	5	1	0	1	5	1	1	0	6	1	0	1	5	0	1	1	3
1	1	0	6	1	1	0	6	1	0	1	5	0	1	1	3	1	1	0	6
1	1	1	7	1	1	1	7	1	1	1	7	1	1	1	7	1	1	1	7
Тип				А Б				А Б				А Б				А Б			

Каждый четвёртый столбец табл. 1.3 есть значение подстановки-образа. Тогда получим следующие подстановки:

$$\varphi_e = \binom{76543210}{76543210}\ \varphi_{(1,0)} = \binom{76543210}{75643120}\ \varphi_{(2,0)} = \binom{76543210}{73516240}\ \varphi_{(2,1)} = \binom{76543210}{76325410}.$$

Таблица 1.4. Вычисление T_3 (конец)

j_2	j_1	j_0	j	$\pi_{(2,1,0)}$			j^π	$\pi_{(2,0,1)}$			j^π	$\pi_{(2,1,0)}$			j^π	$\pi_{(2,0,1)}$			j^π
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	1	0	0	4	0	1	0	2	0	1	0	2	1	0	0	4
0	1	0	2	0	0	1	1	1	0	0	4	1	0	0	4	0	0	1	1
0	1	1	3	1	0	1	5	1	1	0	6	1	1	0	6	1	0	1	5
1	0	0	4	0	1	0	2	0	0	1	1	0	0	1	1	0	1	0	2
1	0	1	5	1	1	0	6	0	1	1	3	0	1	1	3	1	1	0	6
1	1	0	6	0	1	1	3	1	0	1	5	1	0	1	5	0	1	1	3
1	1	1	7	1	1	1	7	1	1	1	7	1	1	1	7	1	1	1	7
Тип				А				А				Б				Б			

Каждый четвёртый столбец табл. 1.4 есть значение подстановки-образа. Для типов действия А и Б они будут различаться:

$$\text{тип А: } \varphi_{(2,1,0)} = \begin{pmatrix}76543210\\73625140\end{pmatrix}\ \varphi_{(2,0,1)} = \begin{pmatrix}76543210\\75316420\end{pmatrix};$$
$$\text{тип Б: } \varphi_{(2,1,0)} = \begin{pmatrix}76543210\\75316420\end{pmatrix}\ \varphi_{(2,0,1)} = \begin{pmatrix}76543210\\73625140\end{pmatrix}.$$

Полученные элементы составляют группу T_3. Вся группа β_3 будет являться произведением полученных множеств элементов. Пример предназначен для демонстрации операций в группе Джевонса, поэтому вся β_3 не приводится. Рассмотрим два элемента группы Джевонса: $D_3\ (z_0\pi_0) = (\{010\}(2,1,0))$ и $(z_1\pi_1) = (\{001\}(1,0))$. Их образы в группе β_3 для первого элемента будут различны, а для второго будут совпадать. Обозначим произведение этих элементов как $(z_2\pi_2) = (z_0\pi_0)(z_1\pi_1)$ и выполним вычисления.

Таблица 1.5. Вычисления произведений в группах D_3 и β_3

Искомый объект	**Тип А**	**Тип Б**
$(z_0\pi_0) = (\{010\}(2,1,0))$ Образ в β_3: $\varphi_{\{010\}}\varphi_{(2,1,0)}$	$\begin{pmatrix}76543210\\54761032\end{pmatrix}\begin{pmatrix}76543210\\73625140\end{pmatrix} = \begin{pmatrix}76543210\\62734051\end{pmatrix}$	$\begin{pmatrix}76543210\\54761032\end{pmatrix}\begin{pmatrix}76543210\\75316420\end{pmatrix} = \begin{pmatrix}76543210\\31752064\end{pmatrix}$
$(z_1\pi_1) = (\{001\}(1,0))$ Образ в β_3: $\varphi_{\{001\}}\varphi_{(1,0)}$	$\begin{pmatrix}76543210\\67452301\end{pmatrix}\begin{pmatrix}76543210\\75643120\end{pmatrix} = \begin{pmatrix}76543210\\57461302\end{pmatrix}$	
Образ в β_3 $(z_0\pi_0)(z_1\pi_1)$	$\begin{pmatrix}76543210\\62734051\end{pmatrix}\begin{pmatrix}76543210\\57461302\end{pmatrix} = \begin{pmatrix}76543210\\73516240\end{pmatrix}$	$\begin{pmatrix}76543210\\31752064\end{pmatrix}\begin{pmatrix}76543210\\57461302\end{pmatrix} = \begin{pmatrix}76543210\\10543276\end{pmatrix}$
$\psi_{\pi_0}(z_1) = z_1^{\pi_0^{-1}}$	$\{001\}^{(2,1,0)^{-1}} = \{001\}^{(2,0,1)} = \{010\}$	$\{001\}^{(2,1,0)^{-1}} = \{001\}^{(2,0,1)} = \{100\}$
$z_2 = z_0 z_1^{\pi_0^{-1}}$	$\{010\}\{010\} = \{000\}$	$\{010\}\{100\} = \{110\}$
π_2	$\pi_0\pi_1 = (2,1,0)(1,0) = (2,0)$	$\pi_1\pi_0 = (1,0)(2,1,0) = (2,1)$
Результат в группе Джевонса $(z_2\pi_2)$	$(\{000\}(2,0))$	$(\{110\}(2,1))$
Образ результата в β_3: $\varphi_{z_2}\varphi_{\pi_2}$	$\begin{pmatrix}76543210\\76543210\end{pmatrix}\begin{pmatrix}76543210\\73516240\end{pmatrix} = \begin{pmatrix}76543210\\73516240\end{pmatrix}$	$\begin{pmatrix}76543210\\10325476\end{pmatrix}\begin{pmatrix}76543210\\76325410\end{pmatrix} = \begin{pmatrix}76543210\\10543276\end{pmatrix}$
Обратный образ в β_3 $(z_0\pi_0)$: $\left(\varphi_{\{010\}}\varphi_{(2,1,0)}\right)^{-1}$	$\begin{pmatrix}76543210\\62734051\end{pmatrix}^{-1} = \begin{pmatrix}76543210\\57134602\end{pmatrix}$	$\begin{pmatrix}76543210\\31752064\end{pmatrix}^{-1} = \begin{pmatrix}76543210\\51407362\end{pmatrix}$
$z_0^{\pi_0}$	$\{010\}^{(2,1,0)} = \{001\}$	$\{010\}^{(2,1,0)} = \{100\}$
$(z_0\pi_0)^{-1} = \left(z_0^{\pi_0}\pi_0^{-1}\right)$	$(\{001\}(2,0,1))$	$(\{100\}(2,0,1))$
Образ обратного элемента $(z_0\pi_0)^{-1}$ в β_3: $\varphi_{z_0^{\pi_0}}\varphi_{\pi_0^{-1}}$	$\begin{pmatrix}76543210\\67452301\end{pmatrix}\begin{pmatrix}76543210\\75316420\end{pmatrix} = \begin{pmatrix}76543210\\57134602\end{pmatrix}$	$\begin{pmatrix}76543210\\32107654\end{pmatrix}\begin{pmatrix}76543210\\73625140\end{pmatrix} = \begin{pmatrix}76543210\\51407362\end{pmatrix}$

В табл. 1.5 показаны этапы вычисления произведения в группе Джевонса и β_3 группы, а также этапы вычисления обратного элемента. Продемонстрируем вычисления для сопряжений по формуле ($1.12^{\text{А}}$) и по формуле ($1.12^{\text{Б}}$), опираясь на результаты табл. 1.5. Определим $(z_3\pi_3) = (z_0\pi_0)^{(z_1\pi_1)}$.

Таблица 1.6. Вычисления сопряжений в группах D_3 и β_3

Искомый объект	**Тип А**	**Тип Б**
$(z_0\pi_0) = (\{010\}(2,1,0))$ Образ в β_3: $\varphi_{\{010\}}\varphi_{(2,1,0)}$	$\binom{76543210}{54761032}\binom{76543210}{73625140} = \binom{76543210}{62734051}$	$\binom{76543210}{54761032}\binom{76543210}{75316420} = \binom{76543210}{31752064}$
$(z_1\pi_1) = (\{001\}(1,0))$ Образ в β_3: $\varphi_{\{001\}}\varphi_{(1,0)}$	$\binom{76543210}{67452301}\binom{76543210}{75643120} = \binom{76543210}{57461302}$	
Обратный образ в β_3 $(z_1\pi_1)$: $\left(\varphi_{\{001\}}\varphi_{(1,0)}\right)^{-1}$	$\binom{76543210}{57461302}^{-1} = \binom{76543210}{64752031}$	
Сопряжение в β_3: $\left(\varphi_{\{010\}}\varphi_{(2,1,0)}\right)^{\varphi_{\{001\}}\varphi_{(1,0)}}$	$\binom{76543210}{31752064}$	$\binom{76543210}{04152637}$
$\psi_{\pi_0}(z_1) = z_1^{\pi_0^{-1}}$	$\{001\}^{(2,1,0)^{-1}} = \{001\}^{(2,0,1)} = \{010\}$	$\{001\}^{(2,1,0)^{-1}} = \{001\}^{(2,0,1)} = \{100\}$
$z_3 = \left(z_0 z_1 z_1^{\pi_0^{-1}}\right)^{\pi_1}$	$(\{011\}\{010\})^{(1,0)} = \{001\}^{(1,0)} = \{010\}$	$(\{011\}\{100\})^{(1,0)} = \{111\}^{(1,0)} = \{111\}$
π_3	$\pi_0^{\pi_1} = (1,0)^{-1}(2,1,0)(1,0) = (2,0,1)$	$\pi_0^{\pi_1^{-1}} = (1,0)(2,1,0)(1,0)^{-1} = (2,0,1)$
Результат в группе Джевонса$(z_3\pi_3)$	$(\{010\}(2,0,1))$	$(\{111\}(2,0,1))$
Образ результата в β_3: $\varphi_{z_3}\varphi_{\pi_3}$	$\binom{76543210}{54761032}\binom{76543210}{75316420} = \binom{76543210}{31752064}$	$\binom{76543210}{01234567}\binom{76543210}{73625140} = \binom{76543210}{73625140}$

В табл. 1.6 не показан этап вычисления сопряжения в образах, приведён только результат. Некоторые результаты для типа А и типа Б могут совпадать.

§ 1.6. Выводы

В результате получено два представления группы Джевонса: типа А и типа Б. Преимущество действия типа А заключается в том, что множители не меняют свой порядок при вычислении действия-результата над БВ. При этом сохраняется естественный порядок операций при действии группы подстановок над БВ, но при действии над БФ это нарушается. В свою очередь, тип Б меняет местами множители при вычислении действия-результата над БВ (что нежелательно), но при действии над БФ их перестановки не происходит. В общем случае не определено, что является целевым объектом – БВ или БФ, поэтому несмотря на то, что оба типа выражаются друг через друга, невозможно выбрать какой-то один тип действия как основной, а второй – как сводимый к нему. Основные результаты главы 1 опубликованы в [59, 63, 64].

Глава 2. Действие группы Джевонса на множествах

В главе 2 определяются и исследуются действия группы Джевонса и её подгрупп на множествах БВ и БФ. Выводятся и доказываются правила вычисления композиций таких действий. Вычисление действия группы Джевонса на множестве БФ может быть сведено к действию на множестве эквивалентных им БВ группой β_n. Вводится новое понятие **эквиморфности групп** – эквивалентности групп, действующих на множестве, относительно их же действия на нём. Доказывается эквиморфизм группы Джевонса и β_n группы.

Исследуются частотные свойства действия группы Джевонса степени n над бинарными векторами длины 2^n, эквивалентными БФ n аргументов. Эти действия в ряде случаев сохраняют частотные и энтропийные характеристики булевых векторов во **всех допустимых для них алфавитах одновременно**. Генерация таких БВ является сложной задачей, поэтому предлагается метод их генерации и приводятся оценки его эффективности. Вычисления действий группы Джевонса над БВ и БФ трудоёмки, и поэтому предполагается использование ИТР. Для проверки их корректности приводятся необходимые контрольные примеры.

§ 2.1. Действие группы Джевонса на множестве БВ

Группы E_n, S_n и D_n заданы. Действие первых двух групп над БВ (в том числе как над целым неотрицательным числом по формуле (1.3)) определено согласно формуле ($1.1^{\text{А}}$), формуле ($1.1^{\text{Б}}$), формуле (1.4), формуле ($1.5^{\text{А}}$) и формуле ($1.5^{\text{Б}}$). Тогда определим действие группы Джевонса D_n на БВ. Пусть $(z\pi) \in D_n$ действует на БВ $x \in E^n$. Для определённости примем, что сначала действует элемент z нормального делителя, а затем подстановка π:

$$x^{(z\pi)} = (x^z)^{\pi}. \tag{2.1}$$

Выражение (2.1) абстрактно и примет различные формы для типов А и Б, оно является определением, а поэтому не может быть истинно или ложно.

Лемма 2.1 (*О композиции действий над бинарным вектором*).

Последовательное действие двух элементов группы Джевонса $(z_0\pi_0)$, $(z_1\pi_1) \in D_n$ *на бинарный вектор* $x \in E^n$ *эквивалентно одному действию произведения этих элементов в исходном порядке по внутригрупповой операции, или в символьном виде* $\left(x^{(z_0\pi_0)}\right)^{(z_1\pi_1)} = x^{(z_0\pi_0)(z_1\pi_1)}$.

Доказательство. На основе выражения (2.1) перейдём к действию на бинарный вектор множителями группы Джевонса $\left(x^{(z_0\pi_0)}\right)^{(z_1\pi_1)}=\left(\left(\left(x^{z_0}\right)^{\pi_0}\right)^{z_1}\right)^{\pi_1}=$ $=\left((x\oplus z_0)^{\pi_0}\oplus z_1\right)^{\pi_1}$. Согласно теореме 1.1, верно, что $\left(x^{\pi_0}\oplus z_0^{\pi_0}\oplus\left(z_1^{\pi_0^{-1}}\right)^{\pi_0}\right)^{\pi_1}=$ $=\left(\left(x\oplus z_0\oplus z_1^{\pi_0^{-1}}\right)^{\pi_0}\right)^{\pi_1}$. Во внутренних скобках получен элемент E_n, а внешние скобки необходимо раскрыть по типу А или Б согласно лемме $1.1^{\text{А}}$ или лемме $1.1^{\text{Б}}$ соответственно. Для типа А: $\left(x^{z_0 z_1^{\pi_0^{-1}}}\right)^{\pi_0\pi_1} = x^{\left(z_0 z_1^{\pi_0^{-1}}\pi_0\pi_1\right)}$, и для типа Б: $\left(x^{z_0 z_1^{\pi_0^{-1}}}\right)^{\pi_1\pi_0} = x^{\left(z_0 z_1^{\pi_0^{-1}}\pi_1\pi_0\right)}$, что является определением операции в группе Джевонса, согласно формуле $(1.10^{\text{А}})$ и формуле $(1.10^{\text{Б}})$. Для обоих типов А и Б получим $x^{(z_0\pi_0)(z_1\pi_1)}$. Что и требовалось доказать. □

Утверждение леммы 2.1 абстрактно, т.е. конкретные расчётные формулы необходимо выводить согласно формуле $(1.10^{\text{А}})$ и формуле $(1.10^{\text{Б}})$ и далее согласно формуле $(1.1^{\text{А}})$ и формуле $(1.1^{\text{Б}})$ соответственно. Важно отметить, что действие элементов симметрической группы над БВ по типу Б переставляет множители местами (см. лемму $1.1^{\text{Б}}$). В свою очередь, действие элементов группы Джевонса над БВ не приводит к перестановке множителей в произведении.

В практических задачах важен вопрос о результирующем действии нескольких элементов различных множителей (БВ и подстановок) группы Джевонса над БВ в произвольном порядке. Например, если сначала на вектор подействовала подстановка, а затем БВ, и требуется найти результат и правила определения эквивалентного по действию над БВ одного элемента группы Джевонса, т.е. правила коммутации элементов множителей группы Джевонса.

Выражение (2.1) однозначно определяет последовательное действие элементов групп E_n и S_n. Тогда сформулируем правила коммутации для такого порядка. Согласно формуле $(1.10^{\text{А}})$ и формуле $(1.10^{\text{Б}})$, верно, что $(z\pi) =$

$= (ze_S)(e_E\pi)$, где e_S и e_E – нейтральные элементы групп S_n и E_n соответственно. С помощью сопряжений выполним перестановку с сохранением в неизменном виде первого и второго множителей.

Для первого множителя: $(ze_S)(e_E\pi) = (e_E\pi)^{(ze_S)^{-1}}(ze_S)$, далее по формуле (1.11) раскрываем отрицание $(e_E\pi)^{\left(z^{e_S}e_S^{-1}\right)}(ze_S) = (e_E\pi)^{(ze_S)}(ze_S)$. Сопряжение раскрывается для типов А и Б неодинаково, даже абстрактно. При этом $e_S^{-1} = e_S$, поэтому в этом случае верно, что выражение ($1.12^{\text{А}}$) и выражение ($1.12^{\text{А}}$) абстрактно совпадают, откуда по формуле ($1.12^{\text{А}}$) получим $(e_E\pi)^{(ze_S)}(ze_S) = \left(\left(e_E z z^{\pi^{-1}}\right)^{e_S}\pi^{e_S}\right)(ze_S) = \left(zz^{\pi^{-1}}\pi\right)(ze_S)$.

Для второго множителя: $(ze_S)(e_E\pi)=(e_E\pi)(ze_S)^{(e_E\pi)}$. При этом $e_S^{\pi}=e_S=e_S^{\pi^{-1}}$, поэтому и в этом случае верно, что выражение ($1.12^{\text{А}}$) и выражение ($1.12^{\text{А}}$) абстрактно совпадают. Откуда по формуле ($1.12^{\text{А}}$) получим $(e_E\pi)(ze_S)^{(e_E\pi)} = (e_E\pi)\left(\left(ze_Ee_E^{e_S^{-1}}\right)^{\pi}e_S^{\pi}\right) = (e_E\pi)(z^{\pi}e_S)$. Запишем правила коммутации следующим образом:

$$(ze_S)(e_E\pi) = \left(zz^{\pi^{-1}}\pi\right)(ze_S) = (e_E\pi)(z^{\pi}e_S) = (z\pi). \tag{2.2}$$

Далее сформулируем правила коммутации для $(e_E\pi)(ze_S)$. Относительно сохранения первого множителя имеем $(ze_S)^{(e_E\pi)^{-1}}(e_E\pi)$. Далее по формуле (1.11) раскрываем отрицание $(ze_S)^{\left(e_E^{\pi^{-1}}\pi^{-1}\right)}(e_E\pi) = (ze_S)^{\left(e_E\pi^{-1}\right)}(e_E\pi)$. Подстановка сопряжения по формуле ($1.12^{\text{А}}$) или по формуле ($1.12^{\text{Б}}$) будет равна e_S, т.к. нейтральный элемент сопряжён сам с собой. Тогда для множителя нормального делителя независимо от типа А и типа Б имеем $\left(e_Eze_E^{e_S^{-1}}\right)^{\pi^{-1}} = z^{\pi^{-1}}$ или $(e_E\pi)(ze_S) = \left(z^{\pi^{-1}}e_S\right)(e_E\pi)$. По формуле (2.2) также будет справедливо $(e_E\pi)(ze_S)=\left(z^{\pi^{-1}}\pi\right)$, и по формуле (1.11) можно перейти к $\left(z^{\pi^{-1}}\left(\pi^{-1}\right)^{-1}\right)=\left(z\pi^{-1}\right)^{-1}$.

Выполним коммутацию с сохранением второго множителя $(ze_S)(e_E\pi)^{(ze_S)^{-1}}=$ $= (ze_S)(e_E\pi)^{(ze_S)}$. При этом $\pi^{e_S} = \pi^{e_S^{-1}} = \pi$, поэтому в данном случае выражение ($1.12^{\text{А}}$) и выражение ($1.12^{\text{А}}$) абстрактно совпадают. Тогда для множителя нормального делителя имеем $\left(ze_Ez^{\pi^{-1}}\right)^{e_S} = zz^{\pi^{-1}}$, откуда $(ze_S)\left(zz^{\pi^{-1}}\pi\right)$. Запишем правила коммутации следующим образом:

$$(e_E\pi)(ze_S) = \left(z^{\pi^{-1}}e_S\right)(e_E\pi) = (ze_S)\left(zz^{\pi^{-1}}\pi\right) = \left(z\pi^{-1}\right)^{-1} = \left(z^{\pi^{-1}}\pi\right). \tag{2.3}$$

Формула (2.2) и формула (2.3) – частные случаи определения (2.1). Они являются инструментом для решения задач, связанных с действием элементов на вектор. Важно, что формула (2.2) и формула (2.3) являются абстрактными, т.е. одинаковы с точностью до типа А и типа Б.

При действии над БВ нескольких элементов E_n подряд допустимо применение внутригрупповой операции в E_n, и такие действия будут коммутативны.

При действии над БВ нескольких элементов из S_n подряд нужно использовать лемму $1.1^{\text{А}}$ и лемму $1.1^{\text{Б}}$. Абстрактные формулы задать не удаётся.

Для проверки ИТР предлагаются следующие контрольные примеры. Для леммы 2.1 пусть на $x \in E^4$ последовательно действуют $\pi \in S_4$ и $z_0, z_1 \in E_4$: $((x^{\pi})^{z_0})^{z_1}$, где $\pi = \binom{3210}{2103} = (3,2,1,0)$, $z_0 = \{1000\}$, $z_1 = \{0100\}$. Нужно привести действия к виду $x^{(z\pi)}$ независимо от типа А или Б. Тогда определим $z \in E_4$: $z = z_0 z_1 = \{1100\}$ и $\pi^{-1} = \binom{3210}{0321} = (3,0,1,2)$, откуда непосредственно по формуле (2.3) получим $\left(\left(x^{(3,2,1,0)}\right)^{\{1000\}}\right)^{\{0100\}} = x^{(\{1100\}(3,0,1,2))^{-1}}$. В итоге для типа А имеем $x^{(\{1001\}(3,2,1,0))}$ и для типа Б – $x^{(\{0110\}(3,2,1,0))}$.

Таблица 2.1. Вычисления коммутации элементов группы Джевонса

Искомый объект	**Тип А**	**Тип Б**
z	$\{0011\}$	
π	$\binom{3210}{2103} = (3,2,1,0)$	
π^{-1}	$\binom{3210}{0321} = (3,0,1,2)$	
z^{π}	$\{1001\}$	$\{0110\}$
$z^{\pi^{-1}}$	$\{0110\}$	$\{1001\}$
$zz^{\pi^{-1}}$	$\{0101\}$	$\{1010\}$
Левый множитель $(ze_S)(e_E\pi)$	$(\{0101\}(3,2,1,0))(\{0011\}e_S)$	$(\{1010\}(3,2,1,0))(\{0011\}e_S)$
Правый множитель $(ze_S)(e_E\pi)$	$(e_E(3,2,1,0))(\{1001\}e_S)$	$(e_E(3,2,1,0))(\{0110\}e_S)$
Произведение $(ze_S)(e_E\pi)$	$(\{0011\}(3,2,1,0))$	
Левый множитель $(e_E\pi)(ze_S)$	$(\{0110\}e_S)(e_E(3,2,1,0))$	$(\{1001\}e_S)(e_E(3,2,1,0))$
Правый множитель $(e_E\pi)(ze_S)$	$(\{0011\}e_S)(\{0101\}(3,2,1,0))$	$(\{0011\}e_S)(\{1010\}(3,2,1,0))$
Обратное произведение $(e_E\pi)(ze_S)$	$(\{0011\}(3,0,1,2))^{-1}$	
Произведение $(e_E\pi)(ze_S)$	$(\{0110\}(3,2,1,0))$	$(\{1001\}(3,2,1,0))$

Контрольные примеры для проверки ИТР правил коммутации рассмот-

рим при $z = \{0011\}$ и $\pi = \binom{3210}{2103} = (3, 2, 1, 0)$. Выполним перестановку множителей с сохранением каждого из них по типу А и типу Б в произведениях $(ze_S)(e_E\pi)$ и $(e_E\pi)(ze_S)$. Результаты сведём в табл. 2.1. Из табл. 2.1 можно заключить, что произведения для $(ze_S)(e_E\pi)$ и обратные произведения для $(e_E\pi)(ze_S)$ могут быть вычислены независимо от типа действия.

§ 2.2. Действие группы Джевонса на множестве БФ

Перед определением действия над булевыми функциями [4, 7], рассмотрим действие над функциями вообще. Определим конечные множества X и Y. Тогда под функцией f будем понимать некоторое отображение $f\colon X \to Y$ или $y = f(x), x \in X, y \in Y$, где X — область определения; Y – область значений функции соответственно.

Действие элементов внешнего множества (т.е. функция не является элементом этого множества) на функцию можно определить многими способами. Такими способами могут быть замена переменных или подфункций в формуле исходной функции и др. Один из способов действия на функцию – преобразование аргумента. Результат этого – исходная функция, взятая в точках значений, над которыми подействовал внешний элемент. Для такого преобразования верно, что внешний элемент реализует отображение $X \to X$. Определим такое действие в следующем виде:

$$\begin{gathered} f, g\colon X \to Y, \\ \mu\colon X \to X, \\ g = f^{\mu}\colon g(x) = f(x^{\mu}), \forall x \in X. \end{gathered} \tag{2.4}$$

Лемма 2.2 (*О композиции действий над булевой функцией*). *Если над функцией $f\colon X \to Y$ проводятся подряд действия через аргумент $\mu, \nu\colon X \to X$, то результат их эквивалентен функции, аргумент которой преобразуется этими же действиями в обратном порядке, или в символьном виде $(f^{\mu})^{\nu} = f((x^{\nu})^{\mu})$.*

Доказательство. Пусть $f, g, h\colon X \to Y$ и $g = f^{\mu}$, и $h = g^{\nu} = (f^{\mu})^{\nu}$. Доказать лемму – значит определить h относительно f как в определении (2.4).

Тогда по определению (2.4) имеем $g(x) = f(x^{\mu})$ и $h(x) = g(x^{\nu})$. Определим для удобства $x' = x^{\nu}$, тогда $h(x) = g(x')$. Для $g(x) = f(x^{\mu})$ получим $g(x') = f((x')^{\mu}) = f((x^{\nu})^{\mu}) = h(x)$. Что и требовалось доказать. □

Под булевой функцией n аргументов $f(x_{n-1}, \ldots, x_i, \ldots, x_0)$ будем понимать классическое отображение $E^n \to E$ [4]. Тогда определим действие элемента группы Джевонса $(z\pi) \in D_n$ согласно определению (2.4) как:

$$f^{(z\pi)} = f\left(x^{(z\pi)}\right). \tag{2.5}$$

Действие группы Джевонса над БВ выполняется в два этапа согласно формуле (2.1). Сначала действует нормальная часть, а затем – подстановка. Но для БФ операции можно свести к одному этапу (под этапом понимать определение (2.4)), так как существует возможность сначала вычислить аргумент, а затем выполнить действие над БФ. Тогда, опираясь на определение (2.4), лемму 2.2, выражение (2.1) и формулу (2.3), непосредственно получим поэтапное абстрактное правило вычисления действия:

$$f^{(z\pi)} = f\left(x^{(z\pi)}\right) = f((x^z)^{\pi}) = \left(f^{(e_E\pi)}\right)^{(ze_S)}; \tag{2.6^1}$$

и эквивалент выражения (2.1) для действия на БФ:

$$\begin{gathered}\left(f^{(ze_S)}\right)^{(e_E\pi)} = f\left(\left(x^{(e_E\pi)}\right)^{(ze_S)}\right) = f\left(x^{(e_E\pi)(ze_S)}\right) = \\ = f\left(x^{\left(z\pi^{-1}\right)^{-1}}\right) = f^{\left(z\pi^{-1}\right)^{-1}} = f^{\left(z^{\pi^{-1}}\pi\right)}.\end{gathered} \tag{2.6^2}$$

На данном этапе изложения совместно существуют три рода операций: групповые операции, действия групп над БВ и действия над БФ. Для разделения операций в выражениях применяются скобки. В частности, крайняя правая часть формулы (2.6^1) и крайняя левая часть формулы (2.6^2) есть последовательные действия над БФ согласно лемме 2.2.

Для проверки ИТР предлагается следующий контрольный пример. Пусть БФ $f(x_3, x_2, x_1, x_0) = x_3(x_2 \oplus x_1x_0) \vee x_2x_1\overline{x_0}$ и элемент группы Джевонса $(z\pi)$, где $z = \{1100\}$ и $\pi = \binom{3210}{2103} = (3, 2, 1, 0)$. Вычислим для типа А и типа Б действия f^z, f^{π}, $f^{(z\pi)}$, $(f^z)^{\pi}$, $(f^{\pi})^z$ и $f^{\left(z^{\pi^{-1}}\pi\right)}$. Дополнительно вычислим также нормальную часть $z^{\pi^{-1}}$.

Операции для контрольного примера сведены в табл. 2.2. Булева функ-

ция $f(x_3,x_2,x_1,x_0) = x_3(x_2 \oplus x_1x_0) \vee x_2x_1\overline{x_0}$ подобрана таким образом, чтобы $f^{(z_0\pi_0)} \neq f^{(z_1\pi_1)}$ при $(z_0\pi_0) \neq (z_1\pi_1)$.

Таблица 2.2. Вычисления действия группы Джевонса над БФ

Искомый объект	**Тип А**	**Тип Б**
f	$x_3(x_2 \oplus x_1x_0) \vee x_2x_1\overline{x_0}$	
x^z	$\{\overline{x_3},\overline{x_2},x_1,x_0\}$	
$f^z = f(x^z)$	$\overline{x_3}(\overline{x_2} \oplus x_1x_0) \vee \overline{x_2}x_1\overline{x_0}$	
x^π	$\{x_0,x_3,x_2,x_1\}$	$\{x_2,x_1,x_0,x_3\}$
$f^\pi = f(x^\pi)$	$x_0(x_3 \oplus x_2x_1) \vee x_3x_2\overline{x_1}$	$x_2(x_1 \oplus x_0x_3) \vee x_1x_0\overline{x_3}$
$x^{(z\pi)} = (x^z)^\pi$	$\{x_0,\overline{x_3},\overline{x_2},x_1\}$	$\{\overline{x_2},x_1,x_0,\overline{x_3}\}$
$f^{(z\pi)} = f\big(x^{(z\pi)}\big)$	$x_0(\overline{x_3} \oplus \overline{x_2}x_1) \vee \overline{x_3}\,\overline{x_2}\,\overline{x_1}$	$\overline{x_2}(x_1 \oplus x_0\overline{x_3}) \vee x_1x_0\overline{\overline{x_3}}$
$(f^z)^\pi = f^z(x^\pi)$	$\overline{x_0}(\overline{x_3} \oplus x_2x_1) \vee \overline{x_3}x_2\overline{x_1}$	$\overline{x_2}(\overline{x_1} \oplus x_0x_3) \vee \overline{x_1}x_0\overline{x_3}$
$(f^\pi)^z = f^\pi(x^z)$	$x_0(\overline{x_3} \oplus \overline{x_2}x_1) \vee \overline{x_3}\,\overline{x_2}\,\overline{x_1}$	$\overline{x_2}(x_1 \oplus x_0\overline{x_3}) \vee x_1x_0\overline{\overline{x_3}}$
$z^{\pi^{-1}}$	$\{1001\}$	$\{0110\}$
$x^{\left(z^{\pi^{-1}}\pi\right)}$	$\{\overline{x_0},\overline{x_3},x_2,x_1\}$	$\{\overline{x_2},\overline{x_1},x_0,x_3\}$
$f^{\left(z^{\pi^{-1}}\pi\right)}$	$\overline{x_0}(\overline{x_3} \oplus x_2x_1) \vee \overline{x_3}x_2\overline{x_1}$	$\overline{x_2}(\overline{x_1} \oplus x_0x_3) \vee \overline{x_1}x_0\overline{x_3}$

Далее, опираясь на лемму 2.2 и выражение (2.5), сформулируем правило последовательного действия для произвольных элементов группы:

$$\Big(f^{(z_0\pi_0)}\Big)^{(z_1\pi_1)} = f^{(z_1\pi_1)(z_0\pi_0)} = f\Big(\big(\big((x^{z_1})^{\pi_1}\big)^{z_0}\big)^{\pi_0}\Big) = f\left(\left(\left(x^{z_1z_0^{\pi_1^{-1}}}\right)^{\pi_1}\right)^{\pi_0}\right). \quad (2.7)$$

Формула (2.7) фактически показывает, что крайняя её правая часть – абстрактное описание произведения в группе Джевонса $(z_1\pi_1)(z_0\pi_0)$, согласно операции ($1.10^{\text{А}}$) или операции ($1.10^{\text{Б}}$), в зависимости от типа А или типа Б.

Вычисление действия элемента группы Джевонса требует наличия формулы исходной БФ. Можно вести такие вычисления без формулы (т.е. БФ задана таблицей значений) непосредственно по определению (2.4).

§ 2.3. Эквиморфизм группы Джевонса и группы β_n

Помимо действия группы Джевонса над БФ, можно определить и действие группы β_n над БФ. Удаётся также установить связь между группой Джевонса и группой β_n по действию над БФ. Использование действий группы β_n не требует наличия формулы исходной БФ [4] и в ряде случаев позволяет снизить вычислительную сложность при расчёте действий Джевонса на БФ.

Элементы группы β_n – это подстановки симметрической группы S_k, и явно задать действие над БФ не получается. Тогда можно пойти следующим путём: связать с каждой БФ бинарный вектор и определить действие группы β_n над БФ как действие над эквивалентным ей бинарным вектором. Обозначим $y \in E^k$ и определим этот вектор:

$$\begin{gathered} y = \{f(11\ldots11), f(11\ldots10), \ldots, f(00\ldots01), f(00\ldots00)\}, \\ y_j = f(j), 0 \leqslant j < k. \end{gathered} \tag{2.8}$$

Например, для функции $f(x_3, x_2, x_1, x_0) = x_3(x_2 \oplus x_1x_0) \vee x_2x_1\overline{x_0}$ будет БВ $y = \{0111\ 1000\ 0100\ 0000\}$.

Под булевой функцией принято понимать отображение $E^n \to E$, которое может быть представлено формулой. В различных базисах [5, 7] может существовать бесконечное множество формул, реализующих одинаковое отображение $E^n \to E$. Поэтому обычно вводится понятие класса эквивалентных БФ [4, 7, 35]. Определение (2.8) показывает отображение класса эквивалентных БФ на бинарный вектор. Фактически определение (2.8) – столбец значений таблицы истинности БФ. В контексте настоящего изложения вопрос способа вычисления БФ (выбор конкретной формулы) не рассматривается. Поэтому понятия БФ и класса эквивалентных БФ в настоящем изложении принимаются как равные.

Действие элементов S_n над БВ и их правила сформулированы ранее, в частности по формуле ($1.1^{\text{А}}$) и по формуле ($1.1^{\text{Б}}$), в зависимости от типа действия. Изоморфизмы группы Джевонса и группы β_n также определены ранее в виде формулы (1.6), формулы (1.7), формулы (1.8), формулы ($1.9^{\text{А}}$) и формулы ($1.9^{\text{Б}}$). Далее рассмотрим вопрос об эквивалентности групп Джевонса и β_n при действии на БФ. Для этого введём новое понятие – «эквимирфизм групп».

Определение 2.1. *Две группы G, G', действующие на некотором множестве M, будем называть* ***эквиморфными****, если существует биекция $\varphi\colon G \to G'$, такая, что для любых $a, b \in G$ и $m \in M$:*

$$(m^a)^b = \left(m^{\varphi(a)}\right)^{\varphi(b)}. \tag{2.9}$$

При этом отображение φ будем называть эквиморфизмом.

Теорема 2.1 (*Об эквиморфизме групп Джевонса и* β_n). *Группа Джевонса* D_n *эквиморфна группе* β_n *по действию над БФ по типу Б и эквиморфна в обратные (отрицательные) элементы* β_n *по действию над БФ по типу А, и эквиморфизмами будут композиции отображения* (1.8), *отображения* ($1.9^{\text{А}}$) *и отображения* ($1.9^{\text{Б}}$).

Доказательство. Сначала определим явное отображение элемента группы Джевонса на элемент группы β_n. Пусть $f' = f^{(z\pi)}, (z\pi) \in D_n$ или $f'(x) = f\left(x^{(z\pi)}\right), x \in E^n$. Тогда, по выражению (2.8), имеем $y'_j = f\left(j^{(z\pi)}\right) = y_{(j^z)^\pi}$. Применим формулу (1.6) и формулу (1.7): $y'_j = y_{\varphi_\pi(\varphi_z(j))} = y_{(\varphi_z\varphi_\pi)(j)}$. Из доказательства теоремы 1.4 примем определение $\varphi_{(z\pi)} = \varphi_z\varphi_\pi$ и получим $y'_j = y_{\varphi_{(z\pi)}(j)}$. Данное выражение есть действие подстановки на бинарный вектор согласно формуле ($1.1^{\text{Б}}$), т.е. $f^{(z\pi)} = f^{\varphi_{(z\pi)}}$ для типа Б. Тип А и тип Б по действию на вектор связаны как обратные элементы из формулы ($1.1^{\text{А}}$) и формулы ($1.1^{\text{Б}}$). Поэтому для типа А имеем $y'_{\varphi^{-1}_{(z\pi)}(j)} = y_j$ или $f^{(z\pi)} = f^{\varphi^{-1}_{(z\pi)}}$. Пусть $(z_0\pi_0), (z_1\pi_1) \in D_n$, тогда для обоих типов получим $\left(f^{(z_0\pi_0)}\right)^{(z_1\pi_1)} = f^{(z_1\pi_1)(z_0\pi_0)}$. По теореме 1.4, изоморфный образ произведения будет отличаться для разных типов.

Для типа А: $f^{(z_1\pi_1)(z_0\pi_0)} = f^{\left(\varphi_{(z_1\pi_1)}\varphi_{(z_0\pi_0)}\right)^{-1}}$. Вычисляя обратный элемент, получим $\left(f^{(z_0\pi_0)}\right)^{(z_1\pi_1)} = f^{\varphi^{-1}_{(z_0\pi_0)}\varphi^{-1}_{(z_1\pi_1)}}$. Правая часть этого выражения может быть преобразована по формуле ($1.1^{\text{А}}$), т.е. $\left(f^{(z_0\pi_0)}\right)^{(z_1\pi_1)} = \left(f^{\varphi^{-1}_{(z_0\pi_0)}}\right)^{\varphi^{-1}_{(z_1\pi_1)}}$. Для типа Б: $f^{(z_1\pi_1)(z_0\pi_0)} = f^{\varphi_{(z_1\pi_1)}\varphi_{(z_0\pi_0)}}$. Правая часть полученного выражения может быть преобразована по формуле ($1.1^{\text{Б}}$), т.е. $\left(f^{(z_0\pi_0)}\right)^{(z_1\pi_1)} = \left(f^{\varphi_{(z_0\pi_0)}}\right)^{\varphi_{(z_1\pi_1)}}$. Что и требовалось доказать. □

Эквиморфизмом типа А будет $(z\pi) \to \varphi^{-1}_{(z\pi)} = \varphi^{-1}_\pi\varphi^{-1}_z$, последние отображения должны вычисляться по формуле (1.8) и формуле ($1.9^{\text{А}}$). Эквиморфизмом типа Б будет $(z\pi) \to \varphi_{(z\pi)} = \varphi_z\varphi_\pi$, последние отображения должны вычисляться по формуле (1.8) и формуле ($1.9^{\text{Б}}$).

Теорему 2.1 можно формулировать как эквиморфное вложение для обоих типов. Это не породит ошибки. Но тогда для типа А эквиморфизм не будет про-

изведением отображения (1.8) и отображения ($1.9^{\text{А}}$), и появляются трудности при выводе более сложных соотношений.

Для проверки ИТР предлагается следующий контрольный пример. Пусть функция будет $f(x_3, x_2, x_1, x_0) = x_3(x_2 \oplus x_1x_0) \vee x_2x_1\overline{x_0}$ и два элемента группы Джевонса $(z_0\pi)$: $z_0 = \{1100\}$, $\pi = \binom{3210}{2103}$ и $(z_1\rho)$: $z_1 = \{1001\}$, $\rho = \binom{3210}{1023}$. Вычислим $\left(f^{(z_0\pi)}\right)^{(z_1\rho)}$.

Таблица 2.3. Вычисления эквиморфизмов в группах Джевонса и β_n

Искомый объект	**Тип А**	**Тип Б**
f	$x_3(x_2 \oplus x_1x_0) \vee x_2x_1\overline{x_0}$	
Эквивалент f	{0111 1000 0100 0000}	
$f^{(z_0\pi)}$	$x_0(\overline{x_3} \oplus \overline{x_2}x_1) \vee \overline{x_3}\,\overline{x_2}\,\overline{x_1}$	$\overline{x_2}(x_1 \oplus x_0\overline{x_3}) \vee x_1x_0\overline{\overline{x_3}}$
Эквивалент $f^{(z_0\pi)}$	{0000 1000 1010 0011}	{1000 1100 0000 0110}
$x^{(z_1\rho)} = (x^{z_1})^{\rho}$	$\{\overline{x_0}, x_1, \overline{x_3}, x_2\}$	$\{x_1, \overline{x_0}, x_2, \overline{x_3}\}$
$\left(f^{(z_0\pi)}\right)^{(z_1\rho)}$	$x_2\left(\overline{\overline{x_0}} \oplus \overline{x_1}\,\overline{x_3}\right) \vee \overline{\overline{x_0}}\,\overline{x_1}\,\overline{\overline{x_3}}$	$\overline{\overline{x_0}}(x_2 \oplus \overline{x_3}\,\overline{x_1}) \vee x_2\overline{x_3}\,\overline{\overline{x_1}}$
Эквивалент $\left(f^{(z_0\pi)}\right)^{(z_1\rho)}$	{1010 0010 1001 0000}	{1010 0000 1100 0010}
φ_{z_0}	$\begin{pmatrix}15&14&13&12&11&10&9&8&7&6&5&4&3&2&1&0\\3&2&1&0&7&6&5&4&11&10&9&8&15&14&13&12\end{pmatrix}$	
φ_{π}	$\begin{pmatrix}15&14&13&12&11&10&9&8&7&6&5&4&3&2&1&0\\15&7&14&6&13&5&12&4&11&3&10&2&9&1&8&0\end{pmatrix}$	$\begin{pmatrix}15&14&13&12&11&10&9&8&7&6&5&4&3&2&1&0\\15&13&11&9&7&5&3&1&14&12&10&8&6&4&2&0\end{pmatrix}$
Эквиморфизм $(z_0\pi)$	$\begin{pmatrix}15&14&13&12&11&10&9&8&7&6&5&4&3&2&1&0\\3&1&7&5&11&9&15&13&2&0&6&4&10&8&14&12\end{pmatrix}$	$\begin{pmatrix}15&14&13&12&11&10&9&8&7&6&5&4&3&2&1&0\\6&4&2&0&14&12&10&8&7&5&3&1&15&13&11&9\end{pmatrix}$
Действие эквиморфизма $(z_0\pi)$ над f	{0000 1000 1010 0011}	{1000 1100 0000 0110}
φ_{z_1}	$\begin{pmatrix}15&14&13&12&11&10&9&8&7&6&5&4&3&2&1&0\\6&7&4&5&2&3&0&1&14&15&12&13&10&11&8&9\end{pmatrix}$	
φ_{ρ}	$\begin{pmatrix}15&14&13&12&11&10&9&8&7&6&5&4&3&2&1&0\\15&7&11&3&14&6&10&2&13&5&9&1&12&4&8&0\end{pmatrix}$	$\begin{pmatrix}15&14&13&12&11&10&9&8&7&6&5&4&3&2&1&0\\15&11&7&3&13&9&5&1&14&10&6&2&12&8&4&0\end{pmatrix}$
Эквиморфизм $(z_1\rho)$	$\begin{pmatrix}15&14&13&12&11&10&9&8&7&6&5&4&3&2&1&0\\6&2&14&10&4&0&12&8&7&3&15&11&5&1&13&9\end{pmatrix}$	$\begin{pmatrix}15&14&13&12&11&10&9&8&7&6&5&4&3&2&1&0\\10&14&2&6&8&12&0&4&11&15&3&7&9&13&1&5\end{pmatrix}$
Действие эквиморфизма $(z_1\rho)$ над f	{1010 0010 1001 0000}	{1010 0000 1100 0010}

Проведём сначала вычисления непосредственно $f^{(z_0\pi)}$ – уже вычислено в табл. 2.2. Аналогично табл. 2.2 выполним вычисления для $\left(f^{(z_0\pi)}\right)^{(z_1\rho)}$ непосредственно. После чего рассчитаем изоморфные образы φ_{z_0}, φ_{z_1}, φ_{π} и φ_{ρ} согласно формуле (1.8), формуле ($1.9^{\text{А}}$) и формуле ($1.9^{\text{Б}}$). Этапы вычисления и результаты для удобства сведены в табл. 2.3. В табл. 2.3 находятся только результаты вычисления образов. Далее для типа А и Б построим эквиморфизмы $\varphi^{-1}_{(z_0\pi)}$, $\varphi^{-1}_{(z_1\rho)}$ (тип А) и $\varphi_{(z_0\pi)}$, $\varphi_{(z_1\rho)}$ (тип Б) соответственно. В заключение выполним последовательное применение действий группы β_n к эквиваленту f.

Эквиморфизм группы Джевонса и группы β_n позволяет упростить вы-

числения при построении действий над БФ. Можно утверждать, что на всём множестве булевых функций задано два набора действий, которые эквиморфны друг другу. БФ ассоциированы с БВ длины k, следовательно, действия заданы и над ними. Но для задач обработки информации важно обратное этому утверждение: **для любого бинарного вектора длины k среди всех возможных его преобразований посредством S_k можно выделить группу действий D_n, которая вкладывается изоморфно и эквиморфно в S_k и задаёт эквивалентность на множестве БВ длины k.** Группа действий D_n и задаваемая ею эквивалентность есть следствие природы бинарных векторов, а не наоборот. Вышеописанный математический аппарат позволяет задать действия группы Джевонса степени n над бинарными векторами длины k.

§ 2.4. Частотные свойства БВ и БФ

Булевы вектора могут рассматриваться как информационные сообщения, построенные на алфавите [1] из двух символов 0 и 1. В зависимости от длины БВ можно выбрать и другие алфавиты, чьи символы сами являются комбинацией 0 и/или 1. Длина БВ должна быть кратна размеру символов таких алфавитов. Далее рассматриваются только БВ длины k.

В § 2.3 доказано, что действие группы Джевонса степени n может быть задано над БВ длины k. При этом состав символов (их количество) в БВ в различных алфавитах меняется в подавляющем большинстве случаев предсказуемо. Дадим ряд определений, необходимых для описания поведения символов алфавитов БВ при действии над ними группы Джевонса.

Определение 2.2. *Алфавит A_i – множество, построенное как декартовое произведение E^{2^i}.*

Определение 2.3. *Символ алфавита – элемент алфавита A_i, встречаемый в векторе y_f.*

БВ y_f может быть разбит на символы в любом из алфавитов A_i, где i пробегает все значения $[0; n]$. При этом разбиение начинается с первого значения

вектора y_f и символы не перекрываются. Длина БВ y_f (количество символов) в каждом из алфавитов рассчитывается как $l_i = 2^{n-i}$.

Определение 2.4. *Частота символа – количество случаев встречи заданного символа из алфавита A_i в векторе y_f.*

Определение 2.5. *Частотное распределение БВ y_f (спектр) над алфавитом A_i – отношение $Q_i(y_f) \subset A_i \times [0;k]$, т.е. множество пар символ – частота.*

Определение 2.6. *Спектральное распределение БВ y_f над алфавитом A_i – отношение $R_i(y_f) \subset [0;k] \times [0;k]$ (производное множество от $Q_i(y_f)$), элементы которого показывают, как часто повторяются частоты в векторе y_f. В элементе отношения сначала указывается частота из $Q_i(y_f)$, а затем количество различных символов, обладающих такой частотой в векторе y_f.*

Таблица 2.4. Частотные характеристики булева вектора y

Индекс алфавита	**Число символов**	$Q_i(f)$	$R_i(f)$
0	16	Символ: 0, 1; Частота: 11, 5	$\{\langle 5,1\rangle, \langle 11,1\rangle\}$
1	8	Символ: 00, 01, 10, 11; Частота: 4, 2, 1, 1	$\{\langle 4,1\rangle, \langle 2,1\rangle, \langle 1,2\rangle\}$
2	4	Символ: 0000, 0100, 1000, 0111; Частота: 1, 1, 1, 1	$\{\langle 1,4\rangle\}$
3	2	Символ: 0100 0000, 0111 1000; Частота: 1, 1	$\{\langle 1,2\rangle\}$
4	1	Символ: 0111 1000 0100 0000; Частота: 1	$\{\langle 1,1\rangle\}$

Покажем на примере БВ $y = \{0111\ 1000\ 0100\ 0000\}$ определённые понятия и для удобства сведём результаты в табл. 2.4. Откуда можно заключить, что значения частот различны только в алфавитах с индексами $i = 0$ и $i = 1$, поэтому только их спектры и спектральные распределения информативны для теории информации.

Понятия спектра и спектрального распределения тесно связаны с понятием энтропии из теории информации. Энтропия показывает среднее количество информации в БВ. Она рассчитывается согласно следующей формуле [1]:

$$H(y) = -\sum_{p} q_p \log_2 q_p = -\sum_{p} \log_2 q_p^{q_p}, \tag{2.10}$$

где p – символ, встречаемый в БВ y, q_p – относительная частота (отнесённая к длине l_i из определения 2.3) символа p в БВ y. Суммирование в формуле (2.10) производится только для символов, которые присутствуют в БВ y. Энтропия определяется частотами символов, – как следствие, является функцией спектрального распределения, которое, в свою очередь, зависит спектра.

Многие алгоритмы обработки информации используют её энтропийные и частотные характеристики. Одни из первых письменных упоминаний использования частотных характеристик датированы IX веком нашей эры. В них Абу Юсуф Якуб ибн Исхак аль-Кинди описал метод криптоанализа шифров простой замены [38, 45]. Метод основывается на подсчёте частот символов и сопоставлении со средними их частотами естественного языка. Ряд алгоритмов обработки информации, преимущественно алгоритмы сжатия и избыточного кодирования, основываются на манипуляции значением энтропии [1, 2, 3].

§ 2.5. Частотные свойства действия группы Джевонса

Действия порождающими элементами множителей группы Джевонса над БВ позволяют закономерно сохранять его спектры и спектральные распределения. В зависимости от того, какие порождающие подгрупп выбраны, будут сохраняться спектры и спектральные распределения для различных индексов алфавитов.

Определение 2.7. *Множество элементов $c_{n-1}, \ldots, c_0 \in E^n$ – порождающее множество группы E_n, причём каждый c_i имеет на позиции i значение* 1, *а на остальных* – 0.

Теорема 2.2 (*Об инвариантности спектров при действии E_n*). *Если элемент c_i действует на БФ $f \in B(n)$, то частотные распределения БВ y_f инвариантны относительно этого действия для алфавитов $A_{i'} : i' \leqslant i, i \in [0; n-1]$, а спектральные распределения БВ y_f инвариантны относительно этого же действия для алфавитов A_i.*

Доказательство. Элемент c_i, действуя на БФ $f(x)$, фактически реализует эквивалентное действие $y_f^{\pi_{c_i}}$, где $\pi_{c_i} \in S_k$. Рассмотрим цикловую структуру подстановки π_{c_i}. Во-первых, реализуется инверсия $x^{c_i} = \{x_{n-1}, \ldots, \overline{x_i}, \ldots, x_0\}$, и тогда верно $(x^{c_i})^{c_i} = x$ и, как следствие, π_{c_i} – инволюция, и все точки подстановки подвижны. Поэтому вся подстановка состоит из 2^{n-1} независимых циклов длины 2 вида $(\{x_{n-1}, \ldots, x_i, \ldots, x_0\}, \{x_{n-1}, \ldots, \overline{x_i}, \ldots, x_0\})$. Во-вторых, инверсия координаты аргумента есть фактически арифметическое сложение вида $\left(x, x + 2^i\right)$ в случае $0 \to 1$ (в противном случае $1 \to 0$ вида $\left(x + 2^i, x\right)$ – то же самое). Поэтому сохраняется взаимное положение точек подстановки, или пара x, x' перейдёт в пару $x + 2^i, x' + 2^i$ в подмножествах точек количеством 2^i. При этом символы алфавитов вплоть до A_i не меняются, а лишь переставляются в y_f. Как следствие, частотные распределения y_f для этих алфавитов инвариантны относительно действия. В-третьих, каждый символ алфавита с индексом больше i (обозначим как $i' > i$) может рассматриваться как упорядоченная комбинация символов алфавита A_i, т.к. размер каждого символа любого алфавита $A_{i'}$ кратен размеру символа алфавита A_i. Размер такой комбинации будет $2^{i'}/2^i = 2^{i'-i}$, т.е. степень двойки. Действие элемента c_i приводит к тому, что меняются местами чётные и нечётные символы алфавита A_i, тем самым выполняется одна и та же перестановка символов в каждой упорядоченной комбинации (в каждом символе) любого алфавита $A_{i'}$. Так как перестановка одна и та же, то фактически выполняется биекция символов любого алфавита $A_{i'}$ на какие-то другие символы этого же алфавита. Поэтому, независимо от выбора i', спектральные распределения для y_f инварианты для $i' > i$ относительно действия. Из инвариантности частотных распределений следует инвариантность спектральных распределений y_f для $i' \leqslant i$. Что и требовалось доказать. □

Энтропия является функцией, зависящей только от частот, а не от символов частотного распределения. Значение частот и их количество определяются спектральным распределением, поэтому верно следствие 2.2.1.

Следствие 2.2.1. *Энтропия БВ y_f инвариантна во всех алфавитах*

$A_i, i \in [0; n-1]$ *относительно действия любого элемента* E_n *над БФ* f.

Теорема 2.3 (*Об инвариантности спектров при действии* S_n). *Если транспозиция* $(i,j) \in S_n, i,j \in [0;n-1]\colon i < j$ *действует на БФ* $f \in B(n)$, *то частотные распределения БВ* y_f *инвариантны относительно этого действия для алфавитов* $A_{i'}\colon i' \leqslant i$, *а спектральные распределения БВ* y_f *инвариантны относительно этого же действия для алфавитов* $A_{i'}$ *и* $A_{j'}\colon j' > j$.

Доказательство. Транспозиция (i,j), действуя на БФ $f(x)$, фактически реализует эквивалентное действие $y_f^{\pi_{(i,j)}}$, где $\pi_{(i,j)} \in S_k$. Рассмотрим цикловую структуру подстановки $\pi_{(i,j)}$. Во-первых, реализуется перестановка координат $x^{(i,j)} = \{x_{n-1}, \ldots, x_i, \ldots, x_j, \ldots, x_0\}$, и тогда верно $\left(x^{(i,j)}\right)^{(i,j)} = x$, и, как следствие, $\pi_{(i,j)}$ – инволюция, и только половина точек подстановки подвижны (где $x_i \neq x_j$). Поэтому вся подстановка состоит из 2^{n-2} независимых циклов длины 2 вида $(\{x_{n-1}, \ldots, x_j, \ldots, x_i, \ldots, x_0\}, \{x_{n-1}, \ldots, x_i, \ldots, x_j, \ldots, x_0\})$. Во-вторых, транспозиция координат аргумента есть фактически арифметическое сложение вида $\left(x, x - 2^j + 2^i\right)$ в случае $x_i = 0, x_j = 1$ (иначе, если $x_i = 1, x_j = 0$, то вида $\left(x + 2^j - 2^i, x\right)$) или тривиальное преобразование в случае $x_i = x_j$. Поэтому сохраняется относительное положение точек подстановки, или пара x, x' перейдёт в пару $x - 2^j + 2^i, x' - 2^j + 2^i$ (или $x + 2^j - 2^i, x' + 2^j - 2^i$) в подмножествах точек количеством 2^i. При этом символы алфавитов вплоть до A_i не меняются, а лишь переставляются в y_f. Как следствие, частотные распределения y_f для этих алфавитов инвариантны относительно действия. В-третьих, каждый символ алфавита с индексом больше i (обозначим как $i'\colon j \geqslant i' > i$) может рассматриваться как упорядоченная комбинация символов алфавита A_i, т.к. размер каждого символа любого алфавита $A_{i'}$ кратен размеру символа алфавита A_i. Размер такой комбинации будет $2^{i'}/2^i = 2^{i'-i}$, т.е. степень двойки. Вплоть до алфавита A_j включительно упорядоченные комбинации символов A_i будут отображаться в общем случае не взаимно однозначно, потому что перестановка будет менять качественный состав комбинации (изменять символы алфавита A_i), и, как следствие, не будет взаимной однозначности символов $A_{i'}$. Начиная

с алфавита $A_{j'}$, где $j' > j$, упорядоченные комбинации символов алфавита A_i отображаются уже взаимно однозначно, потому что перестановка фактически реализуется над множеством символов алфавита A_i внутри символов алфавита A_{j+1} и, как следствие, алфавитов с большим индексом. Фактически выполняется биекция символов любого алфавита $A_{j'}$ на какие-то другие символы этого же алфавита. Поэтому, независимо от выбора j', спектральные распределения для y_f инварианты для $j' > j$ относительно действия. Из инвариантности частотных распределений следует инвариантность спектральных распределений y_f для $i' \leqslant i$. Что и требовалось доказать. □

Энтропия является функцией, зависящей только от частот, а не от символов частотного распределения. Значение частот и их количество определяются спектральным распределением, поэтому верно следствие 2.3.1.

Следствие 2.3.1. *Энтропия БВ y_f инвариантна для алфавитов индексов до i включительно и больше j относительно действия транспозиции $(i, j), i, j \in [0; n-1] : i < j$ группы S_n над БФ f.*

Стоит подчеркнуть следствие теоремы 2.2. При таком действии энтропия БВ сохраняется **во всех допустимых для него алфавитах**. Это же следствие может быть положено в основу метода генерации БВ равной энтропии во всех допустимых для них алфавитах. Под эффективностью генерации будем понимать количество таких генерируемых различных БВ. Для оценки эффективности генерации таких БВ важно подсчитать число различных функций, получаемых из исходной БФ действиями над ней группой E_n.

Определение 2.8. *Подгруппой инерции БФ f в группе G называть подмножество, элементы которого действуют над f тривиально или в символьном виде $J_G(f) = \{g \in G \mid f^g = f\}$.*

Число различных БФ, которые могут быть получены действием над ней элементами группы G, как видно из определения 2.8, равно индексу подгруппы инерции в ней или $[G : J_G(f)]$. Для группы E_n количество различных БФ будет $[E_n : J_{E_n}(f)]$. Это значение будет тем больше, чем меньше порядок подгруппы

инерции $J_{E_n}(f)$, и будет достигать максимума, когда подгруппа инерции $J_{E_n}(f)$ тривиальна. В теории перечислений Пойа доказано, что подавляющее большинство БФ имеют (при $n \to \infty$) тривиальные подгруппы инерции $J_{E_n}(f)$, $J_{S_n}(f)$ и $J_{D_n}(f)$ [4, 20, 35]. Откуда количество различных БФ можно оценить следующим образом:

$$count_{E_n} \approx 2^n. \tag{2.11}$$

Сам же метод генерации БВ равной энтропии во всех допустимых для них алфавитах будет сводиться к действию над некоторым вектором всеми допустимыми элементами группы E_n, согласно теореме 2.1.

§ 2.6. Выводы

Определены и исследованы действия группы Джевонса и её подгрупп на множествах БВ и БФ. Выведены и доказаны правила вычисления композиций таких действий. Вычисление действия группы Джевонса на множестве БФ может быть сведено к действию на множестве эквивалентных им БВ группой β_n. Введено новое понятие **эквиморфности групп** – эквивалентности групп, действующих на множестве, относительно их же действия на нём. Доказан эквиморфизм группы Джевонса и β_n группы.

В результате исследования частотных свойств действия группы Джевонса степени n над бинарными векторами длины 2^n, эквивалентными БФ n аргументов доказано, что эти действия в ряде случаев сохраняют частотные и энтропийные характеристики векторов во **всех допустимых для них алфавитах одновременно**. Такое уникальное свойство действия может использоваться для разработки новых методов анализа алгоритмов обработки информации. Для этого требуется метод генерации БВ с одинаковыми частотными и энтропийными характеристиками. Генерация таких БВ является сложной задачей, поэтому предложен метод их генерации и приведены оценки его эффективности. Основные результаты главы 2 опубликованы в [60, 61, 65, 67].

Глава 3. Исследование джевонс-эквивалентности данных

В главе 3 приводится формальная постановка основной задачи – решение уравнения действия элемента группы Джевонса над БФ относительно неизвестных действующих элементов. Предлагается эффективный алгоритм решения уравнения, основывающийся на найденном каноническом представлении элемента группы Джевонса. Он позволяет последовательно находить множители канонического представления неизвестных действующих элементов на основе частотных свойств их действий.

Эффективность предлагаемого алгоритма можно существенно повысить с помощью более быстрых методов вычисления действий множителей канонических представлений искомых решений. Это достигается за счёт архитектуры процессоров и применения эквиморфизмов группы Джевонса и β_n группы. Предлагается модель эквиморфного вычислителя, позволяющая повысить эффективность вычисления решений в сотни раз. Даны методические рекомендации к реализации эквиморфного вычислителя на ИТР.

§ 3.1. Формальная постановка задачи

Суть классификации БФ заключается в разбиении всего их множества на непересекающиеся классы. После такого разбиения исследуются те или иные свойства представителей классов и доказывается обладание этими свойствами каждой функцией класса. Это позволяет проводить анализ не всего множества БВ, а только представителей классов. Сформированная картина свойств всех представителей отражает в целом свойства всего множества БФ.

Классификация может быть проведена по различным критериям. Например, если для некоторого множества БФ верно $f(0,...,0,...,0)=0$, то для композиции таких функций оно также будет верно. Такой способ лежит в основе работ Поста [7]. Классификация может выполняться группами, действующими на множестве БФ [4]. Дадим ряд необходимых определений из [4, 35].

Определение 3.1. *Если на множестве БФ действует некоторая груп-*

на G, то функции $f, f' \in B(n)\colon f^g = f', g \in G$ называются G-эквивалентными, т.е. принадлежат одному классу.

Определение 3.2. *Инвариант группы G, действующей на множестве БФ, – отображение $\varepsilon\colon f \to \mathbb{R}^u, f \in B(n), u \in \mathbb{N}$, для которого выполняется соотношение $\varepsilon(f^g) = \varepsilon(f), \forall g \in G$.*

Определение 3.3. *Полный инвариант группы G, – такой инвариант группы G, для которого из $\varepsilon(f)=\varepsilon(f'), f, f' \in B(n)$ следует G-эквивалентность БФ f, f'.*

Задачи отыскания полных инвариантов групп, действующих на множестве БФ, как правило, являются сложнорешаемыми, поэтому обычно пользуются инвариантами, не являющимися полными. В ряде случаев инварианты, не являющиеся полными, позволяют существенно упростить вычисления. Классификация БФ относительно групп является одним из основных направлений дискретной математики и включает в себя задачи [4, 35]:

– нахождения числа и мощностей классов G-инвариантных БФ;

– описания подгрупп инерций БФ в группе G;

– изучения инвариантов группы G и G-инвариантных БФ;

– выявления подходящих для исследования и/или использования функций из классов;

– распознавания и конструктивного перечисления G-инвариантных БФ.

Указанные задачи исследуют, начиная с XX века. Наиболее известным примером такой классификации является Гарвардский каталог, созданный в 50-х годах XX века [34]. Нахождение числа классов G-инвариантных БФ было выделено в отдельное направление, которое сводится к применению теории перечисления Пойа [4].

Основная задача, рассматриваемая в настоящей работе, является одной из задач классификации и сводится к поиску решений уравнения действия элемента группы Джевонса над булевой функцией относительно неизвестного действующего элемента. В символьном виде представим это уравнение как:

$$f^{(z\pi)} = g. \tag{3.1}$$

В уравнении (3.1) $f, g \in B(n)$ – исходная и результирующая булевы функции соответственно и $(z\pi)$ – неизвестный действующий элемент группы Джевонса. Группа Джевонса действует на множестве булевых функций интранзитивно, поэтому уравнение (3.1) может не иметь решений вовсе. Необходимым условием наличия хотя бы одного решения будет одинаковое число наборов аргументов, на которых f, g принимают единичное/нулевое значение. Оценим вероятность того, что уравнение (3.1) имеет хотя бы одно решение: $|D_n|/|B(n)| = \frac{2^n n!}{2^{2^n}}$, и при $n \to \infty$ вероятность стремится к нулю.

Если уравнение (3.1) имеет хотя бы одно решение, то можно оценить вероятность того, что оно единственно. Все решения уравнения (3.1) можно выразить через любое его решение $(z\pi)$ и подгруппу инерции f в группе Джевонса как $(z\pi) \cdot J_{D_n}(f)$. Число решений уравнения (3.1) (в случае наличия решений) равно порядку $J_{D_n}(f)$. Опираясь на теорию перечислений Пойя [4, 35], можно заключить, что доля БФ с нетривиальной подгруппой инерции в группе Джевонса стремится к нулю при $n \to \infty$, и в подавляющем большинстве случаев решение (в случае наличия решений) единственно. Далее предлагается эффективный алгоритм решения уравнения (3.1).

§ 3.2. Каноническое представление элемента группы Джевонса

Предлагаемое решение уравнения (3.1) основывается на определяемом в настоящей работе каноническом представлении элемента группы Джевонса. Такое представление единственно, и перебор его множителей позволяет однозначно перечислить все элементы группы Джевонса. В свою очередь, оно основывается на специальном представлении подстановки. При этом известных результатов о разложении подстановки на транспозиции в общей теории [41, 43] недостаточно, потому что в них не учитывается взаимный состав транспозиций.

Лемма 3.1 (*О монотонном представлении подстановки*). *Пусть k есть количество независимых циклов, включая циклы длины 1, нетривиаль-*

ной подстановки π *группы* S_n *степени* n. *Тогда она может быть единственным образом представлена как произведение из* $n-k$ *транспозиций вида:*

$$\pi=\big(0,\pi_0^{-1}(0)\big)\cdots\big(i_0,\pi_{i_0}^{-1}(i_0)\big)\cdots\big(i,\pi_i^{-1}(i)\big)\cdots\big(i_1,\pi_{i_1}^{-1}(i_1)\big)\cdots\big(n{-}2,\pi_{n-2}^{-1}(n{-}2)\big), \quad (3.2)$$

где $0\ldots\leqslant i_0<\ldots<i<\ldots<i_i<\ldots<n-1$. *В произведение включаются только транспозиции, соответствующие точкам* i: $\pi(i)\neq i$ *и* $i\leqslant\pi_i^{-1}(i)$. *Промежуточные подстановки вычисляются рекурсивно как* $\pi_{i+1}=\big(i,\pi_i^{-1}(i)\big)\pi_i$, *при этом* $\pi_0=\pi$.

Доказательство. Представим подстановку в виде таблицы $\pi=\left(\begin{smallmatrix}\ldots & i & \ldots\\ \ldots & \pi(i) & \ldots\end{smallmatrix}\right)$, и пусть $i\neq\pi(i)$. Подстановка раскладывается в произведение независимых циклов, в один из которых входит точка i. Тогда верно представление: $\pi=$ $=(\ldots)\ldots(\ldots,i,\pi(i),\ldots)\ldots(\ldots)$, или в виде таблицы $\pi=\left(\begin{smallmatrix}\ldots & \pi^{-1}(i) & \ldots & i & \ldots\\ \ldots & i & \ldots & \pi(i) & \ldots\end{smallmatrix}\right)$. Определим произведение $\rho[i,\pi]=\big(i,\pi^{-1}(i)\big)\pi$ и вычислим его: $\left(\begin{smallmatrix}\ldots & i & \ldots & \pi^{-1}(i) & \ldots\\ \ldots & \pi^{-1}(i) & \ldots & i & \ldots\end{smallmatrix}\right)$ $\left(\begin{smallmatrix}\ldots & \pi^{-1}(i) & \ldots & i & \ldots\\ \ldots & i & \ldots & \pi(i) & \ldots\end{smallmatrix}\right)=\left(\begin{smallmatrix}\ldots & i & \ldots & \pi^{-1}(i) & \ldots\\ \ldots & i & \ldots & \pi i & \ldots\end{smallmatrix}\right)$, или в виде цикловой структуры $\rho[i,\pi]=$ $=(\ldots)\ldots\big(\ldots,\pi^{-1}(i),\pi(i),\ldots\big)\ldots(\ldots)$. Тогда верны следующие утверждения: имеет место тождество $\rho[i,\pi](i)\equiv i$ и, в случае $\pi(i)\neq i$ длина одного из циклов $\rho[i,\pi]$ на единицу меньше, чем π.

Для удобства примем, что $\pi_0=\pi$ и $\pi_{i+1}=\rho[i,\pi_i]$. Откуда $\pi_{i+1}=\big(i,\pi_i^{-1}(i)\big)\pi_i$ или $\pi_i=\big(i,\pi_i^{-1}(i)\big)\,\pi_{i+1}$. Последнее соотношение позволяет представить подстановку как произведение транспозиции, двигающей точку i, и остаток, стабилизирующий её. Каждый цикл длины $l>1$ исходной подстановки раскладывается на произведение из $l-1$ транспозиций независимо от других циклов. Откуда общее количество транспозиций в произведении будет равно сумме длин всех циклов за вычетом их количества, т.е. $n-k$.

Запустим рекурсию по всем значениям i, начиная с нуля: $\pi=\pi_0=$ $=\big(0,\pi_0^{-1}(0)\big)\pi_1=\big(0,\pi_0^{-1}(0)\big)\big(1,\pi_1^{-1}(1)\big)\pi_2=\ldots=\big(0,\pi_0^{-1}(0)\big)\big(1,\pi_1^{-1}(1)\big)\ldots\big(n{-}2,\pi_{n-2}^{-1}(n{-}2)\big)\pi_{n-1}$. Так как на каждом шаге рекурсии длина какого-то из циклов уменьшается на единицу (или не изменяется, но тогда текущая точка неподвижна в исходной подстановке), то π_{n-1} неподвижными будут $n-1$ точек, т.е. тривиальная подстановка. Откуда получаем разложение $\pi=\big(0,\pi_0^{-1}(0)\big)\big(1,\pi_1^{-1}(1)\big)\ldots\big(i,\pi_i^{-1}(i)\big)\ldots$ $\big(n{-}2,\pi_{n-2}^{-1}(n{-}2)\big)$, из которого нужно убрать тождественные части вида $\pi_{i+1}\equiv$

$\equiv \pi_i$. Транспозиция является инволюцией, и поэтому порядок точек в цикле не важен, тогда для наглядности пусть $i \leqslant \pi_i^{-1}(i)$. Единственность разложения следует из построения. Что и требовалось доказать. □

Например, для $n = 8, \pi \in S_8$: $\pi = \binom{76543210}{42637150} = (7,4,3)(6,2,1,5)(0)$ всего циклов $k = 3$. Всего транспозиций в произведении будет $n-k = 5$. Для удобства представления сведём шаги рекурсии в табл. 3.1. В результате вычислений по табл. 3.1 получим разложение $\pi = (1,2)(2,6)(3,4)(4,7)(5,6)$.

Таблица 3.1. Вычисление монотонного представления подстановки

Индекс шага	**Шаг рекурсии**	**Транспозиция**
0, 1	$\pi_1 \equiv \pi_0 \equiv \pi = (7,4,3)(6,2,1,5)$	$(1, \pi_1^{-1}(1)) = (1,2)$
2	$\pi_2 = (1,2)\pi_1 = \binom{76543210}{76543120}\binom{76543210}{42637150} = \binom{76543210}{42637510} = (7,4,3)(6,2,5)$	$(2, \pi_2^{-1}(2)) = (2,6)$
3	$\pi_3 = (2,6)\pi_2 = \binom{76543210}{72543610}\binom{76543210}{42637510} = \binom{76543210}{45637210} = (7,4,3)(6,5)$	$(3, \pi_3^{-1}(3)) = (3,4)$
4	$\pi_4 = (3,4)\pi_3 = \binom{76543210}{76534210}\binom{76543210}{45637210} = \binom{76543210}{45673210} = (7,4)(6,5)$	$(4, \pi_4^{-1}(4)) = (4,7)$
5,6	$\pi_5 = (4,7)\pi_4 = \binom{76543210}{46573210}\binom{76543210}{45673210} = \binom{76543210}{75643210} = (6,5)$	$(5, \pi_5^{-1}(5)) = (5,6)$

Далее перейдём к описанию и доказательству единственности канонического разложения элемента группы Джевонса. Пусть $b_{n-1}, \ldots, b_i, \ldots, b_0, z \in E_n$, причём $b_i = \{0, \ldots, 0, \ldots, z_i, \ldots, 0, \ldots, 0\}$, т.е. содержит на позиции i значение координаты i БВ z, а на остальных – нули.

Теорема 3.1 (*О каноническом представлении элемента группы Джевонса*). *Любой элемент группы Джевонса $(z\pi) \in D_n$ представим единственным образом в виде произведения:*

$$(b_{n-1}(n-1, j_{n-1}))\cdots(b_{i_1}(i_1, j_{i_1}))\cdots(b_i(i, j_i))\cdots(b_{i_0}(i_0, j_{i_0}))\cdots(b_0(0, j_0)), \qquad (3.3)$$

где $0 \ldots \leqslant i_0 < \ldots < i < \ldots < i_i < \ldots \leqslant n-1$. Элементы симметрической группы (i, j_i): $i \leqslant j_i$ имеют порядок не более 2, и в случае транспозиции соответствуют представлению по лемме 3.1 (для типа А будет π^{-1} и для типа Б – π).

Доказательство. Вычислим указанное в условии произведение. Элемент группы E_n первой пары произведения будет равен $b_{n-1}b_{n-2}^{\binom{n-1, j_{n-1}^{-1}}{}}$ независимо от типа действия (по формуле (1.10$^{\text{А}}$) или формуле (1.10$^{\text{Б}}$)). Из условия $0 \leqslant i_0 < i < i_1 \leqslant n-1$ (условие монотонности для подстановки) верно, что $b_{n-2}^{\binom{n-1, j_{n-1}^{-1}}{}} = b_{n-2}$, и элемент E_n первой пары произведения будет равен $b_{n-1}b_{n-2}$.

Другими словами, при вычислении произведения слева направо подстановки из-за монотонности действуют тривиально на соответствующие БВ. Значит, в рамках всего произведения будет сформирован z.

Результирующая подстановка будет по-разному определяться для типа А и типа Б. Для типа Б (по формуле (1.10$^{\text{Б}}$)) получится $(n{-}2, j_{n-2})(n{-}1, j_{n-1})$, и в рамках всего произведения будут собираться (без циклов длины один) транспозиции справа налево, что в итоге даст представление по лемме 3.1. Для типа А будет аналогичное разложение, но записанное в обратном порядке. Так как произведение составлено из транспозиций, обратный порядок описывает разложение подстановки π^{-1}.

Единственность канонического представления $(z\pi)$ следует из единственности представления БВ z через порождающие и из монотонности представления подстановки согласно лемме 3.1. Что и требовалось доказать. □

В качестве контрольного примера для проверки ИТР выберем элемент группы Джевонса D_8, равный $(z\pi){=}(\{0110\ 0011\}(7,4,3)(6,2,1,5))$. Подстановка для типа Б уже представлена в табл. 3.1, и тогда непосредственно получим каноническое представление: $(z\pi) = (e_E e_S)(\{0100\ 0000\}e_S)(\{0010\ 0000\}(5,6))$ $(e_E(4,7))(e_E(3,4))(e_E(2,6))(\{0000\ 0010\}(1,2))(\{0000\ 0001\}e_S)$. Для типа А требуется найти монотонное представление обратной подстановки $\pi^{-1} = \binom{76543210}{35174620} =$ $= (7,3,4)(6,5,1,2)$. По лемме 3.1 получим $\pi^{-1} = (1,5)(2,5)(3,7)(4,7)(5,6)$. Тогда непосредственно по лемме 3.1 получим каноническое представление для типа А: $(z\pi){=}(e_E e_S)(\{0100\ 0000\}e_S)(\{0010\ 0000\}(5,6))(e_E(4,7))(e_E(3,7))(e_E(2,5))$ $(\{0000\ 0010\}(1,5))(\{0000\ 0001\}e_S)$.

Важно подчеркнуть следующее. Монотонное разложение подстановки π в общем случае не сводимо перестановкой множителей задом наперёд к монотонному разложению π^{-1}. Применительно к примеру для π^{-1} имеем: как обращение π верно $((1,2)(2,6)(3,4)(4,7)(5,6))^{-1} = (5,6)(4,7)(3,4)(2,6)(1,2)$; как монотонное представление верно $\pi^{-1} = (1,5)(2,5)(3,7)(4,7)(5,6)$. Вычисляя оба произведения, очевидно, получим π^{-1}, но при этом первое не является

монотонным представлением, а второе – является. В заключение отметим, что монотонные представления подстановок и канонические представления элементов группы Джевонса в общем случае **не одинаковы** для типа А и типа Б.

§ 3.3. Основной алгоритм решения уравнения

Решение уравнения действия (3.1) строится на следующем принципе. В § 2.5 показано, что отрицания и/или перестановки аргументов выполняют перестановку строк таблицы истинности из формулы (2.8). Как следствие, не изменяется вес БФ. Количество наборов аргументов, на которых БФ принимает единичное и нулевое значение, фактически является спектром исходной функции в алфавите A_0. Откуда можно сделать вывод: необходимым условием решения уравнения (3.1) является равенство частотных спектров $Q_0(f)$ и $Q_0(g)$.

Возникает закономерный вопрос: «сколько и каких необходимых условий нужно выбрать, чтобы их совокупность превратилась в достаточные условия существования решения уравнения (3.1)?». Как будет показано в теореме 3.2, такой совокупностью условий является сохранение частотных спектров во всех допустимых алфавитах согласно теореме 2.2 и теореме 2.3 при последовательном действии (от $i = 0$ до $i = i{-}1$) всеми множителями, затрагивающими конкретный аргумент БФ x_i, канонического представления по формуле (3.3) потенциального решения уравнения (3.1).

Например, пусть для уравнения $f^{(z\pi)}(x_3, x_2, x_1, x_0) = g(x_3, x_2, x_1, x_0)$ верно $Q_0(f) = Q_0(g)$, и пусть решение есть, и оно единственно. Тогда проанализируем все возможные $(z\pi)$, которые затрагивают аргумент x_0. Согласно формуле (3.3), в $(z\pi)$ из уравнения (3.1) может присутствовать только один из множителей вида $(b_0(0, j_0))\colon b_0 \in \{e_E, c_0\}, 0 \leqslant j_0 < n$, откуда имеем: $(e_E e_S)$, $(\{0001\}e_S)$, $(e_E(3,0))$, $(e_E(2,0))$, $(e_E(1,0))$, $(\{0001\}(3,0))$, $(\{0001\}(2,0))$, $(\{0001\}(1,0))$. Потенциально каждый из этих множителей может входить в решение уравнения (3.1). Согласно формуле (2.7) и формуле (3.3), можно вычислить действия этих восьми множителей на f. Согласно теореме 2.2 и теореме 2.3, результаты таких действий дадут не более восьми различных спектров.

Если множитель действительно входит в решение уравнения (3.1), то спектр результата его действия, по теореме 2.2 и/или по теореме 2.3, совпадёт с $Q_1(g)$. В итоге можно отбраковать некоторые множители, действующие на x_0, и вместе с ними множество заведомо ложных решений уравнения (3.1), которые их включают. Перейдём от примера к общему случаю и запишем уравнение (3.1), опираясь на каноническое представление элемента группы Джевонса по формуле (3.3), следующим образом:

$$f^{\left[(b_{n-1}(n-1,j_{n-1}))\cdots\left(b_{i_1}\left(i_1,j_{i_1}\right)\right)\cdots(b_i(i,j_i))\cdots\left(b_{i_0}\left(i_0,j_{i_0}\right)\right)\cdots(b_0(0,j_0))\right]}=g. \tag{3.4}$$

Утверждение леммы 2.2 позволяет выполнить не только композицию, но и декомпозицию действий. Тогда по формуле (2.7) уравнение в виде (3.4) можно свести к последовательному действию множителями канонического представления элемента группы Джевонса в следующем виде:

$$\left(\left(\left(\left(f^{(b_0(0,j_0))}\right)^{\cdots\left(b_{i_0}\left(i_0,j_{i_0}\right)\right)}\right)^{\cdots(b_i(i,j_i))}\right)^{\cdots\left(b_{i_1}\left(i_1,j_{i_1}\right)\right)}\right)^{\cdots(b_{n-1}(n-1,j_{n-1}))}=g. \tag{3.5}$$

Для уравнения действия в виде (3.5), так же как и для канонического представления (3.3), верно, что $0\leqslant i_0<i<i_1\leqslant n-1$. Поэтому каждый множитель затрагивает аргументы БФ, индексы которых **строго** возрастают от 0 до $n-1$, т.е. от x_0 до x_{n-1}. Причём для каждого затрагиваемого аргумента, согласно теореме 2.2 и теореме 2.3, будут инвариантны спектры алфавитов индекса аргумента и, в общем случае, неинвариантны спектры алфавитов с бóльшими индексами. Это позволяет исключать множители канонического произведения для конкретных индексов аргументов. Последовательная отбраковка множителей позволяет построить алгоритм быстрого решения уравнения (3.1). Для его описания потребуется ряд определений.

Определение 3.4. *Гипотезой для значения* $i\colon 0\leqslant i<n$ *будем называть элемент* $h\in D_n$*, равный произведению* $i{+}1$ *множителей в порядке от меньших значений* i' *к бóльшим представления* (3.3) *решения* $(z\pi)$ *уравнения* (3.1)*, для которого верно* $Q_{i+1}\left(f^h\right)=Q_{i+1}(g)$*, где* $i'\colon 0\leqslant i'\leqslant i$ *– индекс множителя.*

Определение 3.5. *Промежуточной функцией* $f^h, h\in D_n$ *будем назы-*

вать БФ, полученную из исходной f под действием h.

Алгоритм 3.1 (*О вычислении нулевого действия*).

Вход: число аргументов БФ n и пара булевых функций $f, g \in B(n)$ в виде БВ по формуле (2.8), и тип действия: А или Б.

Выход: множество $H_n \subseteq D_n$ всех решений уравнения (3.1).

Для нахождения всех решений уравнения (3.1) нужно выполнить шаги:

а) проверить необходимое условие $Q_0(f) = Q_0(h)$. В случае неудачи завершить поиск решения с результатом «нет решений». В случае успеха принять, что исходное множество гипотез H_0 сожержит только единичный элемент группы Джевонса $(e_E e_S)$, задать индекс первого анализируемого аргумента БФ $i = 0$ и перейти к следующему шагу;

б) начало итерации i алгоритма. Вычислить множество элементов группы Джевонса H'_{i+1} из множества гипотез H_i (по формуле (1.10$^{\text{А}}$) или по формуле (1.10$^{\text{Б}}$) в зависимости от типа действия) как (умножить **слева** на H_i) $H'_{i+1} = \left[\bigcup\limits_{j_i=i}^{j_i<n} (e_E(i, j_i))H_i\right] \bigcup \left[\bigcup\limits_{j_i=i}^{j_i<n} (c_i(i, j_i))H_i\right]$. Мощности множеств будут связаны равенством $\left|H'_{i+1}\right| = 2 \cdot (n-i) \cdot |H_i|$, т.е. происходит увеличение мощности H_i в количество допустимых множителей канонического представления по формуле (3.3) для конкретного i. H_i более не нужно. Перейти к следующему шагу;

в) сравнить каждый спектр промежуточной функции $Q_{i+1}\left(f^h\right)$ для всех $h \in H'_{i+1}$ со спектром $Q_{i+1}(g)$. Определить новое множество гипотез H_{i+1}, в которое входят те элементы из H'_{i+1}, для которых $Q_{i+1}\left(f^h\right) = Q_{i+1}(g), h \in H'_{i+1}$. Конец итерации i алгоритма. H'_{i+1} более не нужно и $i = i+1$. Перейти к следующему шагу;

г) если множество H_i пусто, то нужно заключить «нет решений» и завершить алгоритм. Иначе нужно сравнить i и n. Если $i = n$, то алгоритм заканчивает работу и получено множество H_n, содержащее все решения уравнения (3.1). Иначе $(i < n)$ нужно перейти к шагу *б* алгоритма. Входными данными для шага *б* будут множество H_i и значение i. □

Докажем корректность алгоритма 3.1 следующей теоремой.

Теорема 3.2 (*О вычислении нулевого действия*). *Множество* H_n *совпадает с множеством всех решений уравнения* $f^{(z\pi)}$ *и может быть вычислено как* $H'_{i+1}=\left[\bigcup\limits_{j_i=i}^{j_i<n}(e_E(i,j_i))H_i\right]\bigcup\left[\bigcup\limits_{j_i=i}^{j_i<n}(c_i(i,j_i))H_i\right]$ *за* n *шагов последовательно для* $0\leqslant i<n$ *и* $H_{i+1}=\left\{h\in H'_{i+1}\mid Q_{i+1}\left(f^h\right)=Q_{i+1}(g)\right\}$, *начиная с* $H_0=\{(e_Ee_S)\}$.

Доказательство. Для доказательства теоремы сначала покажем, что пропуск шага *в* (т.е. замена множества $H_{i+1}=\left\{h\in H'_{i+1}\mid Q_{i+1}\left(f^h\right)=Q_{i+1}(g)\right\}$ на множество $H_{i+1}=H'_{i+1}$) для каждой итерации алгоритма 3.1 $0\leqslant i<n$ приведёт к тому, что множество H_n совпадёт со всей группой Джевонса. Это следует из того, что вычисление $H'_{i+1}=\left[\bigcup\limits_{j_i=i}^{j_i<n}(e_E(i,j_i))H_i\right]\bigcup\left[\bigcup\limits_{j_i=i}^{j_i<n}(c_i(i,j_i))H_i\right]$ фактически является перебором канонических представлений всех элементов группы Джевонса в порядке вычисления произведения, обратном формуле (3.3). Поэтому либо H_n содержит все решения уравнения (3.1), либо решений нет вовсе. Далее вернём основное условие теоремы и рассмотрим множество $H_{i+1}=$ $=\left\{h\in H'_{i+1}\mid Q_{i+1}\left(f^h\right)=Q_{i+1}(g)\right\}$.

Опираясь на теорему 2.2 и теорему 2.3 об инвариантности частотных спектров, можно заключить, что при последовательном вычислении множителей канонического произведения (3.3) от 0 до $n-1$ спектр промежуточной функции на i-ой итерации в алфавите A_{i+1} совпадает со спектром функции g. Действия на i-ой итерации не затрагивают спектры алфавитов $A_{i'}\colon i'<i+1$. Откуда $H_{i+1}=\left\{h\in H'_{i+1}\mid Q_{i+1}\left(f^h\right)=Q_{i+1}(g)\right\}$ выполняет роль необходимых условий существования решения уравнения (3.1) и позволяет исключать множители канонического произведения (и элементы, их содержащие), не удовлетворяющие уравнению (3.1). В результате на последней итерации будут сравниваться спектры в алфавите A_n, причём символами спектра будут являться сами булевы функции. На последней итерации алгоритма необходимые условия $H_n=\left\{h\in H'_n\mid Q_n\left(f^h\right)=Q_n(g)\right\}$ являются также и достаточными, останутся только гипотезы, удовлетворяющие уравнению (3.1). Если на какой-то итера-

ции алгоритма множество H_i будет пусто, то это означает отсутствие решений уравнения (3.1). Что и требовалось доказать. □

Вопрос корректности алгоритма 3.1 является не единственным основным в настоящем изложении. Интерес представляет вопрос сложности предлагаемого алгоритма по отношению к полному перебору.

Сложность алгоритма поиска решения уравнения (3.1) определяется количеством действий элементов группы Джевонса и расчетом спектров промежуточных функций. Для расчёта спектра промежуточной функции требуется время $\tau(n)$ (как и в табл. 1). Примем значение $\tau(n)$ в качестве единицы сложности, потому что даже для тривиального алгоритма нужно сравнивать результат действия с эталоном, и время этого сравнения соизмеримо с $\tau(n)$. В единицах $\tau(n)$ сложность тривиального алгоритма будет $O(2^n \cdot n!)$. Сложность в единицах $\tau(n)$ предлагаемого алгоритма можно подсчитать исходя из следующего. Пусть r_i – число промежуточных функций (равное $|H_i|$) на каждом шаге. Над каждой промежуточной функцией выполняется $2 \cdot (n-i)$ действий. Откуда общее число действий (сложность) элементов группы Джевонса на БФ n аргументов можно подсчитать как:

$$d = \sum_{i=0}^{n-1} r_i \cdot 2 \cdot (n-i). \tag{3.6}$$

Покажем пример поиска решения и вычисление сложности по формуле (3.6) уравнения: $\{1000\ 0000\ 0011\ 1011\}^{(z\pi)} = \{0001\ 0100\ 1111\ 0000\}$. Выполнение алгоритма по шагам отражено в табл. 3.2. В результате имеем следующий набор действий: $\left(\left(\left(f^{(\{0001\}e_S)}\right)^{(e_E(2,1))}\right)^{(\{0100\}(3,2))}\right)^{(e_E e_S)} = g$, откуда $(z\pi) = (e_E e_S)(\{0100\}(2,3))(e_E(1,2))(\{0001\}e_S)$. Произведение нужно вычислить в зависимости от типа А или типа Б по формуле $(1.10^{\text{А}})$ или по формуле $(1.10^{\text{Б}})$ соответственно. Для типа А решением будет $(\{0101\}(3,1,2))$, а для типа Б – $(\{0101\}(3,2,1))$. Число действий по формуле (3.6) составит: $d = \sum_{i=0}^{3} 2 \cdot (4-i) \cdot r_i = 2 \cdot ((4-0) \cdot 1 + (4-1) \cdot 1 + (4-2) \cdot 2 + (4-3) \cdot 1) = 2 \cdot (4+3+4+1) = 2 \cdot 12 = 24$. При этом число действий тривиального алгоритма составит $2^4 \cdot 4! = 384$ действия.

Таблица 3.2. Пример вычисления решения уравнения

Итерац.	Гипотезы	Промежуточные функции	Спектры промежуточных функций
i=0	$r_0 = 1$	$Q_1(g)$	Символ 00 01 11 / Частота 4 2 2
	$(e_E e_S)$	{1000 0000 0011 1011}	Символ 00 10 11 / Частота 4 2 2
	$(e_E(1,0))$	{1000 0000 0101 1101}	Символ 00 01 10 11 / Частота 3 3 1 1
	$(e_E(2,0))$	{1000 0000 0111 0011}	Символ 00 01 10 11 / Частота 4 1 1 2
	$(e_E(3,0))$	{1001 0101 0001 0001}	Символ 00 01 10 / Частота 2 5 1
	$(\{0001\}e_S)$	{0100 0000 0011 0111}	Символ 00 01 11 / Частота 4 2 2
	$(\{0001\}(1,0))$	{0100 0000 1010 1110}	Символ 00 01 10 11 / Частота 3 1 3 1
	$(\{0001\}(2,0))$	{0100 0000 1011 0011}	Символ 00 01 10 11 / Частота 4 1 1 2
	$(\{0001\}(3,0))$	{0110 1010 0010 0010}	Символ 00 01 10 / Частота 2 1 5
i=1	$r_1 = 1$	$Q_2(g)$	Символ 0000 0001 0100 1111 / Частота 1 1 1 1
	$(\{0001\}e_S)$ $(e_E e_S)$	{0100 0000 0011 0111}	Символ 0000 0011 0100 0111 / Частота 1 1 1 1
	$(\{0001\}e_S)$ $(e_E(2,1))$	{0100 0000 0001 1111}	Символ 0000 0001 0100 1111 / Частота 1 1 1 1
	$(\{0001\}e_S)$ $(e_E(3,1))$	{0100 0001 0011 0011}	Символ 0001 0011 0100 / Частота 1 2 1
	$(\{0001\}e_S)$ $(\{0010\}e_S)$	{0001 0000 1100 1101}	Символ 0000 0001 1100 1101 / Частота 1 1 1 1
	$(\{0001\}e_S)$ $(\{0010\}(2,1))$	{0001 0000 0100 1111}	Символ 0000 0001 0100 1111 / Частота 1 1 1 1
	$(\{0001\}e_S)$ $(\{0010\}(3,1))$	{0001 0100 1100 1100}	Символ 0001 0100 1100 / Частота 1 1 2
i=2	$r_2 = 2$	$Q_3(g)$	Символ 00010100 11110000 / Частота 1 1
	$(\{0001\}e_S)$ $(e_E(2,1))$ $(e_E e_S)$	{0100 0000 0001 1111}	Символ 00011111 01000000 / Частота 1 1
	$(\{0001\}e_S)$ $(e_E(2,1))$ $(e_E(3,2))$	{0100 0001 0000 1111}	Символ 00001111 01000001 / Частота 1 1
	$(\{0001\}e_S)$ $(e_E(2,1))$ $(\{0100\}e_S)$	{0000 0100 1111 0001}	Символ 00000100 11110001 / Частота 1 1
	$(\{0001\}e_S)$ $(e_E(2,1))$ $(\{0100\}(3,2))$	{0001 0100 1111 0000}	Символ 00010100 11110000 / Частота 1 1
	$(\{0001\}e_S)$ $(\{0010\}(2,1))$ $(e_E e_S)$	{0001 0000 0100 1111}	Символ 00010000 01001111 / Частота 1 1
	$(\{0001\}e_S)$ $(\{0010\}(2,1))$ $(e_E(3,2))$	{0001 0100 0000 1111}	Символ 00001111 00010100 / Частота 1 1
	$(\{0001\}e_S)$ $(\{0010\}(2,1))$ $(\{0100\}e_S)$	{0000 0001 1111 0100}	Символ 00000001 11110100 / Частота 1 1
	$(\{0001\}e_S)$ $(\{0010\}(2,1))$ $(\{0100\}(3,2))$	{0100 0001 1111 0000}	Символ 01000001 11110000 / Частота 1 1
i=3	$r_3 = 1$	$Q_4(g)$	Символ 0001010011110000 / Частота 1
	$(\{0001\}e_S)$ $(e_E(2,1))$ $(\{0100\}(3,2))$ $(e_E e_S)$	{0001 0100 1111 0000}	Символ 0001010011110000 / Частота 1
	$(\{0001\}e_S)$ $(e_E(2,1))$ $(\{0100\}(3,2))$ $(\{1000\}e_S)$	{1111 0000 0001 0100}	Символ 1111000000010100 / Частота 1

§ 3.4. Эквиморфный вычислитель

Сложность алгоритма 3.1, согласно формуле (3.6), рассчитывается в единицах $\tau(n)$ (см. § 3.1), и поэтому имеет экспоненциальную временную сложность $O(2^n)$. Аппарат эквиморфизмов, описанный в § 2.3, позволяет вычислять действия элементов группы Джевонса над БФ не последовательно, согласно формуле (2.5), а параллельно, и это снижает сложность в сотни раз. Рассмотрим принцип работы эквиморфного вычислителя на примере действия элементом $\{010\} \in E_3$ над БВ $y \in E^8$: $y = \{y_7, y_6, y_5, y_4, y_3, y_2, y_1, y_0\}$, эквивалентным некоторой БФ $f(x_2, x_1, x_0) \in B(3)$. Согласно формуле (2.5), результатом будет $y' \in E^8$: $y' = \{y_5, y_4, y_7, y_6, y_1, y_0, y_3, y_2\}$.

Фактически y' получен перестановкой чётных и нечётных пар значений y. Рассмотрим детально и разделим значения БВ y как $y_{\text{lo}} = \{0, 0, y_5, y_4, 0, 0, y_1, y_0\}$ и $y_{\text{hi}} = \{y_7, y_6, 0, 0, y_3, y_2, 0, 0\}$. Далее сдвинем координаты y_{lo} в сторону больших индексов на две позиции, а y_{hi} – в сторону меньших: $y_{\text{lo}}^{\leftarrow} = \{y_5, y_4, 0, 0, y_1, y_0, 0, 0\}$ и $y_{\text{hi}}^{\rightarrow} = \{0, 0, y_7, y_6, 0, 0, y_3, y_2\}$. В результате непосредственно заключаем, что $y' = y_{\text{lo}}^{\leftarrow} \oplus y_{\text{hi}}^{\rightarrow}$. Аналогично можно вычислить каждое действие на любой интерации алгоритма 3.1. Для этого потребуется некоторый абстрактный вычислитель, который может обрабатывать подмножество смежных значений БВ, применительно к примеру – восемь значений. Рассмотрим операции, которые он должен выполнять. Всего потребуется пять операций:

а) логическое умножение БВ (логическое «И»), или в символьном виде $xy = \{x_{n-1}y_{n-1}, \ldots, x_iy_i, \ldots, x_0y_0\}, \forall x, y \in E^n$. Имеет высокий приоритет;

б) логическое сложение БВ (логическое «ИЛИ»), или в символьном виде $x \vee y = \{x_{n-1} \vee y_{n-1}, \ldots, x_i \vee y_i, \ldots, x_0 \vee y_0\}, \forall x, y \in E^n$. Имеет средний приоритет;

в) логический левый сдвиг БВ на число, или в символьном виде $x \ll v = \{x_{n-1-v}, \ldots, x_v, \underbrace{0, \ldots, 0}_{v}\}, \forall x \in E^n, 0 \leqslant v < n$. Имеет низкий приоритет;

г) логический правый сдвиг БВ на число, или в символьном виде $x \gg v = \{\underbrace{0, \ldots, 0}_{v}, x_{n-1}, \ldots, x_v\}, \forall x \in E^n, 0 \leqslant v < n$. Имеет низкий приоритет;

д) покомпонентное присвоение вектора $y = x$: $y = \{x_{n-1}, \ldots, x_i, \ldots, x_0\}$, $\forall x, y \in E^n$. Имеет низший приоритет.

Для примера ранее будет y'=$(y\{0011\ 0011\}\ll 2)\vee(y\{1100\ 1100\}\gg 2)$.

Определение 3.6. *Слово – БВ длины $2^{n'}$, над которым вычислителем выполняются примитивные операции а – д, где n' – его степень.*

Определение 3.7. *Символ – подмножество смежных значений БВ, перестановка которых сводится к линейному сдвигу на одинаковое значение.*

Определение 3.8. *Блок – смежное подмножество символов БВ, перестановка которых сводится к линейным сдвигам на минимальные значения.*

Применительно к предыдущему примеру символами будут пары значений БВ. Блок будет содержать пару символов, причём одна будет сдвигаться на размер двух символов влево, другая – вправо. Два блока составляют БВ целиком, и он совпадает по размеру со словом вычислителя степени $n' = log_2 8 = 3$.

Для рассматриваемых далее алгоритмов предполагается разбиение БВ $y, y' \in E^k$ на вектора-слова $y_{index}, y'_{index} \in E^{n'}$: $0 \leqslant index < w$ соответственно, где $w = 2^{n-n'}$ (если $n < n'$, то принять что $w = 1$) – число слов.

Алгоритм 3.2 (*Об эквиморфном вычислении действия E_n*).

Вход: бинарный вектор $y \in E^k$ длины k и значение i: $0 \leqslant i < n$.

Выход: бинарный вектор $y' \in E^k$ длины k.

Для эквиморфного вычисления БВ $y' \in E^k$ длины k, эквивалентного БФ f^{c_i} (результат действия элемента $c_i \in E_n$ над БФ $f \in B(n)$, заданной в виде эквивалентного БВ $y \in E^k$ длины k) нужно выполнить шаги:

а) разбить БВ y, y' на слова. Если $i < n'$, то перейти к шагу *б*, иначе перейти к шагу *в*;

б) $\forall u$: $0 \leqslant u < w$ вычислить $y'_u = (y_u\mathrm{lo} \ll s_E) \vee (y_u\mathrm{hi} \gg s_E)$, где $s_E = 2^i$, $w_b = 2^{n'-i-1}$, $\mathrm{lo} = \{\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{1\ldots1}_{s_E}}^{w_b}\}$ и $\mathrm{hi} = \{\overbrace{\underbrace{1\ldots1}_{s_E}\underbrace{0\ldots0}_{s_E}}^{w_b}\}$. Завершить алгоритм;

в) $\forall v, u$: $0 \leqslant v < b_c, 0 \leqslant u < s_w$ вычислить $y'_{idx} = y_{idx+s_w}$ и $y'_{idx+s_w} = y_{idx}$, где $idx = v{\cdot}b_w{+}u$, $b_c = 2^{n-i-1}$, $b_w = 2^{i+1-n'}$ и $s_w = 2^{i-n'}$. Завершить алгоритм. □

Теорема 3.3 (*Об эквиморфном вычислении действия E_n*). *Вычис-*

ление БВ $y \in E^k$*, эквивалентного БФ* $f \in B(n)$*, по алгоритму 3.2 равносильно действию эквиморфизма* φ_{c_i} *(по формуле (1.8)) над ним. Число операций эквиморфного вычислителя для* $i < n'$ *составит* $2{\cdot}w$ *сдвигов,* $2{\cdot}w$ *умножений,* w *сложений,* w *присвоений, а для* $i \geqslant n'$ *–* w *присвоений.*

Доказательство. Рассмотрим цикловую структуру образа-подстановки $\varphi_{c_i} \in S_k$, получаемой по формуле (1.8) из прообраза $c_i \in E_n$. Каждая точка $x\colon 0 \leqslant x < k$ подстановки переходит в какую-то другую точку посредством инверсии координаты i, т.е. $\varphi_{c_i}(x) = \{x_{n-1}, \ldots, \overline{x_i}, \ldots, x_0\}$, и тогда верно $\varphi_{c_i}(\varphi_{c_i}(x)) = x$ и, как следствие, φ_{c_i} – инволюция, и все точки подстановки подвижны. Поэтому вся подстановка состоит из 2^{n-1} независимых циклов длины 2 вида $(\{x_{n-1}, \ldots, x_i, \ldots, x_0\}, \{x_{n-1}, \ldots, \overline{x_i}, \ldots, x_0\})$. Во-вторых, инверсия координаты точки есть фактически либо арифметическое сложение вида $\left(x, x{+}2^i\right)$ в случае $x_i = 0$, либо арифметическое вычитание вида $\left(x, x{-}2^i\right)$ в случае $x_i = 1$.

Разобьём всё множество точек на 2^{n-i} подмножеств так, что внутри них точки имеют одинаковые координаты $x_{n-1}, \ldots, x_i$ и упорядочены по координатам $x_{i-1}, \ldots, x_0$. Тогда верно заключение, что при перестановке подмножеств будут переставляться их точки, не нарушая порядок, т.е. подмножество является символом размером $s_E = 2^i$, и индексом символа будут являться значения координат точек $x_{n-1}, \ldots, x_i$. При этом каждый символ с индексом $x_{n-1}, \ldots, x_{i+1}, 0$ будет отображаться в символ $x_{n-1}, \ldots, x_{i+1}, 1$ и наоборот. Действие локализовано внутри пары символов, которые составляют блок размером 2^{i+1} бит. Индексом блока будут координаты $x_{n-1}, \ldots, x_{i+1}$.

Для $i < n'$ размер блока меньше или равен размеру слова, поэтому при обработке одного слова будет обработано $w_b = 2^{n'-i+1}$ блоков. Нужно выделить в каждом блоке слова символы с чётными и нечётными индексами и поменять их местами. Выделение символов эквивалентно логическому умножению на константы: для выделения чётных символов (младших полублоков) $low = \{\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{1\ldots1}_{s_E}}^{w_b}\}$ и нечётных символов (старших полублоков) $high = \{\overbrace{\underbrace{1\ldots1}_{s_E}\underbrace{0\ldots0}_{s_E}}^{w_b}\}$. Для взаимной перестановки достаточно нечётные символы сдвинуть влево на раз-

мер символа в битах, а чётные – вправо. Откуда получаем $y'_u = (y_u low \ll s_E) \vee$ $\vee (y_u high \gg s_E)$. Слово содержит один или несколько блоков, – как следствие, действие локализовано внутри слова. Всего слов $w = 2^{n-n'}$. В случае, если размер БВ y меньше размера блока ($n < n'$), то нужно БВ дополнить нулями слева до размера слова и принять, что $w = 1$, и в результирующем слове отбросить это дополнение. Все результирующие слова нужно обработать в любом порядке (допустима параллельная обработка по всем u) $y'_u \colon 0 \leqslant u < 2^{n-n'}$. Всего будет затрачено (исходя из преобразования одного слова): $2{\cdot}w$ логических сдвигов, $2{\cdot}w$ логических умножений, w логических сложений, w присвоений.

Для $i \geqslant n'$ размер блока больше размера слова, а размер символа не меньше размера слова. Правила перестановки будут аналогичны случаю $i < n'$, но при этом ориентированы на размер символа в словах $s_w = 2^{i-n'}$. Блок, так же как и в случае $i < n'$, состоит из чётного и нечётного символов и имеет размер в словах $b_w = 2^{n-i-1}$. При этом символы являются полублоками. Индекс каждого чётного слова и соответственный ему индекс нечётного слова различаются на размер символа s_w. Для выполнения действия нужно переставить в любом порядке (допускается параллельная обработка по всем v, u) все соответственные чётные и нечётные слова для каждого блока $y'_{idx+u} = y_{idx+u+s_w}$ и $y'_{idx+u+s_w} = y_{idx+u}$. Всего блоков (из размера символов) будет $b_c = 2^{n-i-1}$, и индекс первого слова каждого блока будет $idx = v \cdot b_w$, где $0 \leqslant v < b_c$ – индекс блока. Так как обрабатывается сразу пара символов блока, то на обработку всего блока требуется $b_w/2$ шагов, что эквивалентно размеру символа в словах s_w, и индекс шага будет $u \colon 0 \leqslant u < s_w$. При этом будет обработано $w = 2^{n-n'}$ слов. Так как обработка сводится к перестановке всех слов, то всего будет затрачено w присвоений. Что и требовалось доказать. □

Алгоритм 3.3 (*Об эквиморфном вычислении действия* S_n).

Вход: бинарный вектор $y \in E^k$ длины k и значения $i, j \colon 0 \leqslant i < j < n$.

Выход: бинарный вектор $y' \in E^k$ длины k.

Для эквиморфного вычисления БВ $y' \in E^k$ длины k, эквивалентного БФ

$f^{(i,j)}$ (результату действия транспозиции $(i,j)\in S_n$ над БФ $f\in B(n)$, заданной в виде эквивалентного БФ $y\in E^k$ длины k) нужно выполнить шаги:

а) разбить БВ y, y' на слова. Если $j<n'$, то перейти к шагу *б*, иначе если $i<n'$, то перейти к шагу *в*, иначе перейти к шагу *г*;

б) $\forall u\colon 0\leqslant u<w$ вычислить $y'_u=y_u\mathrm{st}\vee(y_u\mathrm{lo}\ll val_E)\vee(y_u\mathrm{hi}\gg val_E)$, где $\mathrm{st}=\{\overbrace{\overbrace{1\ldots1}^{s_E}\overbrace{0\ldots0}^{s_E}}^{sb_{ps}}\overbrace{\overbrace{0\ldots0}^{s_E}\overbrace{1\ldots1}^{s_E}}^{sb_{ps}}\}^{w_b}$, $\mathrm{lo}=\{\overbrace{\overbrace{0\ldots0}^{s_E}\overbrace{0\ldots0}^{s_E}}^{sb_{ps}}\overbrace{\overbrace{1\ldots1}^{s_E}\overbrace{0\ldots0}^{s_E}}^{sb_{ps}}\}^{w_b}$, $\mathrm{hi}=\{\overbrace{\overbrace{0\ldots0}^{s_E}\overbrace{1\ldots1}^{s_E}}^{sb_{ps}}\overbrace{\overbrace{0\ldots0}^{s_E}\overbrace{0\ldots0}^{s_E}}^{sb_{ps}}\}^{w_b}$, $s_E=2^i$, $w_b=2^{n'-j-1}$, $sb_{ps}=2^{j-i-1}$, и $val_E=2^j-2^i$. Завершить алгоритм;

в) $\forall v,u\colon 0\leqslant v<b_c, 0\leqslant u<sb_w$ вычислить $y'_{idx}=y_{idx}\mathrm{st_{lo}}\vee(y_{idx+sb_w}\mathrm{hi}\ll s_E)$ и $y'_{idx+sb_w}=y_{idx+sb_w}\mathrm{st_{hi}}\vee(y_{idx}\mathrm{lo}\gg s_E)$, где $idx=v\cdot b_w+u$, $s_E=2^i$, $w_{ps}=2^{n'-i-1}$, $\mathrm{st_{lo}}=\{\overbrace{\overbrace{0\ldots0}^{s_E}\overbrace{1\ldots1}^{s_E}}^{w_{ps}}\}$, $\mathrm{st_{hi}}=\{\overbrace{\overbrace{1\ldots1}^{s_E}\overbrace{0\ldots0}^{s_E}}^{w_{ps}}\}$, $\mathrm{lo}=\{\overbrace{\overbrace{1\ldots1}^{s_E}\overbrace{0\ldots0}^{s_E}}^{w_{ps}}\}$, $\mathrm{hi}=\{\overbrace{\overbrace{0\ldots0}^{s_E}\overbrace{1\ldots1}^{s_E}}^{w_{ps}}\}$, $b_c=2^{n-j-1}$, $b_w=2^{j+1-n'}$ и $sb_w=2^{j-n'}$. Завершить алгоритм;

г) $\forall v,p,u\colon 0\leqslant v<b_c, 0\leqslant p<sb_{ps}, 0\leqslant u<s_w$ вычислить $y'_{idx}=y_{idx}$, $y'_{idx+s_w}=y_{idx+s_w+val_w}$, $y'_{idx+s_w+val_w}=y_{idx+s_w}$ и $y'_{idx+2\cdot s_w+val_w}=y_{idx+2\cdot s_w+val_w}$, где $idx=v\cdot b_w+p\cdot ps_w+u$, $s_w=2^{i-n'}$, $b_c=2^{n-j-1}$, $b_w=2^{j+1-n'}$, $sb_{ps}=2^{j-i-1}$, $ps_w=2^{i+1-n'}$ и $val_w=2^{j-n'}-2^{i-n'}$. Завершить алгоритм. □

Теорема 3.4 (*Об эквиморфном вычислении действия* S_n). *Вычисление БВ $y\in E^k$, эквивалентного БФ $f\in B(n)$, по алгоритму 3.3 равносильно действию эквиморфизма $\varphi_{(i,j)}$ (по формуле (1.9А) или по формуле (1.9Б)) над ним. Число операций эквиморфного вычислителя для $j<n'$ составит $2\cdot w$ сдвигов, $3\cdot w$ умножений, $2\cdot w$ сложений, w присвоений, а для $j\geqslant n'$ при $i<n'$ – w сдвигов, $2\cdot w$ умножений, w сложений, w присвоений, и при $i\geqslant n'$ – w присвоений.*

Доказательство. Рассмотрим цикловую структуру образа-подстановки $\varphi_{(i,j)}\in S_k$, получаемой по формуле (1.9А) или по формуле (1.9Б) (для транспозиции результат формул будет совпадать) из прообраза $(i,j)\in S_n$. Каждая точка $x\colon 0\leqslant x<k$ подстановки переходит в какую-то другую точку посредством перестановки координат i и j, т.е. $\varphi_{(i,j)}(x)=\{x_{n-1},\ldots,x_i,\ldots,x_j,\ldots,x_0\}$, и тогда вер-

но $\varphi_{(i,j)}\big(\varphi_{(i,j)}(x)\big)=x$, и, как следствие, $\varphi_{(i,j)}$ – инволюция и половина точек подстановки подвижны ($x_i \neq x_j$). Поэтому вся подстановка состоит из 2^{n-2} независимых циклов длины 2 вида $(\{x_{n-1}, ..., x_j, ..., x_i, ..., x_0\}, \{x_{n-1}, ..., x_i, ..., x_j, ..., x_0\})$. Во-вторых, перестановка координат точки для $x_i \neq x_j$ есть фактически либо арифметическая операция вида $\big(x, x+2^j-2^i\big)$ в случае $x_i = 1, x_j = 0$, либо арифметическая операция вида $\big(x, x-2^j+2^i\big)$ в случае $x_i = 0, x_j = 1$. Другими словами, точка будет сдвигаться на постоянное значение $\big|2^j-2^i\big|$.

Разобьём всё множество точек на 2^{n-i} подмножеств так, что внутри них точки имеют одинаковые координаты $x_{n-1}, ..., x_i$ и упорядочены по координатам $x_{i-1}, ..., x_0$. Тогда верно заключение, что при перестановке подмножеств будут переставляться их точки, не нарушая порядок, т.е. подмножество является символом размером $s_E = 2^i$, и индексом символа будут являться значения координат точек $x_{n-1}, ..., x_i$. При этом символы с индексами $x_i = x_j$ будут оставаться на месте, а символы $x_i \neq x_j$ – меняться местами. В результате действие сводится к работе с четвёрками символов и локализуется внутри их массива с общими координатами $x_{n-1}, ..., x_{j+1}$, т.е. массив составляет блок размером 2^{j+1} бит. Всего четвёрок в блоке будет $\frac{2^{j+1}/2^i}{4} = 2^{j-i-1}$. Индексом блока будут координаты $x_{n-1}, ..., x_{j+1}$. Блок состоит из двух полублоков: старшего ($x_j = 1$) и младшего ($x_j = 0$). Полублоки состоят из $sb_{ps} = \frac{2^{j+1}/2}{2^i}/2 = 2^{j-i-1}$ пар символов, причём каждая пара старшего полублока содержит неподвижный ($x_i = 1$) и подвижный ($x_i = 0$) символы, а младшего наоборот – подвижный ($x_i = 1$) и неподвижный ($x_i = 0$) символы.

Для $j < n'$ и из условия $i < j$ верно, что $i < n'$. Размер блока меньше или равен размеру слова, поэтому при обработке одного слова будет обработано $w_b = 2^{n'-j-1}$ блоков. Нужно выделить в каждом блоке слова неподвижные(ый) и подвижные(ый) символы, соответствующие старшим и младшим полублокам. Выделение символов эквивалентно логическому умножению на константы. Размер блока меньше либо равен размеру слова, поэтому неподвижные символы младших(его) и старших(его) полублоков можно выделить

вместе одной константой $base = \{\overbrace{\underbrace{1...1}_{s_E}\underbrace{0...0}_{s_E}}^{sb_{ps}}\overbrace{\underbrace{0...0}_{s_E}\underbrace{1...1}_{s_E}}^{sb_{ps}}\}^{w_b}$. Для выделения подвижных символов старших(его) и младших(его) полублоков подходят константы $low = \{\overbrace{\underbrace{0...0}_{s_E}\underbrace{0...0}_{s_E}}^{sb_{ps}}\overbrace{\underbrace{1...1}_{s_E}\underbrace{0...0}_{s_E}}^{sb_{ps}}\}^{w_b}$ и $high = \{\overbrace{\underbrace{0...0}_{s_E}\underbrace{1...1}_{s_E}}^{sb_{ps}}\overbrace{\underbrace{0...0}_{s_E}\underbrace{0...0}_{s_E}}^{sb_{ps}}\}^{w_b}$. Для взаимной перестановки подвижных символов младших(его) и старших(его) полублоков достаточно их сдвинуть на размер символа в битах $val_E = 2^j - 2^i$ влево и вправо соответственно. Откуда получаем $y'_u = y_u base \vee (y_u low \ll val_E) \vee (y_u high \gg val_E)$. Слово содержит один или несколько блоков, – как следствие, действие локализовано внутри слова. Всего слов $w = 2^{n-n'}$. В случае, если размер БВ y меньше размера блока ($n < n'$), то нужно БВ дополнить нулями слева до размера слова и принять, что $w = 1$, и в результирующем слове отбросить это дополнение. Все результирующие слова нужно обработать в любом порядке (допустима параллельная обработка по всем u) y'_u: $0 \leqslant u < 2^{n-n'}$. Всего будет затрачено (исходя из преобразования одного слова): $2{\cdot}w$ сдвигов, $3{\cdot}w$ умножений, $2{\cdot}w$ сложений, w присвоений.

Для $j \geqslant n'$ возможны два случая. Первый случай $i < n'$, второй – $i \leqslant n'$. В первом случае размер символа меньше либо равен размеру слова, а размер блока больше размера слова. Поэтому слово содержит символы либо младшего, либо старшего полублока. Всего блоков будет $b_c = 2^{n-j-1}$ размером $b_w = 2^{j+1-n'}$ слов. Каждое слово состоит из пар подвижных(ого) и неподвижных(ого) символов, и в каждом слове этих пар будет $w_{ps} = \frac{2^{n'}/2^i}{2} = 2^{n'-i-1}$. Выделение символов эквивалентно логическому умножению на константы. Для слов младшего полублока константы выделения неподвижных и подвижных символов будут $base_{low} = \{\overbrace{\underbrace{0...0}_{s_E}\underbrace{1...1}_{s_E}}^{w_{ps}}\}$ и $low = \{\overbrace{\underbrace{1...1}_{s_E}\underbrace{0...0}_{s_E}}^{w_{ps}}\}$ соответственно, для слов старшего полублока – $base_{high} = \{\overbrace{\underbrace{1...1}_{s_E}\underbrace{0...0}_{s_E}}^{w_{ps}}\}$ и $high = \{\overbrace{\underbrace{0...0}_{s_E}\underbrace{1...1}_{s_E}}^{w_{ps}}\}$. Неподвижные символы должны остаться на месте, а подвижные – сместиться на

значение $\left|2^j - 2^i\right|$. Подвижные символы младшего полублока сместятся влево, старшего – вправо. Для удобства значение смещения можно распределить следующим образом: на 2^j будут смещаться целые слова, поэтому можно просто смещать слово на значение размера полублока в словах $sb_w = 2^{j-n'}$. Вторую отрицательную часть значения смещения $-2^i = -s_E$ в битах нужно учитывать внутри слов. Откуда имеем $y'_{idx} = y_{idx} base_{low} \vee (y_{idx+sb_w} high \ll s_E)$ и $y'_{idx+sb_w} = y_{idx+sb_w} base_{high} \vee (y_{idx} low \gg s_E)$, где $idx = v{\cdot}b_w{+}u$ – базовый индекс каждого слова $u\colon 0 \leqslant u < sb_w$ в полублоке каждого блока $v\colon 0 \leqslant v < b_c$. Все результирующие слова нужно обработать в любом порядке (допустима параллельная обработка по всем u, v). Всего будет затрачено (исходя из преобразования одного слова): w сдвигов, $2{\cdot}w$ умножений, w сложений, w присвоений.

Во втором случае $i < n'$ размер символа больше либо равен размеру слова, а размер блока и полублока больше размера слова. Поэтому нужно переставлять символы по словам целиком, при этом размер символа в словах будет $s_w = 2^{i-n'}$. Всего блоков будет $b_c = 2^{n-j-1}$ размером $b_w = 2^{j+1-n'}$ слов. В каждом блоке должны обрабатываться четвёрки символов так, что одна пара относится к младшему полублоку, а вторая – к старшему. Всего пар символов в полублоке будет $sb_{ps} = \frac{2^{j+1}/2}{2^i}/2 = 2^{j-i-1}$, и размер каждой пары в словах составит $ps_w = s_w = 2^{i-n'+1}$. Младший символ в первой паре и старший символ во второй паре неподвижны, остальные подвижны. Подвижные символы сдвигаются на значение $\left|2^j - 2^i\right|$, что в пересчёте в словах составляет $val_w = 2^{j-n'} - 2^{i-n'}$. Откуда имеем $y'_{idx} = y_{idx}$, $y'_{idx+s_w} = y_{idx+s_w+val_w}$, $y'_{idx+s_w+val_w} = y_{idx+s_w}$ и $y'_{idx+2{\cdot}s_w+val_w} = y_{idx+2{\cdot}s_w+val_w}$, где $idx = v{\cdot}b_w{+}p{\cdot}ps_w{+}u$ – базовый индекс слова четвёрки слов каждого блока $v\colon 0 \leqslant v < b_c$ каждой пары символов полублока $p\colon 0 \leqslant p < sb_{ps}$ каждого слова символа $u\colon 0 \leqslant u < s_w$. Все результирующие слова нужно обработать в любом порядке (допустима параллельная обработка по всем u, p, v). Всего будет затрачено (исходя из преобразования одного слова) w присвоений. Что и требовалось доказать. □

Алгоритм 3.4 (*Об эквиморфном вычислении действия* D_n).

Вход: бинарный вектор $y \in E^k$ длины k и значения $i, j\colon 0 \leqslant i < j < n$.

Выход: бинарный вектор $y' \in E^k$ длины k.

Для эквиморфного вычисления БВ $y' \in E^k$ длины k, эквивалентного БФ $f^{(c_i(i,j))}$ (результату действия элемента $(c_i(i,j)) \in D_n$ над БФ $f \in B(n)$, заданной в виде эквивалентного БФ $y \in E^k$ длины k) нужно выполнить шаги:

а) разбить БВ y, y' на слова. Если $j < n'$, то перейти к шагу *б*, иначе если $i < n'$, то перейти к шагу *в*, иначе перейти к шагу *г*;

б) $\forall u\colon 0 \leqslant u < w$ вычислить $y'_u = (y_u \mathrm{st}_{\mathrm{lo}} \ll s_E) \vee (y_u \mathrm{st}_{\mathrm{hi}} \gg s_E) \vee (y_u \mathrm{lo} \ll val_E) \vee$ $\vee (y_u \mathrm{hi} \gg val_E)$, где $w_b = 2^{n'-j-1}$, $sb_{ps} = 2^{j-i-1}$, $\mathrm{st}_{\mathrm{lo}} = \{\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{0\ldots0}_{s_E}}^{sb_{ps}}\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{1\ldots1}_{s_E}}^{sb_{ps}}\}^{w_b}$, $\mathrm{st}_{\mathrm{hi}} = \{\overbrace{\underbrace{1\ldots1}_{s_E}\underbrace{0\ldots0}_{s_E}}^{sb_{ps}}\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{0\ldots0}_{s_E}}^{sb_{ps}}\}^{w_b}$, $\mathrm{lo} = \{\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{0\ldots0}_{s_E}}^{sb_{ps}}\overbrace{\underbrace{1\ldots1}_{s_E}\underbrace{0\ldots0}_{s_E}}^{sb_{ps}}\}^{w_b}$, $\mathrm{hi} = \{\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{1\ldots1}_{s_E}}^{sb_{ps}}\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{0\ldots0}_{s_E}}^{sb_{ps}}\}^{w_b}$, $val_E = 2^j$. Завершить алгоритм;

в) $\forall v, u\colon 0 \leqslant v < b_c, 0 \leqslant u < sb_w$ вычислить $y'_{idx} = (y_{idx} \mathrm{st}_{\mathrm{lo}} \ll s_E) \vee$ $\vee y_{idx+sb_w} \mathrm{hi}$ и $y'_{idx+sb_w} = (y_{idx+sb_w} \mathrm{st}_{\mathrm{hi}} \gg s_E) \vee y_{idx} \mathrm{lo}$, где $idx = v \cdot b_w + u$, $s_E = 2^i$, $w_{ps} = 2^{n'-i-1}$, $\mathrm{st}_{\mathrm{lo}} = \{\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{1\ldots1}_{s_E}}^{w_{ps}}\}$, $\mathrm{st}_{\mathrm{hi}} = \{\overbrace{\underbrace{1\ldots1}_{s_E}\underbrace{0\ldots0}_{s_E}}^{w_{ps}}\}$, $\mathrm{lo} = \{\overbrace{\underbrace{1\ldots1}_{s_E}\underbrace{0\ldots0}_{s_E}}^{w_{ps}}\}$, $\mathrm{hi} = \{\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{1\ldots1}_{s_E}}^{w_{ps}}\}$, $b_c = 2^{n-j-1}$, $b_w = 2^{j+1-n'}$, $sb_w = 2^{j-n'}$. Завершить алгоритм;

г) $\forall v, p, u\colon 0 \leqslant v < b_c, 0 \leqslant p < sb_{ps}, 0 \leqslant u < s_w$ вычислить $y'_{idx} = y_{idx+s_w+val_w}$, $y'_{idx+s_w} = y_{idx}$, $y'_{idx+s_w+val_w} = y_{idx+2 \cdot s_w+val_w}$ и $y'_{idx+2 \cdot s_w+val_w} = y_{idx+s_w}$, где $idx = v \cdot b_w + p \cdot ps_w + u$, $s_w = 2^{i-n'}$, $b_c = 2^{n-j-1}$, $b_w = 2^{j+1-n'}$, $sb_{ps} = 2^{j-i-1}$, $ps_w = 2^{i+1-n'}$ и $val_w = 2^{j-n'} - 2^{i-n'}$. Завершить алгоритм. □

Теорема 3.5 (*Об эквиморфном вычислении действия* D_n). *Вычисление БВ $y \in E^k$, эквивалентного БФ $f \in B(n)$, по алгоритму 3.4 равносильно действию эквиморфизма $\varphi_{(c_i(i,j))}$ над ним, получаемого по теореме 2.1. Число операций эквиморфного вычислителя для $j < n'$ составит $4 \cdot w$ сдвигов, $4 \cdot w$ умножений, $3 \cdot w$ сложений, w присвоений, а для $j \geqslant n'$ при $i < n'$ – w сдвигов, $2 \cdot w$ умножений, w сложений, w присвоений, и при $i \geqslant n'$ – w присвоений.*

Доказательство. Согласно теореме 2.1, эквиморфизм $\varphi_{(c_i(i,j))}$ для типа А раскроется как $\varphi^{-1}_{(i,j)}\varphi^{-1}_{c_i} = \varphi_{(i,j)}\varphi_{c_i}$, потому что элементы c_i и (i,j) – инволюции. Согласно лемме 1.1$^{\text{А}}$, получим $y^{\varphi_{(i,j)}\varphi_{c_i}} = (y^{\varphi_{(i,j)}})^{\varphi_{c_i}}$. Для типа Б раскроется как $\varphi_{c_i}\varphi_{(i,j)}$, и тогда по лемме 1.1$^{\text{Б}}$ верно $y^{\varphi_{c_i}\varphi_{(i,j)}} = (y^{\varphi_{(i,j)}})^{\varphi_{c_i}}$. Откуда заключаем, что преобразование по алгоритму 3.4 должно быть равносильно последовательному действию алгоритма 3.3 и алгоритма 3.2. Для доказательства этого будем опираться на доказательства теоремы 3.4 и теоремы 3.3 и совместим их шаги. Это можно выполнить двумя способами: непосредственной композицией расчётных формул шагов алгоритмов или качественным анализом перестановок символов. Далее рассматривается способ качественного анализа. Отметим, что во всех шагах алгоритмов размеры символов совпадают.

Для случая $j < n'$ за основу возьмём формулу шага *б* алгоритма 3.3 $y'_u = y_u\text{st} \vee (y_u\text{lo} \ll val_E) \vee (y_u\text{hi} \gg val_E)$. При последующем действии над y'_u согласно теореме 3.3 соответственные чётные и нечётные символы должны быть переставлены. Неподвижные символы младших(его) и старших(его) полублоков должны дополнительно сдвинуться на размер символа в битах. Для этого слагаемое $y_u\text{st}$ нужно заменить на $(y_u\text{st}_\text{lo} \ll s_E) \vee (y_u\text{st}_\text{hi} \gg s_E)$, где $\text{st}_\text{lo} = \{\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{0\ldots0}_{s_E}}^{sb_{ps}}\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{1\ldots1}_{s_E}}^{sb_{ps}}\}^{w_b}$ и $\text{st}_\text{hi} = \{\overbrace{\underbrace{1\ldots1}_{s_E}\underbrace{0\ldots0}_{s_E}}^{sb_{ps}}\overbrace{\underbrace{0\ldots0}_{s_E}\underbrace{0\ldots0}_{s_E}}^{sb_{ps}}\}^{w_b}$ константы для выделения неподвижных символов младших(его) и старших(его) полублоков соответственно. Подвижные символы в y'_u должны также сдвинуться на значение размера символа. Поэтому значение сдвига символов должно быть скорректировано с $2^j - 2^i$ на $val_E = 2^j$. Откуда получаем $y'_u = (y_u\text{st}_\text{lo} \ll s_E) \vee (y_u\text{st}_\text{hi} \gg s_E) \vee (y_u\text{lo} \ll val_E) \vee (y_u\text{hi} \gg val_E)$. Остальные константы, включая lo и hi, соответствуют шагу *б* алгоритма 3.3. Всего будет затрачено (исходя из преобразования одного слова): $4{\cdot}w$ сдвигов, $4{\cdot}w$ умножений, $3{\cdot}w$ сложений, w присвоений.

Для случая $j \geqslant n'$, так же как и в теореме 3.4, возможно два варианта. В первом варианте $i < n'$ константы будут эквивалентны шагу *в* алгоритма 3.3, но расчётные формулы $y'_{idx} = y_{idx}\text{st}_\text{lo} \vee (y_{idx+sb_w}\text{hi} \ll s_E)$ и $y'_{idx+sb_w} = y_{idx+sb_w}\text{st}_\text{hi} \vee$

$\vee(y_{idx}\mathrm{lo} \gg s_E)$ нужно заменить на $y'_{idx} = (y_{idx}\mathrm{st_{lo}} \ll s_E) \vee y_{idx+sb_w}\mathrm{hi}$ и $y'_{idx+sb_w} = = (y_{idx+sb_w}\mathrm{st_{hi}} \gg s_E) \vee y_{idx}\mathrm{lo}$, потому что чётные и нечётные символы должны быть переставлены согласно теореме 3.3; неподвижные символы младш(их)его полублоков(а) сдвинуться влево, старших(его) – вправо. Аналогично для подвижных символов. Отметим, что для них дополнительный сдвиг слова на символ эквивалентен его отсутствию, потому что значение сдвига есть разность $sb_w{=}2^j$ минус $s_E{=}2^i$. В результате значение сдвига только sb_w. Сложность этого алгоритма эквивалентна сложности алгоритма 3.3 для случая $j{\geqslant}n'$ и $i{<}n'$.

Во втором варианте $i \geqslant n'$ константы будут равны шагу e алгоритма 3.3, но расчётные формулы $y'_{idx} = y_{idx}$, $y'_{idx+s_w} = y_{idx+s_w+val_w}$, $y'_{idx+s_w+val_w} = y_{idx+s_w}$ и $y'_{idx+2\cdot s_w+val_w} = y_{idx+2\cdot s_w+val_w}$ должны быть заменены на $y'_{idx} = y_{idx+s_w+val_w}$, $y'_{idx+s_w} = y_{idx}$, $y'_{idx+s_w+val_w} = y_{idx+2\cdot s_w+val_w}$ и $y'_{idx+2\cdot s_w+val_w} = y_{idx+s_w}$, потому что чётные и нечётные символы должны быть переставлены согласно теореме 3.3. Применительно к этому варианту должны быть попарно переставлены исходные слова. Сложность эквивалентна сложности алгоритма 3.3 для случая $i{\geqslant}n'$. Что и требовалось доказать. □

§ 3.5. Выводы

Предложена модель канонического представления элемента группы Джевонса, и на её основе создан эффективный алгоритм решения уравнения. Для проверки ИТР, реализующих предлагаемый алгоритм, приводятся контрольный пример вычисления решения уравнения для БФ четырёх аргументов и контрольные примеры рассматриваемых представлений подстановок и элементов группы Джевонса.

Предложен эквиморфный вычислитель, основывающийся на эквиморфизме группы Джевонса и β_n группы. Для него разработаны алгоритмы, позволяющие в сотни раз повысить эффективность вычисления действий элементов группы Джевонса над БФ. Даны методические рекомендации к реализации эквиморфного вычислителя на ИТР. Основные результаты главы 3 опубликованы в [62, 66, 68, 69, 71].

Глава 4. Оценки сложности предложенных решений

В главе 4 рассматриваются различные подходы к оценке сложности предлагаемого алгоритма. Приводятся теоретические оценки максимального и минимального числа действий при вычислении решения уравнения. Для практического использования алгоритма этого недостаточно, т.к. опыт показывает, что в подавляющем большинстве случаев число действий n^2+n. Это число зависит от тривиальности $J_{D_n}(f)$, поэтому проведён эмпирический анализ её тривиальности для всех БФ $n = 1, 2, 3, 4, 5$ и теоретический анализ для любого n.

Предлагается метод спектрального анализа для оценки числа действий при решении всех уравнений для $n = 4, 5$. Приводятся результаты эмпирических оценок числа действий миллионов уравнений для $5 < n < 24$, отражающих реальные данные. Формулируются предположения о реальной сложности предлагаемого алгоритма и о возможности его применения для решения прикладных задач. Исследование проводилось с применением ИТР, основывающихся на специально разработанной библиотеке ***domain object processor*** (или **dop**).

§ 4.1. Теоретические оценки сложности

Опираясь на формулу (3.6), можно рассчитать число действий для различных случаев использования алгоритма 3.1. Оценим возможное значение числа действий для максимальных r_i. Из шага a алгоритма 3.1 верно, что $r_0 \equiv 1$. Если принять, что на каждой итерации алгоритма 3.1 необходимые условия выполняются для всех гипотез, то остальные r_i можно рассчитать рекуррентно, как $r_i = 2 \cdot (n - (i-1)) \cdot r_{i-1}$:

$r_0 = 1,$

$r_1 = 2 \cdot (n - (1-1)) \cdot 1 = 2 \cdot n,$

$r_2 = 2 \cdot (n - (2-1)) \cdot 2n = 2(n-1) \cdot 2n,$

$r_3 = 2 \cdot (n - (3-1)) \cdot 2(n-1) \cdot 2n = 2(n-2) \cdot 2(n-1) \cdot 2n,$

$\vdots$

$r_i = 2^i \cdot \frac{n!}{(n-i)!}.$

Откуда число действий по формуле (3.6) примет следующий вид:

$$d_{max} = \sum_{i=0}^{n-1} 2^i \cdot \frac{n!}{(n-i)!} \cdot 2 \cdot (n-i). \tag{4.1}$$

Нетрудно видеть, что последнее слагаемое суммы (4.1) есть $2^n \cdot n!$ (порядок группы Джевонса и сложность тривиального алгоритма). Откуда можно заключить, что сложность предлагаемого алгоритма 3.1, без отбраковки гипотез (эквивалент тривиального алгоритма) превосходит сложность тривиального. Такое заключение не верно, потому что значения r_i зависят друг от друга, т.к. группа Джевонса действует интранзитивно, и не могут появиться промежуточные функции, не принадлежащие одному классу D_n-эквивалентности. Например, для БФ $f(x_{n-1}, \ldots, x_i, \ldots, x_0) \equiv 0$ значения r_i на каждом шаге действительно максимальны, но при этом все промежуточные функции совпадают, поэтому для такой БФ можно принять, что $r_i \equiv 1, \forall i$. Промежуточные функции принадлежат одному и тому же классу D_n-эквивалентности, поэтому заключим, что $d_{max} = d_{trivial} = 2^n \cdot n!$.

Аналогично можно оценить минимальное число действий алгоритма 3.1. Оно будет соответствовать значениям $r_i \equiv 1, \forall i$ и может быть рассчитано (как арифметическая прогрессия) следующим образом:

$$d_{min} = \sum_{i=0}^{n-1} 2 \cdot (n-i) = 2 \cdot n \cdot \frac{(n-0) + (n-(n-1))}{2} = n^2 + n. \tag{4.2}$$

Значения r_i из формулы (4.1) являются только теоретическими. Опыт показывает, что реальные значения r_i соизмеримы со значениями из формулы (4.2). На момент написания настоящей работы теоретические оценки значений r_i не получены, но рассчитаны их эмпирические значения при решении уравнения (3.1). Основываясь на этих эмпирических значениях, сформулируем ряд предположений о том, что сложность решения уравнения (3.1) соизмерима, в подавляющем большинстве случаев, с минимальной оценкой по формуле (4.2). Для получения эмпирических значений r_i разработан метод спектрального анализа БФ.

Для постановки численных экспериментов была разработана библиотека

domain operations processor (или **dop**). Она содержит набор алгоритмов, специализированных для обработки подстановок и их действий на бинарных векторах и булевых функциях [46]. Библиотека распространяется под лицензией *GNU LGPL* (*GNU Lesser General Public License*). **dop** написана на языке C++ в виде системы функций и макросов для архитектуры процессора IA-32 [47, 48, 49, 50]. Библиотека является кроссплатформенной [51], т.к. не использует программный интерфейс Windows [52, 53] или POSIX [54] подобных систем. Библиотека включает в себя: инструменты ввода-вывода объектов, обработки (групповые операции, изоморфизмы, антиизоморфизмы, действия и пр.), перечисления объектов (для построения стендов при исследовании предметной области), средства рандомизации. Состав библиотеки включает документацию разработчика (*Software Development Kit* или *SDK*).

Для дальнейшего изложения потребуются единицы количества информации. Согласно [55], величинами единиц информации являются 1 КБайт (килобайт), 1 МБайт (мегабайт) и 1 ГБайт (гигобайт), – равны 2^{10} байт, 2^{20} байт и 2^{30} байт соответственно. При этом указанный документ вступает в противоречие с [56] и [57], где соответственные степени двойки названы 1 КиБайт (кибибайт), 1 МиБайт (мебибайт) и 1 ГиБайт (гибибайт), а обычные приставки кило-, мега- и гига- используются для обозначения десятичных множителей 10^3, 10^6 и 10^9 соответственно. Последний указанный документ является международным стандартом МЭК (*IEC*) и, чтобы не допустить разночтений, далее будут использоваться единицы количества информации из него.

Библиотека **dop** может работать с бинарными векторами длиной до 2^{31} включительно, т.е. $2^3 \cdot 2^{20} \cdot 2^8$ бит или 256 МиБ.

§ 4.2. Анализ тривиальности подгрупп инерции булевых функций

В настоящем изложении будут рассмотрены классификации относительно веса БФ, инверсии БФ и действия групп E_n, S_n и D_n. Далее потребуется определение из [2].

Определение 4.1. *Вес Хемминга булева вектора* $x \in E^n$ *– количество*

значений 1 в нём. В символьном виде будем обозначать как $Weight(x)$.

Аналогично с определением 4.1 можно определить вес БФ, как вес Хемминга, эквивалентного ей БВ. Представление БФ в виде эквивалентного вектора (2.8) не требует наличия формулы БФ, но хранить эту информацию в виде нулей и единиц неудобно. Более того, этот способ порождает ошибки при вычислениях, т.к. длины векторов экспоненциально зависят от n, и их элементами являются только нули и единицы. Начиная с $n > 1$, длина вектора (2.8) кратна четырём, и БВ может быть записан тетрадами значений. Предлагается для удобства использовать шестнадцатеричную систему записи тетрад.

Таблица 4.1. Кодирования значений бинарного вектора

Binary	***Hexadecimal***	***Decimal***	***Weight***	***Binary***	***Hexadecimal***	***Decimal***	***Weight***
0000	0	0	0	1000	8	8	1
0001	1	1	1	1001	9	9	2
0010	2	2	1	1010	a	10	2
0011	3	3	2	1011	b	11	3
0100	4	0	1	1100	c	12	2
0101	5	1	2	1101	d	13	3
0110	6	2	2	1110	e	14	3
0111	7	3	3	1111	f	15	4

В табл. 4.1 приведено соответствие двоичных, десятичных, шестнадцатеричных значений, а также вес Хемминга тетрады. Например, вышеописанная в примерах функция (см. табл. 2.3) f будет представлена как $\{7840\}$, и результат действия над ней $f^{(z_0\pi)}$ будет представлен для типа А $\{08a3\}$ и для типа Б $\{8c06\}$. Условимся в дальнейшем применять шестнадцатеричную запись для БВ, эквивалентных БФ, и двоичную запись для их аргументов.

Определение 4.2. *Имя булевой функции есть эквивалентный ей бинарный вектор в нотации L2R.*

Начнём классификацию БФ в настоящем изложении по весу Хемминга имён БФ. Согласно определению 4.1, вес БФ $f \in B(n)$ принимает целочисленные значения $0 \leqslant Weight(f) \leqslant k$. Всё множество БФ по признаку одинакового веса Хемминга разобьётся на классы эквивалентности. Определим такие классы следующим образом.

Определение 4.3. *Класс* $W_k^j = \{f \in B(n) \mid Weight(f) = j\}, \forall j \in [0; k]$.

Мощность классов W_k^j можно рассчитать комбинаторно как $|W_k^j| = C_k^j = \frac{k!}{j!(k-j)!}$. Всего таких классов в множестве БФ будет $k+1$. Любая функция из класса W_n^j может быть получена из одного его представителя действием над ним элементом группы S_k. Подходящие представители всех классов $W_{2^n}^j$ могут быть получены непосредственно из значения веса с линейной сложностью от n. Такими представителями являются функции вида $\{00\ldots11\}$ и $\{11\ldots00\}$. Например, для $n=4$ представителями будут (для удобства в двоичном виде): $\{0000\}$, $\{0001\}$, $\{0011\}$, $\{0111\}$ и $\{1111\}$, $\{1110\}$, $\{1100\}$ и $\{1000\}$.

Далее перейдём к классификации БФ по группе Джевонса и её подгруппам. Стоит отметить, что действие этих групп на множестве БФ разбивает на классы не только всё их множество, но и классы W_k^j. Действия групп E_n, S_n и D_n над БФ не меняют её вес (согласно изоморфизму (1.8), изоморфизму ($1.9^{\text{А}}$) и изоморфизму ($1.9^{\text{Б}}$)). Каждой БФ можно поставить в соответствие инверсную функцию. Опираясь на свойство двойственности [4, 7], можно утверждать, что если два класса образованы БФ и функцией, ей инверсной соответственно, то они обладают одинаковыми свойствами. В результате достаточно анализировать только один класс (либо содержащий функцию, либо её инверсию).

Таблица 4.2. Краткая статистика по классам E_n для $n = 1, 2, 3, 4, 5$

n	1	2	3	4	5
Максимальное число функций в классе $\|E_n\| = 2^n$	2	4	8	16	32
Общее число классов	3	7	46	4336	134 281 216
среди них SN-классов	1	3	14	240	63 448
в т.ч. тривиальных классов	1	2	23	3 904	134 156 284
среди них тривиальных SN-классов	1	0	7	120	58 652
в т.ч. нетривиальных классов	2	5	23	432	124 932
среди них нетривиальных SN-классов	0	3	7	120	4 796
Максимальное число функций в двойном классе	4	8	16	32	64
Общее число двойных классов	2	5	30	2 288	67 172 332
в т.ч. тривиальных двойных классов	1	1	15	2 012	67 107 468
в т.ч. нетривиальных двойных классов	1	4	15	276	64 864
Общее число функций $\|B(n)\|$	4	16	256	65536	4 294 967 296
в т.ч. с тривиальной подгруппой инерции	2	8	184	62 464	4 293 001 088
в т.ч. с нетривиальной подгруппой инерции	2	8	72	3 072	1 966 208

Определение 4.4. *Класс G-эквивалентных булевых функций (или класс БФ) – подмножество всего множества БФ, в котором все функции G-эквива-*

лентны. В символьном виде обозначим как f^G.

Определение 4.5. *Самоотрицательный класс булевых функций – класс БФ, который совпадает с классом их инверсий, т.е. верно* $f^G = \overline{f}^G$. *В символьном виде будем обозначать такие классы как SN.*

Определение 4.6. *Двойной класс булевых функций – объединение класса БФ и класса их инверсий. В символьном виде* $[f] = f^G \bigcup \overline{f}^G$.

Допуская вольность в речи, будем называть тривиальным классом БФ такой, чьи представители имеют тривиальную подгруппу инерции. В противном случае – нетривиальным классом. В табл. 4.2, табл. 4.3 и табл. 4.4 приведены краткие статистики классов эквивалентных БФ для $n = 1, 2, 3, 4, 5$ аргументов по группам E_n, S_n и D_n соответственно.

Таблица 4.3. Краткая статистика по классам S_n для $n = 1, 2, 3, 4, 5$

n	1	2	3	4	5
Максимальное число функций в классе $\lvert S_n \rvert = n!$	1	2	6	24	120
Общее число классов	4	12	80	3984	37 333 248
среди них *SN*-классов	0	0	0	0	0
в т.ч. тривиальных классов	4	4	16	1 792	34 339 072
среди них тривиальных *SN*-классов	0	0	0	0	0
в т.ч. нетривиальных классов	0	8	64	2 192	2 994 176
среди них нетривиальных *SN*-классов	0	0	0	0	0
Максимальное число функций в двойном классе	2	4	12	48	240
Общее число двойных классов	2	6	40	1 992	18 666 624
в т.ч. тривиальных двойных классов	2	2	8	896	17 169 536
в т.ч. нетривиальных двойных классов	0	4	32	1 096	1 497 088
Общее число функций $\lvert B(n) \rvert$	4	16	256	65536	4 294 967 296
в т.ч. с тривиальной подгруппой инерции	4	8	96	43 008	4 120 688 640
в т.ч. с нетривиальной подгруппой инерции	0	8	160	22 528	174 278 656

В табл. 4.2, табл. 4.3 и табл. 4.4 серым подсвечены графы, которые являются исходными данными таблиц, остальные вычисляются. Графа «Общее число классов» взята из [4], остальные исходные данные вычислены в рамках настоящей работы. Число нетривиальных классов может быть найдено простым вычитанием. Число двойных классов определяется как полусумма общего числа классов и числа SN-классов. Более полная статистика классов БФ приведена в приложении А. Из табл. 4.3 можно заключить, что SN-классы по группе S_n для 1,2,3,4 и 5 аргументов отсутствуют.

Определение 4.7. *Имя класса БФ – имя его представителя, эквива-*

лентный БВ которого имеет наименьшее ординальное (числовое) значение по формуле (1.3) среди всех других представителей этого же класса.

Таблица 4.4. Краткая статистика по классам D_n для $n = 1, 2, 3, 4, 5$

n	1	2	3	4	5
Максимальное число функций в классе $\lvert D_n \rvert = 2^n \cdot n!$	2	8	48	384	3 840
Общее число классов	3	6	22	402	1 228 158
среди них SN-классов	1	2	6	42	4 094
в т.ч. тривиальных классов	1	0	0	59	1 022 524
среди них тривиальных SN-классов	1	0	0	11	2 664
в т.ч. нетривиальных классов	2	6	22	343	205 634
среди них нетривиальных SN-классов	0	2	6	31	1 430
Максимальное число функций в двойном классе	4	16	96	7687 680	
Общее число двойных классов	2	4	14	222	616 126
в т.ч. тривиальных двойных классов	1	0	0	35	512 594
в т.ч. нетривиальных двойных классов	1	4	14	187	103 532
Общее число функций $\lvert B(n) \rvert$	4	16	256	65536	4 294 967 296
в т.ч. с тривиальной подгруппой инерции	2	0	0	22 656	3 926 492 160
в т.ч. с нетривиальной подгруппой инерции	2	16	256	42 880	368 475 136

Каталоги имён классов БФ по группам E_n, S_n и D_n для $n = 1, 2, 3, 4$ аргументов с указанием весов и мощностей приведены в приложении Б. Классы в каталогах сгруппированы таким образом, что перечислены в том числе и двойные классы. Из статистики классов и каталогов классов можно заключить, что число БФ с нетривиальной подгруппой инерции в группах E_n, S_n и D_n при увеличении n пренебрежимо мало. Опираясь на выводы теории перечислений Пойа [4, 20, 35], можно заключить, что при $n \to \infty$ доля БФ с нетривиальными подгруппами инерции будет близка к нулю. Мощность множества гипотез при переходе от итерации к итерации в алгоритме 3.1 в соответствии с теоремой 3.2 достигает порядка подгруппы инерции БФ. В результате можно заключить, что в подавляющем большинстве случаев этого не произойдёт.

§ 4.3. Спектральный анализ булевых функций

Для эмпирической оценки сложности алгоритма 3.1 нужно рассчитать числа r_i из формулы (3.6) для любой пары функций f, g из уравнения (3.1). Даже для небольших значений n это вычислительно сложно, т.к. таких пар будет $\left(2^{2^n}\right)^2 = 2^{2^{n+1}}$. Спектральный анализ БФ позволяет снизить вычислительные затраты настолько, что числа r_i могут быть рассчитаны за время $O\left(2^{2^n}\right)$.

Таблица 4.5. Преобразование алгоритма 3.1 для спектрального анализа

Итерация i–1	**Итерация i**	**Итерация i+1**
Q_{i-1}, $f^{H_{i-1}} = \{f_0, f_1, ..., f_v, ..., f_{r_{i-1}-1}\}$, $\lvert H_{i-1}\rvert = r_{i-1}$	$Q_{i,0}$, $f^{H_{i,0}} = \{f_{0,0}, f_{0,1}, ..., f_{0,v_0}, ..., f_{0,r_{i,0}-1}\}$ $\lvert H_{i,0}\rvert = r_{i,0}$	$Q_{i+1,0,0}, f^{H_{i+1,0,0}} = \{f_{0,0,0}, f_{0,0,1}, ..., f_{0,0,v_{0,0}}, ..., f_{0,0,r_{i+1,0,0}-1}\}$, $\lvert H_{i+1,0,0}\rvert = r_{i+1,0,0}$
		$Q_{i+1,0,1}, f^{H_{i+1,0,1}} = \{f_{0,1,0}, f_{0,1,1}, ..., f_{0,1,v_{0,1}}, ..., f_{0,1,r_{i+1,0,1}-1}\}$, $\lvert H_{i+1,0,1}\rvert = r_{i+1,0,1}$
		⋮
		$Q_{i+1,0,u_0}, f^{H_{i+1,0,u_0}} = \{f_{0,u_0,0}, f_{0,u_0,1}, ..., f_{0,u_0,v_{0,u_0}}, ..., f_{0,u_0,r_{i+1,0,u_0}-1}\}$, $\lvert H_{i+1,0,u_0}\rvert = r_{i+1,0,u_0}$
		⋮
		$Q_{i+1,0,w_0-1}, f^{H_{i+1,0,w_0-1}} = \{f_{0,w_0-1,0}, f_{0,w_0-1,1}, ..., f_{0,w_0-1,v_{0,w_0-1}}, ..., f_{0,w_0-1,r_{i+1,0,w_0-1}-1}\}$, $\lvert H_{i+1,0,w_0-1}\rvert = r_{i+1,0,w_0-1}$
	$Q_{i,1}$, $f^{H_{i,1}} = \{f_{1,0}, f_{1,1}, ..., f_{1,v_1}, ..., f_{1,r_{i,1}-1}\}$ $\lvert H_{i,1}\rvert = r_{i,1}$	$Q_{i+1,1,0}, f^{H_{i+1,1,0}} = \{f_{1,0,0}, f_{1,0,1}, ..., f_{1,0,v_{1,0}}, ..., f_{1,0,r_{i+1,1,0}-1}\}$, $\lvert H_{i+1,1,0}\rvert = r_{i+1,1,0}$
		$Q_{i+1,1,1}, f^{H_{i+1,1,1}} = \{f_{1,1,0}, f_{1,1,1}, ..., f_{1,1,v_{1,1}}, ..., f_{1,1,r_{i+1,1,1}-1}\}$, $\lvert H_{i+1,1,1}\rvert = r_{i+1,1,1}$
		⋮
		$Q_{i+1,1,u_1}, f^{H_{i+1,1,u_1}} = \{f_{1,u_1,0}, f_{1,u_1,1}, ..., f_{1,u_1,v_{1,u_1}}, ..., f_{1,u_1,r_{i+1,1,u_1}-1}\}$, $\lvert H_{i+1,1,u_1}\rvert = r_{i+1,1,u_1}$
		⋮
		$Q_{i+1,1,w_1-1}, f^{H_{i+1,1,w_1-1}} = \{f_{1,w_1-1,0}, f_{1,w_1-1,1}, ..., f_{1,w_1-1,v_{1,w_1-1}}, ..., f_{1,w_1-1,r_{i+1,1,w_1-1}-1}\}$, $\lvert H_{i+1,1,w_1-1}\rvert = r_{i+1,1,w_1-1}$
	⋮	⋮
	$Q_{i,u}$, $f^{H_{i,u}} = \{f_{u,0}, f_{u,1}, ..., f_{u,v_u}, ..., f_{u,r_{i,u}-1}\}$ $\lvert H_{i,u}\rvert = r_{i,u}$	$Q_{i+1,u,0}, f^{H_{i+1,u,0}} = \{f_{u,0,0}, f_{u,0,1}, ..., f_{u,0,v_{u,0}}, ..., f_{u,0,r_{i+1,u,0}-1}\}$, $\lvert H_{i+1,u,0}\rvert = r_{i+1,u,0}$
		$Q_{i+1,u,1}, f^{H_{i+1,u,1}} = \{f_{u,1,0}, f_{u,1,1}, ..., f_{u,1,v_{u,1}}, ..., f_{u,1,r_{i+1,u,1}-1}\}$, $\lvert H_{i+1,u,1}\rvert = r_{i+1,u,1}$
		⋮
		$Q_{i+1,u,u_u}, f^{H_{i+1,u,u_u}} = \{f_{u,u_u,0}, f_{u,u_u,1}, ..., f_{u,u_u,v_{u,u_u}}, ..., f_{u,u_u,r_{i+1,u,u_u}-1}\}$, $\lvert H_{i+1,u,u_u}\rvert = r_{i+1,u,u_u}$
		⋮
		$Q_{i+1,u,w_u-1}, f^{H_{i+1,u,w_u-1}} = \{f_{u,w_u-1,0}, f_{u,w_u-1,1}, ..., f_{u,w_u-1,v_{u,w_u-1}}, ..., f_{u,w_u-1,r_{i+1,u,w_u-1}-1}\}$, $\lvert H_{i+1,u,w_u-1}\rvert = r_{i+1,u,w_u-1}$
	⋮	⋮
	$Q_{i,w-1}$, $f^{H_{i,w-1}} = \{f_{w-1,0}, f_{w-1,1}, ..., f_{w-1,v_{w-1}}, ..., f_{w-1,r_{i,w-1}-1}\}$, $\lvert H_{i,w-1}\rvert = r_{i,w-1}$	$Q_{i+1,w-1,0}, f^{H_{i+1,w-1,0}} = \{f_{w-1,0,0}, f_{w-1,0,1}, ..., f_{w-1,0,v_{w-1,0}}, ..., f_{w-1,0,r_{i+1,w-1,0}-1}\}$, $\lvert H_{i+1,w-1,0}\rvert = r_{i+1,w-1,0}$
		$Q_{i+1,w-1,1}, f^{H_{i+1,w-1,1}} = \{f_{w-1,1,0}, f_{w-1,1,1}, ..., f_{w-1,1,v_{w-1,1}}, ..., f_{w-1,1,r_{i+1,w-1,1}-1}\}$, $\lvert H_{i+1,w-1,1}\rvert = r_{i+1,w-1,1}$
		⋮
		$Q_{i+1,w-1,u_{w-1}}, f^{H_{i+1,w-1,u_{w-1}}} = \{f_{w-1,u_{w-1},0}, f_{w-1,u_{w-1},1}, ..., f_{w-1,u_{w-1},v_{w-1,u_{w-1}}}, ..., f_{w-1,u_{w-1},r_{i+1,w-1,u_{w-1}}-1}\}$, $\lvert H_{i+1,w-1,u_{w-1}}\rvert = r_{i+1,w-1,u_{w-1}}$
		⋮
		$Q_{i+1,w-1,w_{w-1}-1}, f^{H_{i+1,w-1,w_{w-1}-1}} = \{f_{w-1,w_{w-1}-1,0}, f_{w-1,w_{w-1}-1,1}, ..., f_{w-1,w_{w-1}-1,v_{w-1,w_{w-1}-1}}, ..., f_{w-1,w_{w-1}-1,r_{i+1,w-1,w_{w-1}-1}-1}\}$, $\lvert H_{i+1,w-1,w_{w-1}-1}\rvert = r_{i+1,w-1,w_{w-1}-1}$
–	$\tilde{r}_i = \max\limits_{u=0}^{w-1}(r_{i,u})$	$\tilde{r}_{i+1} = \max\limits_{u=0}^{w-1}\left(\max\limits_{u_u=0}^{w_u-1}(r_{i+1,u,u_u})\right)$

В результате для анализа при $n = 5$ потребуется перебрать не 2^{64} пар функций, а всего лишь 2^{32}. Суть спектрального анализа сводится к следующему. Зафиксируем функцию f и пусть g – произвольно, т.е. рассмотрим сразу все уравнения (3.1) с участием f (для заданного n). Тогда все спектры промежуточных функций $Q_i(f^h)$ на каждой итерации алгоритма 3.1 будут соответствовать всем допустимым g (допустимым, т.е. на итерации i множество гипотез H_i ещё не пусто). Отдельно стоит рассмотреть ситуацию отсутствия решения уравнения (3.1). При ней произойдёт прерывание алгоритма 3.1 (пустое множество H_i) на какой-то итерации i. Числа r_i будут так же показывать количество действий группы Джевонса на БФ, но их будет не полный набор, т.е. в формуле (3.6) верхняя граница суммы будет меньше $n{-}1$. Поэтому сложность алгоритма для пары не D_n-эквивалентных функций f, g будет меньше, чем сложность для пары D_n-эквивалентных.

Для спектрального анализа нужно преобразовать итерации алгоритма 3.1 согласно следующей модели. В табл. 4.5 приведена модель преобразования итерации i для удобства её изложения. На каждой итерации i алгоритма 3.1 производятся действия над промежуточными функциями множества гипотез $f^{H_{i-1}}$ вида $f_v^{(b_i(i,j_i))}, \forall b_i \in \{e_E, c_i\}, i \leqslant j_i < n, 0 \leqslant v < r_{i-1}$, где r_{i-1} – мощность множества гипотез предыдущей итерации $i{-}1$, и всего таких действий будет $r_{i-1} \cdot 2 \cdot (n-i)$ (см. левый столбец табл. 4.5). Полученные в результате промежуточные функции не исключаются согласно шагу *в* алгоритма 3.1, а группируются по спектрам. Пусть результирующее множество промежуточных функций $f^{(b_i(i,j_i))H_{i-1}}$ разбивается на классы эквивалентности $f^{H_{i,u}}$ по отношению равенства спектров и пусть таких классов будет w и $0 \leqslant u < w{-}1$. Их спектры обозначим $Q_{i,u}$ соответственно. Промежуточную функции в таком классе будем обозначать двумя индексами как f_{u,v_u}, где v_u – индекс БФ внутри класса $f^{H_{i,u}}$ и $0 \leqslant v_u < r_{i,u}$ (см. центральный столбец табл. 4.5).

В общем случае классы $f^{H_{i,u}}$ не равномощны (т.е. числа $r_{i,u}$ могут быть различны). Максимальное число действий группы Джевонса на итерации $i{+}1$

будет соответствовать максимальному числу $r_{i,u}$. Определим максимум как $\tilde{r}_i = \max_{u=0}^{w-1}(r_{i,u})$. Очевидно, что независимо от того, какой будет функция g в уравнении (3.1), число гипотез на итерации i строго меньше $\tilde{r}_i$, и это значение допустимо использовать при расчёте сложности (3.6). Модель, представленная в табл. 4.5, отражает первую итерацию алгоритма 3.1 (когда на входе только одно множество гипотез H_0). На следующих итерациях на вход уже будет подаваться множество множеств гипотез $\{H_{i,0}, H_{i,1}, ..., H_{i,u}, ..., H_{i,w-1}\}$.

Каждое из указанных множеств $H_{i,u}$ отражает какие-то конкретные g в уравнении (3.1), и обрабатывать на следующей итерации $i{+}1$ их нужно отдельно (см. правый столбец табл. 4.5). Над каждой промежуточной функцией будут выполняться действия $f_{u,v_u}^{(b_{i+1}(i+1,j_{i+1}))}, \forall b_{i+1} \in \{e_E, c_{i+1}\}, i{+}1 \leqslant j_{i+1} < n, 0 \leqslant v_u < r_{i,u}$, и всего таких действий будет $r_{i,u} \cdot 2 \cdot (n-i-1)$. В результате будут получены новые промежуточные функции $f^{H_{i+1,u}}$. Каждое из этих множеств также разобьётся на классы эквивалентности по отношению равенства спектров. Обозначим количества спектров для каждого $f^{H_{i+1,u}}$ как $w_0, w_1, ..., w_u, ..., w_{w-1}$. Сами классы будут иметь три индекса $f^{H_{i+1,u,u_u}}$, где u_u – индекс спектра внутри множества $f^{H_{i+1,u}}$, Q_{i+1,u,u_u} – спектры и верно $0 \leqslant u_u < w_u$. Промежуточные функции внутри классов эквивалентности также будут иметь три индекса $f_{u,u_u,v_{u,u_u}}$, где v_{u,u_u} – индекс функции внутри класса эквивалентности $f^{H_{i+1,u,u_u}}$ и $0 \leqslant v_{u,u_u} < r_{i+1,u,u_u}$. В результате для каждого $H_{i,u}$ получится множество значений $r_{i+1,u,0}, r_{i+1,u,1}, ..., r_{i+1,u,u_u}, ..., r_{i+1,u,w_u-1}$, и всего таких множеств будет w. В результате появляется трудность выбора конкретного r_{i+1}.

Можно выделить как минимум два направления преодоления этой трудности. Первое – вычислить по всем допустимым значениям $r_{i,u}$ такой вектор $r_{i,u}$, r_{i+1,u,u_u} и т.д., который будет давать максимальное значение сложности по формуле (3.6), – это и будет верхняя точная оценка сложности. Второе направление сводится к тому, чтобы выбрать просто максимальное из всех допустимых r_{i+1,u,u_u}. Если выбрать такой максимум на каждой итерации спектрального анализа, то сложность, рассчитанная по формуле (3.6), может быть больше

реальной, т.к. числа $r_{i+1,u}$ и r_{i+1,u,u_u} не всегда совместны. Покажем это на следующем примере: $r_{i,0} = 2, r_{i,0} = 8$, и для итерации $i{+}1$ возьмём максимумы $\max\limits_{u_0=0}^{w_0-1}(r_{i+1,0,u_0}) = 10$ и $\max\limits_{u_1=0}^{w_1-1}(r_{i+1,1,u_1}) = 4$. Точные верхние оценки будут для каждого вектора (в примере для упрощения рассматривается только два вектора) $2 \times 10 = 20$ и $8 \times 4 = 32$. Если же просто выбрать максимумы, на каждой итерации получится $8 \times 10 = 80$. Другими словами, второе направление даёт грубую верхнюю оценку сложности, но оно проще при расчётах. Для спектрального анализа БФ выбран второй способ, поэтому $\tilde{r}_{i+1} = \max\limits_{u=0}^{w-1}\left(\max\limits_{u_u=0}^{w_u-1}(r_{i+1,u,u_u})\right)$. В результате каждой БФ f поставлен в соответствие вектор $\tilde{r}_0, \tilde{r}_1, ..., \tilde{r}_{n-1}$, по значениям которого можно грубо оценить максимальную сложность сразу для всех уравнений (3.1) с участием f.

Следующим этапом является анализ выборки множества функций для заданного n. В результате анализа функции будут группироваться по значениям $\tilde{r}_i$ или набору таких чисел будет соответствовать некоторая доля БФ выборки. Тогда максимум для этих чисел для всей выборки покажет наихудший вариант применения алгоритма 3.1. Математическое ожидание чисел $\tilde{r}_i$ по долям выборки для таких группировок покажет среднюю сложность алгоритма 3.1.

Перед демонстрацией результатов спектрального анализа нужно показать причины наличия значений $\tilde{r}_i$, больших единицы. Из доказательства теоремы 3.2 можно заключить, что если уравнение (3.1) имеет больше одного решения, то на последнем шаге будет ровно столько же решений.

Наличие значения $\tilde{r}_i$ больше единицы может показывать, что для канонического представления (3.3) перебираются множители, входящие в элементы подгруппы инерции БФ в группе Джевонса $J_{D_n}(f)$, потому что будут выполняться условия теоремы 3.2. Такой рост сложности будет устойчивым до окончания работы алгоритма 3.1. Например, для БФ $f(x_{n-1}, \ldots, x_i, \ldots, x_0) \equiv 0$ $J_{D_n}(f)$ совпадает с группой Джевонса $J_{D_n}(f) = D_n$, и числа $\tilde{r}_i$ на каждой итерации алгоритма 3.1 имеют максимально допустимые значения.

Откуда можно заключить следующее. БФ с нетривиальной $J_{D_n}(f)$ могут

давать экспоненциальный рост сложности алгоритма 3.1. При этом сложность сопоставима с порядком $J_{D_n}(f)$. Верно и другое: мощность множества БФ с нетривиальной $J_{D_n}(f)$ стремится к нулю при $n \to \infty$. Это доказано в теории Пойа [4, 35], поэтому такими случаями можно пренебречь без потери общности. Более того, для функций с нетривиальной $J_{D_n}(f)$ нет необходимости хранить все гипотезы, и можно модифицировать алгоритм 3.1 так, что он будет вычислять порождающее множество $J_{D_n}(f)$. Это показано в предыдущем примере для $f(x_{n-1}, \ldots, x_i, \ldots, x_0) \equiv 0$.

В результате эмпирического анализа было показано, что для БФ с тривиальной $J_{D_n}(f)$ также значения $\tilde{r}_i$ могут быть больше единицы. При этом, исходя из мощности класса D_n-эквивалентных БФ, которая может быть выражена как индекс $[D_n : J_{D_n}(f)]$, на последней итерации алгоритма 3.1 остаётся ровно одна гипотеза, которая и является решением уравнения (3.1). Это позволяет заключить, что в процессе работы алгоритма 3.1 появляются ложные промежуточные решения, которые с каждой последующей итерацией отбраковываются.

При анализе всех БФ с тривиальной $J_{D_n}(f)$ для $n = 4, 5$ и некоторого числа (десятки миллионов) функций с бóльшим количеством аргументов выявлена только одна причина появления ложных промежуточных решений. На каждой итерации (кроме последней) алгоритма 3.1 не производится работа ни с промежуточными функциями f^h, ни с функцией g. Работа производится с их спектрами в соответствующих итерациям алфавитах A_{i+1}. Таким образом, вместо f^h и g рассматривается множество БФ, которые могут быть образованы перестановкой символов A_{i+1} в f^h и g. Другими словами, отображение БФ на спектр $A_i \colon i < n$ – сюръекция. Для проанализированного множества БФ выявлено, что если значение $\tilde{r}_i$ больше единицы, то среди прообразов спектров всегда присутствует БФ с нетривиальной $J_{D_n}(f)$. Более того, для такой БФ в её подгруппе инерции присутствует элемент, действующий на аргумент x_i. Таким образом, ложные промежуточные функции ложны в рамках всего алгоритма 3.1, но в рамках конкретной итерации такие промежуточные функ-

ции ожидаемы, т.к. алгоритм 3.1 «не может» отличить БФ f^h или g от других прообразов с нетривиальной $J_{D_n}(f)$.

В результате можно выдвинуть три предположения:

а) появление ложных промежуточных функций обусловлено сюръекцией БФ с тривиальной и нетривиальной $J_{D_n}(f)$ на один и тот же спектр, и именно БФ с нетривиальной $J_{D_n}(f)$ являются причиной $\tilde{r}_i > 1$;

б) в первом случае доля БФ, дающих ложные промежуточные решения при $n \to \infty$ стремиться к нулю, т.к. доля БФ с нетривиальной $J_{D_n}(f)$ также стремится к нулю. Более того, количество ложных промежуточных функций при работе алгоритма 3.1 должно экспоненциально падать от итерации к итерации, т.к. количество прообразов в сюръекции уменьшается экспоненциально с ростом индекса алфавита;

в) алгоритм 3.1 невозможно модифицировать так, чтобы его сложность строго соответствовала формуле (4.2) в общем случае, т.к. причина роста сложности – сюръекция БФ с тривиальной и нетривиальной $J_{D_n}(f)$ на один и тот же спектр, но это основа самого алгоритма 3.1. При этом, если верно второе, то сложность алгоритма 3.1 должна быть достаточна для вычисления решения уравнения (3.1) за разумное время (см. табл. 1).

Далее показан эмпирический результат отбраковки ложных промежуточных функций для БФ четырёх и пяти аргументов. Результат не противоречит предположению *а* и *б*, но не доказывает их. Полученные решения уравнений (3.1) алгоритмом 3.1 для $5 < n < 24$ указывают на непротиворечивость предположения *в*, но также не доказывают его.

Таблица 4.6. Результаты спектрального анализа БФ при $n = 4$

i	$\tilde{r}_i = 1$					$\tilde{r}_i = 2$			$\tilde{r}_i = 3$	$\tilde{r}_i = 4$
1	1-1 3 072 13,56 %	–	–	–	–	1-2 17 664 77,97 %	–	–	1-3 768 3,39 %	1-4 1 152 5,08 %
2	1-1-1 3 072 13,56 %	1-2-1 8 832 38,98 %	–	–	–	1-2-2 8 832 38,98 %	1-3-2 768 3,39 %	1-4-2 1 152 5,08 %	–	–
3	1-1-1-1 3 072 13,56 %	1-2-1-1 8 832 38,98 %	1-2-2-1 8 832 38,98 %	1-3-2-1 768 3,39 %	1-4-2-1 1 152 5,08 %	–	–	–	–	–

Рассмотрим результаты спектрального анализа для $n = 4$. Для удобства данные сведены в табл. 4.6. Значение $r_0 \equiv 1$ в табл. 4.6 не приведено. Для остальных итераций $i = 1, 2, 3$ алгоритма 3.1 имеем следующие значения $\tilde{r}_i$. В ячейках табл. 3.1 указан набор значений $\tilde{r}_i$ через дефис, чтобы показать, как разделяются множества гипотез при переходе от итерации к итерации алгоритма. Дополнительно указана доля таких функций по отношению к объёму генеральной совокупности. Анализ производился для 22656 функций с тривиальной $J_{D_n}(f)$. Например, множество «1-2» мощностью 17664 (причём каждая функция имеет максимум две гипотезы $\tilde{r}_1 = 2$) формируется после нулевой итерации алгоритма и составляет больше половины генеральной совокупности. На следующей итерации из него формируются два равномощных множества: «1-2-1» ($\tilde{r}_2 = 1$) и «1-2-2» ($\tilde{r}_2 = 2$). Для «1-2-1» сложность возвращается в полиномиальные границы, а для «1-2-2» возврат произойдёт только на третьей итерации алгоритма.

На следующих итерациях алгоритма ложные промежуточные решения устраняются, потому что с ростом индекса алфавита уменьшается экспоненциально количество совпадений спектров БФ с тривиальной и нетривиальной $J_{D_n}(f)$. Задачей спектрального анализа является оценка значений $\tilde{r}_i$ для БФ с тривиальной $J_{D_n}(f)$. Анализ был проведён для всех таких функций при $n = 4, 5$. Аналог табл. 4.6 для $n = 5$ приведён в приложении В и далее показаны итоги по нему. В результате было выявлено, что доля БФ с тривиальной $J_{D_n}(f)$, но дающих ложные промежуточные функции на разных итерациях алгоритма, крайне мала и при росте n уменьшается, что указывает на непротиворечивость предположения *в*, но не доказывает его.

Таблица 4.7. Значения $\tilde{r}_i$ для БФ при $n = 4$

Число $\tilde{r}_i$	$\tilde{r}_0$	$\tilde{r}_1$	$\tilde{r}_2$	$\tilde{r}_3$
Среднее значение	1	2	1,474 6	1
Максимальное значение	1	4	2	1
Тривиальное значение	1	8	48	192

Опираясь на данные спектрального анализа, можно рассчитать средние и худшие оценки чисел $\tilde{r}_i$ для $n = 4, 5$. Вычисление среднего производится с

учётом числа БФ. Для удобства данные сведены в табл. 4.7 и табл. 4.8. Для сравнения также приводятся значения чисел $\tilde{r}_i$ для тривиального алгоритма.

Таблица 4.8. Значения $\tilde{r}_i$ для БФ при $n = 5$

Число $\tilde{r}_i$	$\tilde{r}_0$	$\tilde{r}_1$	$\tilde{r}_2$	$\tilde{r}_3$	$\tilde{r}_4$
Среднее значение	1	2,131 7	1,506 0	1,045 8	1
Максимальное значение	1	8	16	3	1
Тривиальное значение	1	10	80	480	1 920

В табл. 4.9 и табл. 4.10 приведен расчёт среднего и максимального количества действий группы Джевонса по формуле (3.6) для $n = 4, 5$ соответственно. В дополнение приводится минимальная оценка сложности алгоритма 3.1, чтобы показать, что существует объективное минимальное количество действий, без которых решение уравнения (3.1) не может быть найдено. Приводится также оценка эффективности алгоритма 3.1. Под эффективностью понимается сложность предлагаемого алгоритма по отношению к тривиальному.

Таблица 4.9. Эффективность алгоритма для $n = 4$

Характеристика	**Сложность**	**Эффективность**
Лучший случай	20	94,791 7 %
Средний случай	27,898 3	92,734 8 %
Худший случай	42	89,062 5 %
Тривиальный алгоритм	384	–

Анализ производился для выборки, совпадающей с генеральной совокупностью для $n = 4, 5$, т.е. для всех БФ указанного количества аргументов. Для больших значений ($n > 5$) анализ всех БФ вычислительно сложен. Из полученных эмпирических данных удалось сформулировать четвёртое предположение *г* о том, что для определения $\tilde{r}_i$, показывающих среднюю оценку сложности алгоритма 3.1, нужно увеличивать число случайно выбираемых БФ для исследования методом спектрального анализа, пока не будет встречена первая БФ с нетривиальной $J_{D_n}(f)$.

Таблица 4.10. Эффективность алгоритма для $n = 5$

Характеристика	**Сложность**	**Эффективность**
Лучший случай	42	99,218 8 %
Средний случай	42,273 0	98,899 1 %
Худший случай	184	95,208 3 %
Тривиальный алгоритм	384 0	–

Из табл. 4.9 и табл. 4.10 можно также заключить, что эффективность алгоритма растёт с ростом количества аргументов БФ, что указывает на непротиворечивость предположения *б*, но не доказывает его.

Для бóльших значений $n > 5$ спектральный анализ не подходит, т.к. число уравнений будет соизмеримо с числом БФ. Для эмпирической оценки числа действий алгоритма 3.1 проведён статистический анализ для БФ при $5 < n < 24$. Значение $n = 23$ соответствует БВ в 1 МиБ, т.е. реальным данным.

Таблица 4.11. Число действий для $5 < n < 24$ (10^6 экспериментов)

n	6	7	8	9	10	11	12	13	14
$n^2 + n$	42	56	72	90	110	132	156	182	210
Эксперимент	46,028	58.918	74,106	91,469	111,037	132,708	156,479	182,338	210,240
n	15	16	17	18	19	20	21	22	23
$n^2 + n$	240	272	306	342	380	420	462	506	552
Эксперимент	240,169	272,118	306,078	342,066	380,049	420,034	462,019	506,020	552,005

Для статистического анализа числа действий алгоритма 3.1 БФ выбирались равномерно случайно без ограничения на тривиальность $J_{D_n}(f)$. Проанализировано по одному миллиону уравнений для каждого $5 < n < 24$. Вычислительный эксперимент проводился на базе эквиморфного вычислителя, описанного в § 3.4, и занял не более 100 часов. В приложении Г приведены результаты вычислительных экспериментов в разбивкой по числу действий. В табл. 4.11 сведены средние значения числа действий алгоритма 3.1. В результате анализа установлено, что БФ с нетривиальной $J_{D_n}(f)$ появляются только для $n = 6$. Для $6 < n < 24$ равномерно случайно выбираются БФ с тривиальной $J_{D_n}(f)$.

Статистический анализ полученных результатов проводился исходя из следующих суждений. Во время вычислительного эксперимента могут произойти только два события: первое – число действий меньше $3,2\left(n^2 + n\right)$ («неудачное событие»), второе – число действий больше либо равно $3,2\left(n^2 + n\right)$ («успешное событие»). Такое распределение является геометрическим [58], т.е. испытания проводятся до первого успеха. Для такого распределения математическое ожидание обратно пропорционально вероятности успешного события. В случае отсутствия успешного события математическое ожидание совпадёт с

числом экспериментов. Откуда заключаем, что с вероятностью меньшей, чем 10^{-6}, наступит успешное событие, т.е. число действий превысит $3,2\big(n^2+n\big)$. Полученные суммарные результаты анализа тривиальности $J_{D_n}(f)$, результаты спектрального анализа и статистические результаты вычислительных экспериментов позволяют сделать вывод об эффективности предложенных алгоритмов определения джевонс-эквивалентности данных.

§ 4.4. Выводы

Выполнена эмпирическая оценка числа действий для множества конкретных уравнений, отражающих реальные данные. Для более чем $2^{64} \approx 10^{20}$ уравнений были исследованы причины увеличения числа действий выше минимального и сформулированы предположения о реальной сложности алгоритма и о возможности его применения для решения прикладных задач.

Для БФ с нетривиальной подгруппой инерции в группе Джевонса появление числа действий при решении уравнения больше минимального следует из доказательства корректности алгоритма, но при этом таких БФ подавляющее меньшинство. Для формирования статистики случайные БВ распределены равномерно, потому что при обработке реальных данных, в общем случае, будет такое же распределение. В результате исследования выявлено, что с вероятностью меньше 10^{-6} число действий при вычислении решения уравнения превосходит n^2+n. Это позволяет сделать заключение о возможности использования предлагаемых алгоритмов при решении прикладных задач. Основные результаты главы 4 опубликованы в [70, 72].

Заключение

Найдены два типа представления группы Джевонса: А – для действия над БВ и Б – над БФ (теорема 1.4). Выбор типа действия, в зависимости от исследуемого объекта при разработке модели программной системы, существенно снижает трудозатраты за счёт упрощения модели и этапа её проектирования.

Найдены частотные свойства действия элемента группы Джевонса, которые заключаются в инвариантности частотных (энтропийных) характеристик в заданных действующим элементом алфавитах (теорема 2.2 и теорема 2.3). Это влияние на энтропию позволяет разрабатывать алгоритмы генерации данных для анализа алгоритмов их преобразования. Отдельно стоит подчеркнуть действия E_n, т.к. они сохраняют энтропию **во всех допустимых алфавитах** данных.

Предложена модель канонического представления элемента группы Джевонса (теорема 3.1) и создан новый эффективный алгоритм решения уравнения действия её элемента над БФ (теорема 3.2). Он эффективен при решении уравнений, включающих БФ с тривиальной подгруппой инерции в группе Джевонсна. Таких БФ подавляющее большинство, поэтому показана возможность использования предложенного алгоритма для решения практических задач анализа джевонс-эквивалентности данных. Опираясь на полученные результаты, важно отметить, что появляются сомнения в применении криптографических примитивов в алгоритмах шифрования, основанных на управляемых операциях, где элемент группы Джевонса является ключом шифрования, а БФ – исходными данными и шифротекстом.

Доказано эквиморфное вложение группы Джевонса в симметрическую группу степени 2^n (теорема 2.1). Разработаны эквиморфный вычислитель и его алгоритмы работы (теорема 3.3, теорема 3.4 и теорема 3.5), позволяющие ещё больше повысить эффективность анализа джевонс-эквивалентности данных. Его практическая проверка подтверждает возможность интеграции предложенных алгоритмов в программные системы обработки данных.

Полученные результаты позволяют вести исследования в данной и смежных предметных областях в направлениях:

– создание расширенного алгоритма анализа джевонс-эквивалентности данных, позволяющего вычислять порождающие подгруппы инерции БФ в группе Джевонса и находить решения уравнения для произвольной подгруппы инерции в группе Джевонса. Разработка расширенного алгоритма включает в себя отдельное исследование нерешённых теоретических и практических задач, таких как определение диаметра графа Кэли для группы Джевонса, заданной множителями канонического представления;

– создание алгоритмов анализа данных, эквивалентных относительно других групп. Задачи, решаемые такими алгоритмами, появляются естественным образом в прикладных областях. Показательным примером является задача решения уравнения действия аддитивной группы кольца вычетов над данными, эквивалентными БФ, при приёме спутникового сигнала ГЛОНАСС;

– разработка и исследование моделей и алгоритмов обработки информации, основывающихся на операциях над классами джевонс-эквивалентных данных. Исследования в этом направлении наиболее интересны, потому что являются теоретической основой для разработки качественно новых алгоритмов сжатия данных. Исследования операций над джевонс-эквивалентными данными (над джевонс-эквивалентными БФ) позволят также разработать более точные методы распознавая образов. Отдельные направления работ позволят создать методы помехоустойчивого кодирования при условии невозможности добавления избыточности комбинаторными методами (задача восстановления повреждённого спутникового сигнала).

Список сокращений и условных обозначений

GNU – GNU not Unix (GNU не Unix)

IEC – international electrotechnical commission (Международная электротехническая комиссия)

LGPL – lesser general public license (стандартная общественная лицензия ограниченного применения)

POSIX – portable operating system interface (переносимый интерфейс операционных систем)

SDK – software development kit (комплект средств разработки)

SN – selfnegative (самоотрицательный)

БВ – бинарный вектор

БФ – булева функция

выч. – вычислительный

ВК – вычислительный комплекс

ГЛОНАСС – глобальная навигационная спутниковая система

дв. – двойной

ДНФ – дизъюнктивная нормальная форма

итерац. – итерация

ИТР – инженерно-техническое решение

КНФ – конъюнктивная нормальная форма

макс. – максимальный

МЭК – международная электротехническая комиссия

нетрив. – нетривиальный

подгр. ин. – подгруппа инерции

сред. – средний

табл. – таблица

трив. – тривиальный

ЧД – число действий

ЭВМ – электронно-вычислительная машина

Список литературы

1. Шеннон, К. Работы по теории информации и кибернетике: Пер. с. англ. Под ред. Р. Л. Добрушина и О. Б. Лупанова. С пред. А. Н. Колмогорова. / К. Шеннон. – М.: Издательство иностранной литературы, 1963. – 829 с. – ил.

2. Хэмминг, Р. В. Теория кодирования и теория информации: Пер. с англ. / Р. В. Хэмминг. – М.: Радио и связь, 1983. – 176 с. – ил.

3. Сэломон, Д. Сжатие данных, изображений и звука. Пер. с. англ. В. В. Чепыжова. / Д. Сэломон. – М.: Техносфера, 2004. – 368 с.

4. Логачёв, О. А. Булевы функции в теории кодирования и криптологии. / О. А. Логачёв, А. А. Сальников, В. В. Ященко. – М.: МЦМНО, 2004. – 470 с.

5. Яблонский С. В. Введение в дискретную математику: Учеб. пособие для вузов. – 2 изд., перераб. и доп. М.: Наука. Гл. ред. физ.-мат. лит., 1986. – 384 с.

6. Джевонс, С. Основы науки / С. Джевонс. – СПб., 1881.

7. Марченко, С. С. Замкнутые классы булевых функций. / С. С. Марченко – М.: ФИЗМАТЛИТ, 2000. – 128 с.

8. Young, A. A quantitative substitutional analysis / A. Young // Proc. London Math. Soc. – 1930. – Vol. 31. – P. 273–388.

9. Geissinger, L. Representations of the Hyperoctahedral Groups / L. Geissinger, D. Kinch // Journal of algebra. – University of North Carolina, 1978. – Vol. 53. – P. 1–20.

10. Baake, M. Structure and representation of the hyperoctahedral group / M. Baake // Journal of Mathematical Physics. – 1984. – V. 25. – No. 11. – P. 3171–3182.

11. Иванов, В. Н. Бисферические функции на симметрической группе, связанные с гипероктаэдральной подгруппой / В. Н. Иванов // Записки научных семинаров ПОМИ. – СПб., 1997. – Т. 240. – С. 96–114.

12. Billey, Sara Vexillary Elements in the Hyperoctahedral Group / Sara Billey, Tao Kai Lam // Journal of Algebraic Combinatorics. Kluwer Academic Publishers.

Manufactured in The Netherlands. – 1998. – Vol. 8. – P. 139–152.

13. Parvathi, M. R–S correspondence for the Hyper-octahedral group of type Bn – A different approach / M. Parvathi, B. Sivakumar, A. Tamilselvi // Algebra Discrete Mathematic. – 2007. – No. 1. P. 86–107.

14. Bajnok, Béla Orbits of the hyperoctahedral group as Euclidean designs / Béla Bajnok // Journal of Algebra Comb. – Gettysburg College. Gettysburg. Pennsylvania USA, 2007. – Vol. 25. – P. 375–397.

15. Gonda, János Metric on the hyper-octahedral group: the minimal deviation / János Gonda // Acta University Sapientiae. Mathematica. – 2012. – Vol. 4. – No. 2. – P. 109–116.

16. Олийнык, Б. В. Группы изометрий пространств Хемминга периодических последовательностей / Б. В. Олийнык, В. И. Сущанский // Сибирский математический журнал. – Новосибирск, 2013. – Т. 54. – № 1. – С. 163–179.

17. Олийнык, Б. В. Системы импримитивности и решётки нормальных делителей D-гипероктаэдральных групп / Б. В. Олийнык, В. И. Сущанский // Сибирский математический журнал. – Новосибирск, 2014. – Т. 55. – № 1. – С. 165–177.

18. Slepian, David On the number of symmetry types of Boolean functions of n variables / David Slepian // Canadian Journal of Mathematics. – 1953. – Vol. 5. – P. 185–193.

19. Constantinescu, Paul On the number of types of Boolean functions with respect to some subgroups of the hyperoctahedral group / Paul Constantinescu // Bulletin mathématique de la Société des Sciences Mathématiques et Physiques de la République Populaire Roumaine Nouvelle Série. – 1960. – Vol. 4(52). – No. 1. – P. 3–16.

20. Де Брёйн, Н. Дж. Теория перечисления Пойа / Н. Дж. Де Брейн // Прикладная комбинаторная математика. Под. ред. Э. Беккенбаха. — М.: Мир, 1968. – С. 61–106.

21. Денисов, О. В. Двоичные коды, образованные функциями с нетриви-

альной группой инерции / О. В. Денисов // Проблемы передачи информации. – М., 2001. – Т. 37. – № 4. – С. 71–84.

22. Wiedemann, Douglas H. Hamming geometry / Douglas H. Wiedemann // Thesis Mathematics University of Waterloo. – Waterloo, Ontario, 1986, Re-typeset July, 2006.

23. Тарасов, А. В. Некоторые свойства групп инерции булевых биюнктивных функций и индуктивный метод генерации таких функций / А. В. Тарасов // Дискретная математика. – М., 2002. – Т. 14. – № 2. – С. 33–47.

24. Никонов, В. Г. Методы компактной реализации биективных отображений, заданных регулярными системами однотипных булевых функций / В. Г. Никонов, А. В. Саранцев // Вестник РУДН. Серия Прикладная и компьютерная математика. – М., 2003. – Т. 2. – № 1. – С. 94–105.

25. Буряков, М. Л. Об уровне аффинности булевых функций / М. Л. Буряков, О. А. Логачев // Дискретная математика. – М., 2005. – Т. 17. – № 4. – С. 98–107.

26. Погорелов, Б. А. Свойства графов орбиталов надгрупп группы Джевонса / Б. А. Погорелов, М. А. Пудовкина // Математические вопросы криптографии. – М., 2010. – Т. 1. – № 1. – С. 55–83.

27. Погорелов, Б. А. О классификации дистанционно-транзитивных графов орбиталов надгрупп группы Джевонса / Б. А. Погорелов, М. А. Пудовкина // Прикладная дискретная математика. Приложение. – Томск, 2016. – № 9. – С. 16–18.

28. Горшков, С. П. Функции из классов Шефера, переходящие при отрицании в другие классы Шефера / С. П. Горшков // Математические вопросы криптографии. – М., 2015. – Т. 6. – № 4. – С. 23–48.

29. Алексеев, Е. К. Классификация корреляционно-имунных и минимальных корреляционно-имунных булевых функций от 4 и 5 переменных / Е. К. Алексеев, Е. К. Карелина // Дискретная математика. – М., 2015. – Т. 27. – №

1. С. 22–33.

30. Hannenhalli, S. Transforming cabbage into turnip (polynomial algorithm for sorting signed permutation by reversal) / S. Hannenhalli, P. A. Pevzner // Journal of the Association Computing Machinery. – 1999. – Vol. 46. – No. 1. P. 1–27.

31. Zappa, Emilio On the subgroup structure of the hyperoctahedral group in six dimensions / Emilio Zappa, Eric C. Dykeman, Reidun Twarock // Acta Crystallographica. Section A. Foundations and Advances. – 2014. – Vol. 70. – P. 417–428.

32. Gates, W. H. Bounds for sorting by prefix-reversal / W. H. Gates, C. H. Papadimitriou // Discrete Mathematics. – 1979. – Vol. 27. – P. 47–57.

33. Клейнберг, Дж. Алгоритмы: разработка и применение. Классика Computers Science. Пер. с англ. Е. Матвеева. (Серия «Классика computer science») / Дж. Клейнберг, Е. Тардос. – СПб.: Питер, 2016. – 800 с. – ил.

34. Howard, H. Aiken Synthesis of electronic computing and control circuits / H. Howard. – The Staff of the Computation Laboratory at Harvard University. Cambridge, Mass., Harvard Univ. Press, 1951.

35. Глухов, М. М. Обзор по теории k-значных функций. Часть 1. Справочное пособие. Ред. Н.Р. Емельянов. Заказ № 163ф. / М. М. Глухов, А. Б. Ремизов, В. А. Шапошников. – М.: Типография в/ч 33965, 125040, Москва А-40, 1988. – 153 с.

36. Golomb, S. W. On classification of Boolean functions / S. W. Golomb // IRE, Trans.circuit theory. Spec.Suppl. – 1959. – No. 6. – P. 176–186.

37. Яубайтис, Э. А. Субклассы и классы булевых функций / Э. А. Яубайтис // Автоматика и вычислительная техника. – Рига: Зинатне, 1974. – № 1. – С. 1–8.

38. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер. – М.: Триумф, 2002. – 816 с.

39. Шниперов, А. Н. Синтез и анализ высокоскоростных симметричных криптосистем на основе управляемых операций / А. Н. Шниперов // Инфор-

мационные технологии. – М., 2008. – Т. 137. – № 1. – С. 36–41.

40. Кострикин, А. И. Введение в алгебру. Часть I. Основы алгебры: Учебник для вузов. – 3-е изд. / А. И. Кострикин. – М.: ФИЗМАТЛИТ, 2004. – 272 с.

41. Каргаполов, М. И. Основы теории групп. – 3-е изд., перераб. и доп. / М. И. Каргаполов, Ю. И. Мерзляков. – М: Наука, 1982. – 288 с.

42. Курош, Александр Геннадиевич Теория групп. – 3-е изд., доп. / Александр Геннадиевич Курош. – М.: Наука. Гл. ред. физ.-мат. лит., 1967. – 648 с.

43. Супруненко, Д. А. Группы подстановок. / Д. А. Супруненко. – Мн.: Навука і тэхніка, 1996. – 366 с.

44. Манин, Ю. И. Введение в современную теорию чисел. / Ю. И. Манин, А. А. Панчишкин. – М.: МЦНМО, 2009. – 552 с. – ил.

45. Al-Kadit, Ibrahim A. Origins of cryptology: The Arab contributions / Ibrahim A. Al-Kadit // Cryptologia. – 1992. – Vol. 16. – No. 2(April). – P. 97–126.

46. Кормен, Томас Х. Алгоритмы: построение и анализ, 2-е издание: Пер. с англ. – Парал. тит. англ. / Томас Х. Кормен, Чарльз И. Лейзерсон, Рональд Л. Ривест, Клиффорд Штайн. – М.: Издательский дом «Вильямс», 2005. – 1296 с. – ил.

47. Керниган, Брайан У. Язык программирования C, 2-е издание.: Пер. с англ. – Парал. тит. англ. / Брайан У. Керниган, Деннис М. Ритчи. – М.: Издательский дом «Вильямс», 2009. – 304 с. – ил.

48. Страуструп, Бьерн Язык программирования C++. Специальное издание. Пер. с англ. / Бьерн Страуструп. – М.: Издательство Бином, 2011 г. – 1136 с. – ил.

49. Бентли, Дж. Жемчужины программирования. 2-е издание. / Дж. Бентли. – СПб.: Питер, 2002. – 272 с. – ил.

50. Intel® 64 and IA-32 Architectures Software Developer's Manual Volume

1: Basic Architecture, Order Number: 253665-060US September 2016. – P. 482.

51. Таненбаум, Э. Современные операционные системы. 3-е изд. / Э. Таненбаум. – СПб.: Питер, 2010. – 1120 с.

52. Руссинович, М. Внутреннее устройство Microsoft Windows. 6-е изд. (Серия «Мастер-класс») / М. Руссинович, Д. Соломон. – СПб.: Питер, 2013. – 800 с. – ил.

53. Руссинович, М. Внутреннее устройство Microsoft Windows. 6-е изд. Основные подсистемы ОС (Серия «Мастер-класс») / М. Руссинович, Д. Соломон. – СПб.: Питер, 2014. – 672 с. – ил.

54. Бовет, Д. Ядро Linux, 3-е изд.: Пер. с англ. / Д. Бовет, М. Чезати. – СПб.: БВХ-Петербург, 2007. – 1104 с. – ил.

55. Постановлению Правительства РФ от 31.10.09 № 879 «Об утверждении положения о единицах величин, допускаемых к применению в Российской Федерации» с изменениями и дополнениями от 15.08.15 [электронный ресурс]. – Режим доступа: http://base.garant.ru/196573/.

56. ГОСТ 8.417–2002 Межгосударственный стандарт. Государственная система обеспечения единства измерений. Единицы величин. Издание официальное. – М.: Стандартинформ, 2010. – 31 с.

57. ГОСТ IEC 60027-2-2015 Межгосударственный стандарт. Обозначения буквенные, применяемые в электротехнике. Часть 2. Электросвязь и электроника (IEC 60027–2:2005, IDT). Издание официальное. – М.: Стандартинформ, 2016. – 87 с.

58. Вентцель, Е. С. Теория вероятностей и её инженерные приложения. Учеб. пособие для втузов. – 2-е изд., стер. / Е. С. Вентцель, Л. А. Овчаров. – М.: Высш. шк., 2000. – 480 с. – ил.

Публикации основных результатов работы в изданиях, рекомендованных ВАК:

59. Кукарцев, А. М. О конструктивном представлении группы Джевонса для инженерно-технических решений обработки информации / А. М. Кукарцев,

А. А. Кузнецов // Программная инженерия. – М., 2015. – № 11. – С. 25–33.

60. Кукарцев, А. М. О действиях группы Джевонса на множествах бинарных векторов и булевых функций для инженерно-технических решений обработки информации / А. М. Кукарцев, А. А. Кузнецов // Программная инженерия. – М., 2016. – Т. 7. – № 1. – С. 29–36.

61. Кукарцев, А. М. О частотных свойствах действий группы Джевонса на булевых функциях / А. М. Кукарцев // Программная инженерия. – М., 2016. Том 7. – № 11. – С. 515–521.

62. Кукарцев, А. М. Об эффективном алгоритме решении уравнения действия группы Джевонса над булевыми функциями / А. М. Кукарцев, А. А. Кузнецов // Программная инженерия. – М., 2017. – Т. 8. – № 2. – С. 76–87.

Публикации основных результатов работы в других изданиях:

63. Кукарцев, А. М. О действии группы Джевонса на множестве бинарных последовательностей и булевых функций / А. М. Кукарцев // Алгебра и логика: теория и приложения: тез. докл. междунар. конф., посвящ. памяти В. П. Шункова, Красноярск, 21–27 июля 2013 г. / отв. за вып.: В. М. Левчук, Я. Н. Нужин, А. И. Созутов, Ю. Ю. Ушаков. – Красноярск: Сиб. федер. ун-т, 2013. – 192 с. – С. 81–82.

64. Кузнецов, А. А. Применение комбинаторных и алгоритмических методов для реализации основных операций в группах подстановок / А. А. Кузнецов, А. М. Кукарцев // Решетнёвские чтения: материалы XVIII Междунар. науч. конф., посвящ. 90-летию со для рождения генер. конструктора ракет.-космич. систем акад. М. Ф. Решетнёва (11–14 нояб. 2014, г. Красноярск): в 3 ч. / под общ. ред. Ю. Ю. Логинова; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2014. – Ч. 2. – 530 с. – С. 79–80.

65. Кукарцев, А. М. Применение спаренных красно-чёрных деревьев для снижения пространственных характеристик алгоритмов частотного анализа информационных сообщений экспоненциального размера / А. М. Кукарцев // Решетнёвские чтения: материалы XVIII Междунар. науч. конф., посвящ. 90-

летию со для рождения генер. конструктора ракет.-космич. систем акад. М. Ф. Решетнёва (11–14 нояб. 2014, г. Красноярск): в 3 ч. / под общ. ред. Ю. Ю. Логинова; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2014. – Ч. 2. – 530 с. – С. 82–84.

66. Кузнецов, А. А. О применении частотного анализа для решения проблемы расстояний в группе Джевонса, индуцирующей действие на множестве булевых функций / А. А. Кузнецов, А. М. Кукарцев // Мальцевские чтения: Тезисы докладов. Междунар. конф. (10–13 нояб. 2014, г. Новосибирск). – Новосибирск: Инст. мат. им. С. Л. Соболева Сиб. отд. Росс. ак. наук, 2014. – 160 с. – С. 67–67.

67. Кукарцев, А. М. О способе индукции действия на множестве булевых функций, эквивалентной индукции действия группы Джевонса / А. М. Кукарцев // Мальцевские чтения: Тезисы докладов. Междунар. конф. (10–13 нояб. 2014, г. Новосибирск). – Новосибирск: Инст. мат. им. С. Л. Соболева Сиб. отд. Росс. ак. наук, 2014. – 160 с. – С. 29–29.

68. Кукарцев, А. М. О применении частотного анализа для решения некоторых групповых уравнений индукции действия группы Джевонса и её подгрупп на множестве булевых функций / А. М. Кукарцев, А. А. Кузнецов // Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20–22 мая 2015г.: Труды / Отв. ред. В. Б. Алексеев, Д. С. Романов, Б. Р. Данилов. – М.: МАКС Пресс, 2015. – 284 с. – С. 136–138.

69. Кукарцев, А. М. О быстром решении уравнения действия группы Джевонса на булевых функциях / А. М. Кукарцев // Решетнёвские чтения XX: тезисы докладов. – Красноярск: Сиб. гос. аэрокосмич. ун-т., 2016. – Ч. 2. – 576 с. – С. 104–106.

70. Кукарцев, А. М. О спектральном анализе булевых функций / А. М. Кукарцев, А. А. Кузнецов // Мальцевские чтения 2016: Тезисы докладов. – Новосибирск: Инст. мат. им. С. Л. Соболева Сиб. отд. Росс. ак. наук, 2016. –

227 с. – С. 39–39.

Свидетельства о государственной регистрации программ для ЭВМ:

71. Кукарцев, А. М. Библиотека domain object processor (dop) / А. М. Кукарцев. – Свидетельство о государственной регистрации программы для ЭВМ № 2016615233 от 18.05.2016 г.

72. Кукарцев, А. М. Программный комплекс спектрального анализа булевых функций SpectrumAnalyzer. / А. М. Кукарцев. – Свидетельство о государственной регистрации программы для ЭВМ № 2016615313 от 20.05.2016 г.

Приложение A
(справочное)
Подробная статистика классов БФ

В табл. A.1, табл. A.2 и табл. A.3 приведена подробная статистика по классам БФ относительно групп E_n, S_n и D_n соответственно для $n = 1, 2, 3, 4, 5$. В статистике приведены расчёты по самоотрицательным и двойным классам с разбивкой по тривиальности подгруппы инерции в соответственных группах.

Таблица A.1. Подробная статистика по классам E_n для $n = 1, 2, 3, 4, 5$

n	1	2	3	4	5
Общее число классов	3	7	46	4336	134 281 216
среди них *SN*-классов	1	3	14	240	63 448
доля *SN*-классов	33,333 %	42,857 %	30,435 %	5,535 %	0,047 %
в т.ч. трив. классов	1	2	23	3 904	134 156 284
доля трив. классов	33,333 %	28,571 %	50,000 %	90,037 %	99,907 %
среди них трив. *SN*-классов	1	0	7	120	58 652
доля трив. *SN*-классов	33,333 %	0,000 %	15,217 %	2,768 %	0,044 %
в т.ч. нетрив. классов	2	5	23	432	124 932
доля нетрив. классов	66,667 %	71,429 %	50,000 %	9,963 %	0,093 %
среди них нетрив. *SN*-классов	0	3	7	120	4 796
доля нетрив. *SN*-классов	0,000 %	42,857 %	15,217 %	2,768 %	0,004 %
Макс. число БФ в классе $\lvert E_n\rvert = 2^n$	2	4	8	16	32
Сред. число БФ в классе	1,333	2,286	5,565	15,114	31,985
Сред. полнота класса	66,667 %	57,143 %	69,565 %	94,465 %	99,953 %
Сред. число БФ в трив. классе	1,000	1,600	3,130	7,111	15,738
Сред. полнота трив. класса	50,000 %	40,000 %	39,130 %	44,444 %	49,182 %
Общее число дв. классов	2	5	30	2 288	67 172 332
в т.ч. трив. дв. классов	1	1	15	2 012	67 107 468
доля трив. дв. классов	50,000 %	20,000 %	50,000 %	87,937 %	99,903 %
в т.ч. нетрив. дв. классов	1	4	15	276	64 864
доля нетрив. дв. классов	50,000 %	80,000 %	50,000 %	12,063 %	0,097 %
Макс. число БФ в дв. классе	4	8	16	32	64
Сред. число БФ в дв. классе	2,000	3,200	8,533	28,643	63,940
Сред. полнота дв. класса	50,000 %	40,000 %	53,333 %	89,510 %	99,906 %
Сред. число БФ в трив. дв. классе	2,000	8,000	12,267	31,046	63,972
Сред. полнота трив. дв. класса	50,000 %	100,000 %	76,667 %	97,018 %	99,956 %
Сред. число БФ в нетрив. дв. классе	2,000	2,000	4,800	11,130	30,313
Сред. полнота нетрив. дв. класса	50,000 %	25,000 %	30,000 %	34,783 %	47,364 %
Общее число функций $\lvert B(n)\rvert$	4	16	256	65536	4 294 967 296
в т.ч. с трив. подгр. ин.	2	8	184	62 464	4 293 001 088
доля БФ с трив. подгр. ин.	50,000 %	50,000 %	71,875 %	95,313 %	99,954 %
в т.ч. с нетрив. подгр. ин.	2	8	72	3 072	1 966 208
доля БФ с нетрив. подгр. ин.	50,000 %	50,000 %	28,125 %	4,688 %	0,046 %

Таблица A.2. Подробная статистика по классам S_n для $n = 1, 2, 3, 4, 5$

n	1	2	3	4	5
Общее число классов	4	12	80	3984	37 333 248
среди них *SN*-классов	0	0	0	0	0
доля *SN*-классов	–	–	–	–	–
в т.ч. трив. классов	4	4	16	1 792	34 339 072
доля трив. классов	100,000 %	33,333 %	20,000 %	44,980 %	91,980 %
среди них трив. *SN*-классов	0	0	0	0	0
доля трив. *SN*-классов	–	–	–	–	–
в т.ч. нетрив. классов	0	8	64	2 192	2 994 176
доля нетрив. классов	0,000 %	66,667 %	80,000 %	55,020 %	8,020 %
среди них нетрив. *SN*-классов	0	0	0	0	0
доля нетрив. *SN*-классов	–	–	–	–	–
Макс. число БФ в классе $\lvert S_n \rvert = n!$	1	2	6	24	120
Сред. число БФ в классе	1,000	1,333	3,200	16,450	115,044
Сред. полнота класса	100,000 %	66,667 %	53,333 %	68,541 %	95,870 %
Сред. число БФ в трив. классе	–	1,000	2,500	10,277	58,206
Сред. полнота трив. класса	–	50,000 %	41,667 %	42,822 %	48,505 %
Общее число дв. классов	2	6	40	1 992	18 666 624
в т.ч. трив. дв. классов	2	2	8	896	17 169 536
доля трив. дв. классов	100,000 %	33,333 %	20,000 %	44,980 %	91,980 %
в т.ч. нетрив. дв. классов	0	4	32	1 096	1 497 088
доля нетрив. дв. классов	0,000 %	66,667 %	80,000 %	55,020 %	8,020 %
Макс. число БФ в дв. классе	2	4	12	48	240
Сред. число БФ в дв. классе	2,000	2,667	6,400	32,900	230,088
Сред. полнота дв. класса	100,000 %	66,667 %	53,333 %	68,541 %	95,870 %
Сред. число БФ в трив. дв. классе	2,000	4,000	12,000	48,000	240,000
Сред. полнота трив. дв. класса	100,000 %	100,000 %	100,000 %	100,000 %	100,000 %
Сред. число БФ в нетрив. дв. классе	–	2,000	5,000	20,555	116,412
Сред. полнота нетрив. дв. класса	–	50,000 %	41,667 %	42,822 %	48,505 %
Общее число функций $\lvert B(n) \rvert$	4	16	256	65536	4 294 967 296
в т.ч. с трив. подгр. ин.	4	8	96	43 008	4 120 688 640
доля БФ с трив. подгр. ин.	100,000 %	50,000 %	37,500 %	65,625 %	95,942 %
в т.ч. с нетрив. подгр. ин.	0	8	160	22 528	174 278 656
доля БФ с нетрив. подгр. ин.	0,000 %	50,000 %	62,500 %	34,375 %	4,058 %

Таблица A.3. Подробная статистика по классам D_n для $n = 1, 2, 3, 4, 5$

n	1	2	3	4	5
Общее число классов	3	6	22	402	1 228 158
среди них *SN*-классов	1	2	6	42	4 094
доля *SN*-классов	33,333 %	33,333 %	27,273 %	10,448 %	0,333 %
в т.ч. трив. классов	1	0	0	59	1 022 524
доля трив. классов	33,333 %	0,000 %	0,000 %	14,677 %	83,257 %
среди них трив. *SN*-классов	1	0	0	11	2 664
доля трив. *SN*-классов	33,333 %	0,000 %	0,000 %	2,736 %	0,217 %
в т.ч. нетрив. классов	2	6	22	343	205 634
доля нетрив. классов	66,667 %	100,000 %	100,000 %	85,323 %	16,743 %
среди них нетрив. *SN*-классов	0	2	6	31	1 430
доля нетрив. *SN*-классов	0,000 %	33,333 %	27,273 %	7,711 %	0,116 %
Макс. число БФ в классе $\lvert D_n\rvert = 2^n \cdot n!$	2	8	48	384	3 840
Сред. число БФ в классе	1,333	2,667	11,636	163,025	3 497,080
Сред. полнота класса	66,667 %	33,333 %	24,242 %	42,454 %	91,070 %
Сред. число БФ в трив. классе	1,000	2,667	11,636	125,015	1 791,898
Сред. полнота трив. класса	50,000 %	33,333 %	24,242 %	32,556 %	46,664 %
Общее число дв. классов	2	4	14	222	616 126
в т.ч. трив. дв. классов	1	0	0	35	512 594
доля трив. дв. классов	50,000 %	0,000 %	0,000 %	15,766 %	83,196 %
в т.ч. нетрив. дв. классов	1	4	14	187	103 532
доля нетрив. дв. классов	50,000 %	100,000 %	100,000 %	84,234 %	16,804 %
Макс. число БФ в дв. классе	4	16	96	768	7 680
Сред. число БФ в дв. классе	2,000	4,000	18,286	295,207	6 970,924
Сред. полнота дв. класса	50,000 %	25,000 %	19,048 %	38,438 %	90,767 %
Сред. число БФ в трив. дв. классе	2,000	–	–	647,314	7 660,043
Сред. полнота трив. дв. класса	50,000 %	–	–	84,286 %	99,740 %
Сред. число БФ в нетрив. дв. классе	2,000	4,000	18,286	229,305	3 559,046
Сред. полнота нетрив. дв. класса	50,000 %	25,000 %	19,048 %	29,857 %	46,342 %
Общее число функций $\lvert B(n)\rvert$	4	16	256	65536	4 294 967 296
в т.ч. с трив. подгр. ин.	2	0	0	22 656	3 926 492 160
доля БФ с трив. подгр. ин.	50,000 %	0,000 %	0,000 %	34,570 %	91,421 %
в т.ч. с нетрив. подгр. ин.	2	16	256	42 880	368 475 136
доля БФ с нетрив. подгр. ин.	50,000 %	100,000 %	100,000 %	65,430 %	8,579 %

Приложение Б
(справочное)
Каталоги классов БФ

В табл. Б.1 приведены каталоги БФ относительно групп E_n, S_n и D_n для $n = 1, 2, 3, 4$. В ячейках таблицы указано число двойных орбит. Каталоги разделены по классам W_k^j. Внутри каждого каталога классы отсортированы по именам БФ и сгруппированы относительно отрицания БФ (т.е. показаны двойные классы). Для удобства классы с меньшим весом БФ отмечены как «+», с большим – «–». Для классов $W_k^{2^{n-1}}$ положительным считается класс с меньшим значением имени, иначе – отрицательным. Самоотрицательные классы отмечены «0». В последнем столбце каждого каталога указывается мощность класса ($|\ |$). Некоторые классы с меньшим именем являются отрицательными, и для них «+» и «–» классы поменяны местами и строка каталога подствечена серым. Поэтому левое имя класса в каталоге является ещё и именем дв. класса.

Таблица Б.1. Перечень каталогов БФ

Вес	E_n		S_n		D_n	
	Число	Каталог	Число	Каталог	Число	Каталог
$n = 1$						
W_2^0/W_2^2	1	табл. Б.2	1	табл. Б.4	1	табл. Б.6
W_2^1	–	–	1	табл. Б.5	–	–
$W_2^1(SN)$	1	табл. Б.3	–	–	1	табл. Б.7
$n = 2$						
W_4^0/W_4^4	1	табл. Б.8	1	табл. Б.11	1	табл. Б.14
W_4^1/W_4^3	1	табл. Б.9	3	табл. Б.12	1	табл. Б.15
W_4^2	–	–	2	табл. Б.13	–	–
$W_4^2(SN)$	3	табл. Б.10	–	–	2	табл. Б.16
$n = 3$						
W_8^0/W_8^8	1	табл. Б.17	1	табл. Б.22	1	табл. Б.27
W_8^1/W_8^7	1	табл. Б.18	4	табл. Б.23	1	табл. Б.28
W_8^2/W_8^6	7	табл. Б.19	9	табл. Б.24	3	табл. Б.29
W_8^3/W_8^5	7	табл. Б.20	16	табл. Б.25	3	табл. Б.30
W_8^4	–	–	10	табл. Б.26	–	–
$W_8^4(SN)$	14	табл. Б.21	–	–	6	табл. Б.31
$n = 4$						
W_{16}^0/W_{16}^{16}	1	–	1	–	1	табл. Б.32
W_{16}^1/W_{16}^{15}	1	–	5	–	1	табл. Б.33
W_{16}^2/W_{16}^{14}	15	–	17	–	4	табл. Б.34
W_{16}^3/W_{16}^{13}	35	–	52	–	6	табл. Б.35
W_{16}^4/W_{16}^{12}	140	–	136	–	19	табл. Б.36
W_{16}^5/W_{16}^{11}	273	–	284	–	27	табл. Б.37
W_{16}^6/W_{16}^{10}	553	–	477	–	50	табл. Б.38
W_{16}^7/W_{16}^9	715	–	655	–	56	табл. Б.39
W_{16}^8	315	–	365	–	16	табл. Б.40
$W_{16}^8(SN)$	240	–	–	–	42	табл. Б.41

Таблица Б.2. W_2^0/W_2^2 по E_1

№	«+»	«−»	| |
1	(0)	(3)	1

Таблица Б.3. $W_2^1(SN)$ по E_1

№	«0»	| |
1	(1)	2

Таблица Б.4. W_2^0/W_2^2 по S_1

№	«+»	«−»	| |
1	(0)	(3)	1

Таблица Б.5. W_2^1 по S_1

№	«+»	«−»	| |
1	(1)	(2)	1

Таблица Б.6. W_2^0/W_2^2 по D_1

№	«+»	«−»	| |
1	(0)	(3)	1

Таблица Б.7. $W_2^1(SN)$ по D_1

№	«0»	| |
1	(1)	2

Таблица Б.8. W_4^0/W_4^4 по E_2

№	«+»	«−»	| |
1	(0)	(f)	1

Таблица Б.9. W_4^1/W_4^3 по E_2

№	«+»	«−»	| |
1	(1)	(7)	4

Таблица Б.10. $W_4^2(SN)$ по E_2

№	«0»	| |
1	(3)	2
2	(5)	2
3	(6)	2

Таблица Б.11. W_4^0/W_4^4 по S_2

№	«+»	«−»	| |
1	(0)	(f)	1

Таблица Б.12. W_4^1/W_4^3 по S_2

№	«+»	«−»	| |
1	(1)	(e)	1
2	(2)	(b)	2
3	(7)	(8)	1

Таблица Б.13. W_4^2 по S_2

№	«+»	«−»	| |
1	(3)	(a)	2
2	(6)	(9)	1

Таблица Б.14. W_4^0/W_4^4 по D_2

№	«+»	«−»	| |
1	(0)	(f)	1

Таблица Б.15. W_4^1/W_4^3 по D_2

№	«+»	«−»	| |
1	(1)	(7)	4

Таблица Б.16. $W_4^2(SN)$ по D_2

№	«0»	| |
1	(3)	4
2	(6)	2

Таблица Б.17. W_8^0/W_8^8 по E_3

№	«+»	«−»	| |
1	(00)	(ff)	1

Таблица Б.18. W_8^1/W_8^7 по E_3

№	«+»	«−»	| |
1	(01)	$(7f)$	8

Таблица Б.19. W_8^2/W_8^6 по E_3

№	«+»	«−»	| |
1	(03)	$(3f)$	4
2	(05)	$(5f)$	4
3	(06)	$(6f)$	4
4	(11)	(77)	4
5	(12)	$(7b)$	4
6	(14)	$(7d)$	4
7	(18)	$(7e)$	4

Таблица Б.20. W_8^3/W_8^5 по E_3

№	«+»	«−»	| |
1	(07)	$(1f)$	8
2	(13)	(37)	8
3	(15)	(57)	8
4	(16)	$(6b)$	8
5	(19)	(67)	8
6	$(1a)$	$(5b)$	8
7	$(1c)$	$(3d)$	8

Таблица Б.21. $W_8^4(SN)$ по E_3

№	«0»	| |
1	$(0f)$	2
2	(17)	8
3	$(1b)$	8
4	$(1d)$	8
5	$(1e)$	8
6	(33)	2
7	(35)	8
8	(36)	8
9	$(3c)$	2
10	(55)	2
11	(56)	8
12	$(5a)$	2
13	(66)	2
14	(69)	2

Таблица Б.22. W_8^0/W_8^8 по S_3

№	«+»	«−»	| |
1	(00)	(ff)	1

Таблица Б.23. W_8^1/W_8^8 по S_3

№	«+»	«−»	| |
1	(01)	(fe)	1
2	(02)	(ef)	3
3	(08)	(bf)	3
4	$(7f)$	(80)	1

Таблица Б.24. W_8^2/W_8^8 по S_3

№	«+»	«−»	| |
1	(03)	(ee)	3
2	(06)	(eb)	3
3	(09)	(be)	3
4	$(0a)$	(af)	6
5	(18)	(bd)	3
6	(28)	$(9f)$	3
7	$(3f)$	(88)	3
8	$(6f)$	(82)	3
9	$(7e)$	(81)	1

Таблица Б.25. W_8^3/W_8^8 по S_3

№	«+»	«−»	| |
1	(07)	(ea)	3
2	$(0b)$	(ae)	6
3	$(0e)$	(ab)	3
4	(16)	$(e9)$	1
5	(19)	(bc)	3
6	$(1a)$	(ad)	6
7	$(1f)$	$(a8)$	3
8	(29)	$(9e)$	3
9	$(2a)$	$(8f)$	3
10	$(2c)$	$(9b)$	6
11	$(2f)$	$(8a)$	6
12	$(3d)$	(98)	3
13	$(3e)$	(89)	3
14	(68)	(97)	1
15	$(6b)$	(86)	3
16	$(6e)$	(83)	3

Таблица Б.26. W_8^4 по S_3

№	«+»	«−»	| |
1	$(0f)$	(aa)	3
2	(17)	$(e8)$	1
3	$(1b)$	(ac)	6
4	$(1e)$	$(a9)$	3
5	$(2b)$	$(8e)$	3
6	$(2d)$	$(9a)$	6
7	$(2e)$	$(8b)$	6
8	$(3c)$	(99)	3
9	(69)	(96)	1
10	$(6a)$	(87)	3

Таблица Б.27. W_8^0/W_8^8 по D_3

№	«+»	«−»	| |
1	(00)	(ff)	1

Таблица Б.28. W_8^1/W_8^7 по D_3

№	«+»	«−»	| |
1	(01)	$(7f)$	8

Таблица Б.29. W_8^2/W_8^6 по D_3

№	«+»	«−»	| |
1	(03)	$(3f)$	12
2	(06)	$(6f)$	12
3	(18)	$(7e)$	4

Таблица Б.30. W_8^3/W_8^5 по D_3

№	«+»	«−»	| |
1	(07)	$(1f)$	24
2	(16)	$(6b)$	8
3	(19)	$(3d)$	24

Таблица Б.31. $W_8^4(SN)$ по D_3

№	«0»	| |
1	$(0f)$	6
2	(17)	8
3	$(1b)$	24
4	$(1e)$	24
5	$(3c)$	6
6	(69)	2

Таблица Б.32. W_{16}^0/W_{16}^{16} по D_4

№	«+»	«−»	| |
1	(0000)	$(ffff)$	1

Таблица Б.33. W_{16}^{1}/W_{16}^{15} по D_4

№	«+»	«−»	| |
1	(0001)	(7fff)	16

Таблица Б.34. W_{16}^{2}/W_{16}^{14} по D_4

№	«+»	«−»	| |
1	(0003)	(3fff)	32
2	(0006)	(6fff)	48
3	(0018)	(7eff)	32
4	(0180)	(7ffe)	8

Таблица Б.35. W_{16}^{3}/W_{16}^{13} по D_4

№	«+»	«−»	| |
1	(0007)	(1fff)	96
2	(0016)	(6bff)	64
3	(0019)	(3dff)	192
4	(0118)	(6ffb)	96
5	(0181)	(3ffd)	64
6	(0182)	(6ff7)	48

Таблица Б.36. W_{16}^{4}/W_{16}^{12} по D_4

№	«+»	«−»	| |
1	(000f)	(0fff)	24
2	(0017)	(17ff)	64
3	(001b)	(1bff)	192
4	(001e)	(1eff)	192
5	(003c)	(3cff)	48
6	(0069)	(69ff)	16
7	(0116)	(6bbf)	16
8	(0119)	(1ff7)	96
9	(011a)	(3ddf)	192
10	(012c)	(3def)	192
11	(0168)	(6bfd)	64
12	(0183)	(1ffb)	192
13	(0186)	(6bdf)	96
14	(0189)	(3dfd)	96
15	(0198)	(3dfe)	192
16	(01a8)	(1ffe)	96
17	(03c0)	(3ffc)	16
18	(0660)	(6ff6)	12
19	(0690)	(6ff9)	24

Таблица Б.37. W_{16}^{5}/W_{16}^{11} по D_4

№	«+»	«−»	| |
1	(001f)	(07ff)	192
2	(003d)	(19ff)	192
3	(006b)	(16ff)	64
4	(0117)	(177f)	16
5	(011b)	(17bf)	192
6	(011e)	(1eef)	96
7	(012d)	(1bef)	384
8	(013c)	(3cdf)	192
9	(0169)	(3dd7)	64
10	(016a)	(1ef7)	192
11	(0187)	(17ef)	192
12	(018b)	(1bdf)	192
13	(0196)	(69bf)	64
14	(0199)	(1ff3)	192
15	(019a)	(1efb)	384
16	(01a9)	(1efe)	192
17	(01aa)	(0ff7)	96

Окончание таблицы Б.37

18	(01ac)	(1bfd)	384
19	(01e8)	(17fe)	64
20	(0358)	(3ded)	192
21	(0368)	(3dde)	192
22	(03c1)	(1ffa)	192
23	(0661)	(6bd7)	48
24	(0662)	(1ff9)	96
25	(0691)	(3ddb)	192
26	(06b0)	(1ff6)	96
27	(1681)	(6bbd)	16

Таблица Б.38. W_{16}^{6}/W_{16}^{10} по D_4

№	«+»	«−»	| |
1	(003f)	(03ff)	96
2	(006f)	(06ff)	96
3	(007e)	(18ff)	32
4	(011f)	(077f)	96
5	(012f)	(07bf)	192
6	(013d)	(179f)	192
7	(013e)	(19f7)	192
8	(016b)	(16bf)	192
9	(016e)	(19ef)	192
10	(018f)	(07ef)	96
11	(0197)	(167f)	64
12	(019b)	(17af)	384
13	(019e)	(16ef)	192
14	(01ab)	(07f7)	192
15	(01ad)	(19fb)	384
16	(01ae)	(07fb)	384
17	(01bc)	(19fe)	192
18	(01e9)	(16fe)	64
19	(01ea)	(07fe)	192
20	(033c)	(3ccf)	32
21	(0356)	(1eee)	48
22	(0359)	(1bd7)	192
23	(035a)	(1bee)	384
24	(0369)	(1eeb)	192
25	(036a)	(17bd)	192
26	(036c)	(1ef3)	384
27	(03c3)	(0ff3)	96
28	(03c5)	(1bdb)	192
29	(03c6)	(1efa)	192
30	(03d4)	(17ee)	192
31	(03d8)	(1bfc)	192
32	(0663)	(17eb)	192
33	(0666)	(1ff1)	48
34	(0669)	(699f)	48
35	(0672)	(1bde)	192
36	(0678)	(1ef9)	192
37	(0693)	(1be7)	192
38	(0696)	(3cd7)	96
39	(06b1)	(1bed)	384
40	(06b2)	(17be)	192
41	(06b4)	(1ef6)	192
42	(06f0)	(0ff6)	48
43	(07b0)	(1ff2)	96
44	(07e0)	(1ff8)	48
45	(1668)	(6bd6)	8
46	(1683)	(1ee7)	96

Окончание таблицы Б.38

47	(1686)	(3cdb)	96
48	(1689)	(3dd6)	64
49	(1698)	(3dda)	96
50	(177e)	(1781)	16

Таблица Б.39. W_{16}^{7}/W_{16}^{9} по D_4

№	«+»	«−»	| |
1	(007f)	(01ff)	64
2	(013f)	(037f)	192
3	(016f)	(06bf)	192
4	(017e)	(18ef)	64
5	(019f)	(067f)	192
6	(01af)	(03df)	384
7	(01bd)	(178f)	192
8	(01be)	(06fb)	192
9	(01eb)	(06f7)	192
10	(01ee)	(03fd)	192
11	(033d)	(1797)	64
12	(0357)	(0777)	48
13	(035b)	(07b7)	384
14	(035e)	(19f3)	192
15	(036b)	(077b)	192
16	(036d)	(16af)	384
17	(036e)	(179b)	384
18	(037c)	(19ee)	192
19	(03c7)	(07f3)	384
20	(03d5)	(07e7)	192
21	(03d6)	(16ee)	192
22	(03d9)	(19fa)	384
23	(03dc)	(07fa)	384
24	(0667)	(17ab)	96
25	(066b)	(166f)	96
26	(0673)	(07eb)	192
27	(0676)	(19f9)	192
28	(0679)	(16eb)	192
29	(067a)	(17ad)	384
30	(0697)	(169f)	192
31	(06b3)	(07bd)	384
32	(06b5)	(19eb)	384
33	(06b6)	(16be)	192
34	(06b9)	(19f6)	192
35	(06f1)	(07f9)	192
36	(06f2)	(07f6)	192
37	(0778)	(1ef1)	96
38	(077e)	(1783)	96
39	(07b1)	(17ae)	384
40	(07b4)	(1bec)	384
41	(07e1)	(17ea)	192
42	(07e2)	(1bd9)	192
43	(07f0)	(0ff1)	96
44	(1669)	(6997)	16
45	(166a)	(17e9)	64
46	(167e)	(1789)	64
47	(1687)	(19e7)	192
48	(168b)	(16bd)	192
49	(168e)	(179e)	192
50	(1696)	(3cc7)	64
51	(1699)	(1ee3)	192
52	(169a)	(1be5)	384

Окончание таблицы Б.39

53	(16a9)	(1ee9)	96
54	(16ac)	(1bd6)	192
55	(1798)	(17bc)	192
56	(19e1)	(1ee6)	48

Таблица Б.40. W_{16}^{8} по D_4

№	«+»	«−»	| |
1	(037d)	(06bb)	192
2	(037e)	(1787)	192
3	(03d7)	(0677)	192
4	(03db)	(07b3)	192
5	(03de)	(06f3)	384
6	(067e)	(178b)	192
7	(06bd)	(168f)	192
8	(0776)	(19f1)	48
9	(0779)	(16ab)	96
10	(077a)	(1799)	192
11	(07b6)	(16ae)	384
12	(07bc)	(19ea)	192
13	(07e6)	(19f8)	96
14	(07e9)	(16ea)	96
15	(166e)	(17a9)	96
16	(16bc)	(19e9)	192

Таблица Б.41. $W_{16}^{8}(SN)$ по D_4

№	«0»	| |
1	(00ff)	8
2	(017f)	64
3	(01bf)	192
4	(01ef)	192
5	(01fe)	64
6	(033f)	32
7	(035f)	192
8	(036f)	384
9	(03cf)	96
10	(03dd)	384
11	(03fc)	96
12	(066f)	48
13	(067b)	384
14	(069f)	48
15	(06b7)	384
16	(06f6)	96
17	(06f9)	96
18	(07b5)	384
19	(07e3)	384
20	(07f1)	192

Окончание таблицы Б.41

21	(07f2)	384
22	(07f8)	192
23	(0ff0)	12
24	(166b)	64
25	(1697)	64
26	(169b)	384
27	(169e)	192
28	(16ad)	384
29	(16e9)	64
30	(178e)	96
31	(1796)	64
32	(179a)	384
33	(17ac)	384
34	(17e8)	32
35	(18e7)	32
36	(19e3)	192
37	(19e6)	192
38	(1bd8)	24
39	(1be4)	96
40	(1ee1)	48
41	(3cc3)	8
42	(6996)	2

Каталоги БФ относительно E_n и S_n для $n = 4$ не приводятся из-за большого числа классов.

Приложение B
(обязательное)
Результаты спектрального анализа

Таблица B.1. Результаты спектрального анализа для $n = 5$

i	$\tilde{r}_i = 1$							
0	1-1 596 382 720 15,188 7 %	–	–	–	–	–	–	–
1	1-1-1 596 382 720 15,188 7 %	1-2-1 1 381 393 920 35,181 4 %	–	–	–	–	–	–
2	1-1-1-1 596 382 720 15,188 7 %	1-2-1-1 1 381 393 920 35,181 4 %	1-2-2-1 1 134 927 360 28,904 4 %	–	1-2-3-1 69 120 0,001 8 %	–	1-2-4-1 2 833 920 0,072 2 %	–
3	1-1-1-1-1 596 382 720 15,188 7 %	1-2-1-1-1 1 381 393 920 35,181 4 %	1-2-2-1-1 1 134 927 360 28,904 4 %	1-2-2-2-1 106 698 240 2,717 4 %	1-2-3-1-1 69 120 0,001 8 %	1-2-3-2-1 1 098 240 0,028 0 %	1-2-4-1-1 2 833 920 0,072 2 %	1-2-4-2-1 860 160 0,021 9 %

i	$\tilde{r}_i = 1$								
0	–	–	–	–	–	–	–	–	–
1	1-3-1 46 375 680 1,181 1 %	–	–	–	–	–	–	–	–
2	1-3-1-1 46 375 680 1,181 1 %	1-3-2-1 261 189 120 6,652 0 %	–	1-3-3-1 53 760 0,001 4 %	–	–	–	–	–
3	1-3-1-1-1 46 375 680 1,181 1 %	1-3-2-1-1 261 189 120 6,652 0 %	1-3-2-2-1 29 625 600 0,754 5 %	1-3-3-1-1 53 760 0,001 4 %	1-3-3-2-1 537 600 0,013 7 %	1-3-3-3-1 307 200 0,007 8 %	1-3-4-1-1 986 880 0,025 1 %	1-3-4-2-1 5 310 720 0,135 3 %	1-3-6-2-1 26 880 0,000 7 %

i	$\tilde{r}_i = 1$								
0	–	–	–	–	–	–	–	–	–
1	1-4-1 55 438 080 1,411 9 %	–	–	–	–	–	–	–	–
2	1-4-1-1 55 438 080 1,411 9 %	1-4-2-1 212 663 040 5,416 1 %	–	1-4-3-1 126 720 0,003 2 %	–	–	1-4-4-1 32 121 600 0,818 1 %	–	–
3	1-4-1-1-1 55 438 080 1,411 9 %	1-4-2-1-1 212 663 040 5,416 1 %	1-4-2-2-1 20 912 640 0,532 6 %	1-4-3-1-1 126 720 0,003 2 %	1-4-3-2-1 230 400 0,005 9 %	1-4-3-3-1 42 240 0,001 1 %	1-4-4-1-1 32 121 600 0,818 1 %	1-4-4-2-1 7 622 400 0,194 1 %	1-4-4-3-1 3 840 0,000 1 %

i	$\tilde{r}_i = 1$								
0	–	–	–	–	–	–	–	–	–
1	–	–	–	–	–	–	–	–	–
2	1-4-6-1 15 360 0,000 4 %	–	1-4-8-1 1 639 680 0,041 8 %	–	–	1-5-2-1 764 160 0,019 5 %	–	–	1-5-4-1 76 800 0,002 0 %
3	1-4-6-1-1 15 360 0,000 4 %	1-4-6-2-1 23 040 0,000 6 %	1-4-8-1-1 1 639 680 0,041 8 %	1-4-8-2-1 545 280 0,013 9 %	1-4-8-3-1 11 520 0,000 3 %	1-5-2-1-1 764 160 0,019 5 %	1-5-2-2-1 53 760 0,001 4 %	1-5-3-3-1 23 040 0,000 6 %	1-5-4-1-1 76 800 0,002 0 %

i	$\tilde{r}_i = 1$								
0	–	–	–	–	–	–	–	–	–
1	–	–	–	1-6-1 241 920 0,006 2 %	–	–	–	–	–
2	–	–	–	1-6-1-1 241 920 0,006 2 %	1-6-2-1 14 215 680 0,362 0 %	–	1-6-3-1 7 680 0,000 2 %	–	–
3	1-5-4-2-1 84 480 0,002 2 %	1-5-4-3-1 7 680 0,000 2 %	1-5-6-2-1 7 680 0,000 2 %	1-6-1-1-1 241 920 0,006 2 %	1-6-2-1-1 14 215 680 0,362 0 %	1-6-2-2-1 1 355 520 0,034 5 %	1-6-3-1-1 7 680 0,000 2 %	1-6-3-2-1 34 560 0,000 9 %	1-6-3-3-1 15 360 0,000 4 %

i	$\tilde{r}_i = 1$								
0	–	–	–	–	–	–	–	–	–
1	–	–	–	–	–	–	–	–	–
2	1-6-4-1 5 168 640 0,131 6 %	–	–	–	1-6-8-1 752 640 0,019 2 %	–	–	–	1-8-2-1 318 720 0,008 1 %
3	1-6-4-1-1 5 168 640 0,131 6 %	1-6-4-2-1 2 184 960 0,055 6 %	1-6-6-2-1 7 680 0,000 2 %	1-6-6-3-1 23 040 0,000 6 %	1-6-8-1-1 752 640 0,019 2 %	1-6-8-2-1 460 800 0,011 7 %	1-6-8-3-1 11 520 0,000 3 %	1-6-16-2-1 7 680 0,000 2 %	1-8-2-1-1 318 720 0,008 1 %

i	$\tilde{r}_i = 1$								
0	–	–	–	–	–	–	–	–	–
1	–	–	–	–	–	–	–	–	–
2	–	–	1-8-4-1 245 760 0,006 3 %	–	1-8-6-1 11 520 0,000 3 %	–	1-8-8-1 57 600 0,001 5 %	–	–
3	1-8-2-2-1 23 040 0,000 6 %	1-8-3-2-1 7 680 0,000 2 %	1-8-4-1-1 245 760 0,006 3 %	1-8-4-2-1 119 040 0,003 0 %	1-8-6-1-1 11 520 0,000 3 %	1-8-6-2-1 23 040 0,000 6 %	1-8-8-1-1 57 600 0,001 5 %	1-8-8-2-1 103 680 0,002 6 %	1-8-16-2-1 3 840 0,000 1 %

i	$\tilde{r}_i = 2$							
0	1-2 2 627 880 960 66,926 9 %	–	–	–	–	–	–	–
1	1-2-2 1 241 625 600 31,621 8 %	–	–	1-3-2 290 814 720 7,406 5 %	–	–	–	–
2	1-2-2-2 106 698 240 2,717 4 %	1-2-3-2 1 098 240 0,028 0 %	1-2-4-2 860 160 0,021 9 %	1-3-2-2 29 625 600 0,754 5 %	1-3-3-2 537 600 0,013 7 %	1-3-4-1 986 880 0,025 1 %	1-3-4-2 5 310 720 0,135 3 %	1-3-6-2 26 880 0,000 7 %
3	–	–	–	–	–	–	–	–

i	$\tilde{r}_i = 2$								
0	–	–	–	–	–	–	–	–	–
1	1-4-2 233 575 680 5,948 7 %	–	–	–	–	1-5-2 817 920 0,020 8 %	–	–	1-6-2 15 571 200 0,396 6 %
2	1-4-2-2 20 912 640 0,532 6 %	1-4-3-2 230 400 0,005 9 %	1-4-4-2 7 622 400 0,194 1 %	1-4-6-2 23 040 0,000 6 %	1-4-8-2 545 280 0,013 9 %	1-5-2-2 53 760 0,001 4 %	1-5-4-2 84 480 0,002 2 %	1-5-6-2 7 680 0,000 2 %	1-6-2-2 1 355 520 0,034 5 %
3	–	–	–	–	–	–	–	–	–

i	$\tilde{r}_i = 2$								
0	–	–	–	–	–	–	–	–	–
1	–	–	–	–	–	1-8-2 341 760 0,008 7 %	–	–	–
2	1-6-3-2 34 560 0,000 9 %	1-6-4-2 2 184 960 0,055 6 %	1-6-6-2 7 680 0,000 2 %	1-6-8-2 460 800 0,011 7 %	1-6-16-2 7 680 0,000 2 %	1-8-2-2 23 040 0,000 6 %	1-8-3-2 7 680 0,000 2 %	1-8-4-2 119 040 0,003 0 %	1-8-6-2 23 040 0,000 6 %
3	–	–	–	–	–	–	–	–	–

i	$\tilde{r}_i = 2$		$\tilde{r}_i = 3$						
0	–	–	1-3 344 413 440 8,771 5 %	–	–	–	–	–	–
1	–	–	1-2-3 1 167 360 0,029 7 %	1-3-3 898 560 0,022 9 %	1-4-3 399 360 0,010 2 %	–	–	1-5-3 23 040 0,000 6 %	–
2	1-8-8-2 103 680 0,002 6 %	1-8-16-2 3 840 0,000 1 %	–	1-3-3-3 307 200 0,007 8 %	1-4-3-3 42 240 0,001 1 %	1-4-4-3 3 840 0,000 1 %	1-4-8-3 11 520 0,000 3 %	1-5-3-3 23 040 0,000 6 %	1-5-4-3 7 680 0,000 2 %
3	–	–	–	–	–	–	–	–	–

i	$\tilde{r}_i = 3$				$\tilde{r}_i = 4$				
0	–	–	–	–	1-4 331 395 840 8,440 0 %	–	–	–	–
1	1-6-3 57 600 0,001 5 %	–	–	1-8-3 7 680 0,000 2 %	1-2-4 3 694 080 0,094 1 %	1-3-4 6 297 600 0,160 4 %	1-4-4 39 747 840 1,012 3 %	1-5-4 168 960 0,004 3 %	1-6-4 7 353 600 0,187 3 %
2	1-6-3-3 15 360 0,000 4 %	1-6-6-3 23 040 0,000 6 %	1-6-8-3 11 520 0,000 3 %	–	–	–	–	–	–
3	–	–	–	–	–	–	–	–	–

i	$\tilde{r}_i = 4$	$\tilde{r}_i = 5$	$\tilde{r}_i = 6$					$\tilde{r}_i = 8$	
0	–	1-5 1 017 600 0,025 9 %	1-6 24 487 680 0,623 7 %	–	–	–	–	1-8 913 920 0,023 3 %	–
1	1-8-4 364 800 0,009 3 %	–	1-3-6 26 880 0,000 7 %	1-4-6 38 400 0,001 0 %	1-5-6 7 680 0,000 2 %	1-6-6 30 720 0,000 8 %	1-8-6 34 560 0,000 9 %	1-4-8 2 196 480 0,055 9 %	1-6-8 1 224 960 0,031 2 %
2	–	–	–	–	–	–	–	–	–
3	–	–	–	–	–	–	–	–	–

i	$\tilde{r}_i = 8$	$\tilde{r}_i = 16$	
0	–	–	–
1	1-8-8 161 280 0,004 1 %	1-6-16 7 680 0,000 2 %	1-8-16 3 840 0,000 1 %
2	–	–	–
3	–	–	–

Приложение Г
(обязательное)
Результаты вычислительных экспериментов

Таблица Г.1. Результаты выч. экспериментов $n = 6$

ЧД	42	50	52	56	60	62	66
Частота	684 064	664	255 136	20	10 704	25 048	80
Доля	68,4064 %	0,0664 %	25,5136 %	0,0020 %	1,0704 %	2,5048 %	0,0080 %

ЧД	70	72	76	80	82	86	90
Частота	2 760	17 512	24	1 720	132	16	16
Доля	0,2760 %	1,7512 %	0,0024 %	0,1720 %	0,0132 %	0,0016 %	0,0016 %

ЧД	92	96	100	102	112	116	120	128
Частота	1216	140	212	4	48	52	32	4
Доля	0,1216 %	0,0140 %	0,0212 %	0,0004 %	0,0048 %	0,0052 %	0,0032 %	0,0004 %

Таблица Г.2. Результаты выч. экспериментов $n = 6$ (нетрив. случай)

ЧД	44	48	54	58	62	64	72
Частота	20	60	72	8	56	12	112
Доля	0,0020 %	0,0060 %	0,0072 %	0,0008 %	0,0056 %	0,0012 %	0,0112 %

ЧД	74	82	92	108	112	132
Частота	4	16	24	4	4	4
Доля	0,0004 %	0,0016 %	0,0024 %	0,0004 %	0,0004 %	0,0004 %

Для $n = 6$: среднее число действий – 46,028, эффективность – 99,900113 %.

Таблица Г.3. Результаты выч. экспериментов $n = 7$

ЧД	56	66	68	78	80	90	92
Частота	789 880	56	186 944	2 596	11 520	416	7 712
Доля	78,9880 %	0,0056 %	18,6944 %	0,2596 %	1,1520 %	0,0416 %	0,7712 %

ЧД	102	104	114	116	122	126	140	146
Частота	304	24	4	480	20	28	12	4
Доля	0,0304 %	0,0024 %	0,0004 %	0,0480 %	0,0020 %	0,0028 %	0,0012 %	0,0004 %

Для $n = 7$: среднее число действий – 58,918, эффективность – 99,990867 %.

Таблица Г.4. Результаты выч. экспериментов $n = 8$

ЧД	72	86	98	100	112	114
Частота	862 644	128 144	724	4 864	64	3 348
Доля	86,2644 %	12,8144 %	0,0724 %	0,4864 %	0,0064 %	0,3348 %

ЧД	126	128	142	154	170	182
Частота	64	4	132	4	4	4
Доля	0,0064 %	0,0004 %	0,0132 %	0,0004 %	0,0004 %	0,0004 %

Для $n = 8$: среднее число действий – 74,106, эффективность – 99,999282 %.

Таблица Г.5. Результаты выч. экспериментов $n = 9$

ЧД	90	106	120	122
Частота	912 976	83 756	188	1 616
Доля	91,2976 %	8,3756 %	0,0188 %	0,1616 %

ЧД	136	138	152	170
Частота	4	1 420	12	28
Доля	0,0004 %	0,1420 %	0,0012 %	0,0028 %

Для $n = 9$: среднее число действий – 91,469, эффективность – 99,999 951 %.

Таблица Г.6. Результаты выч. экспериментов $n = 10$

ЧД	110	128	144	146	164	200
Частота	944 220	54 608	36	504	620	12
Доля	94,4220 %	5,4608 %	0,0036 %	0,0504 %	0,0620 %	0,0012 %

Для $n = 10$: среднее число действий – 111,037, эффективность – 100 %.

Таблица Г.7. Результаты выч. экспериментов $n = 11$

ЧД	132	152	170	172	192	232
Частота	965 320	34 216	16	216	228	4
Доля	96,5320 %	3,4216 %	0,0016 %	0,0216 %	0,0228 %	0,0004 %

Для $n = 11$: среднее число действий – 132,708, эффективность – 100 %.

Таблица Г.8. Результаты выч. экспериментов $n = 12$

ЧД	156	178	198	200	222
Частота	978 436	21 416	12	60	76
Доля	97,8436 %	2,1416 %	0,0012 %	0,0060 %	0,0076 %

Для $n = 12$: среднее число действий – 156,479, эффективность – 100 %.

Таблица Г.9. Результаты выч. экспериментов $n = 13$

ЧД	182	206	230	254
Частота	985 972	13 992	12	24
Доля	98,5972 %	1,3992 %	0,0012 %	0,0024 %

Для $n = 13$: среднее число действий – 182,338, эффективность – 100 %.

Таблица Г.10. Результаты выч. экспериментов $n = 14$

ЧД	210	236	262	288
Частота	990 792	9 192	8	8
Доля	99,0792 %	0,9192 %	0,0008 %	0,0008 %

Для $n = 14$: среднее число действий – 210,240, эффективность – 100 %.

Таблица Г.11. Результаты выч. экспериментов $n = 15$

ЧД	240	268	324
Частота	993 996	5 996	8
Доля	99,3996 %	0,5996 %	0,0008 %

Для $n = 15$: среднее число действий – 240,169, эффективность – 100 %.

Таблица Г.12. Результаты выч. экспериментов $n = 16$

ЧД	272	302	362
Частота	996 064	3 932	4
Доля	99,6064 %	0,3932 %	0,0004 %

Для $n = 16$: среднее число действий – 272,118, эффективность – 100 %.

Таблица Г.13. Результаты выч. экспериментов $n = 17$

ЧД	306	338
Частота	997 550	2 450
Доля	99,7550 %	0,2450 %

Для $n = 17$: среднее число действий – 306,078, эффективность – 100 %.

Таблица Г.14. Результаты выч. экспериментов $n = 18$

ЧД	342	376
Частота	998 050	1 950
Доля	99,8050 %	0,1950 %

Для $n = 18$: среднее число действий – 342,066, эффективность – 100 %.

Таблица Г.15. Результаты выч. экспериментов $n = 19$

ЧД	380	416
Частота	998 650	1 350
Доля	99,8650 %	0,1350 %

Для $n = 19$: среднее число действий – 380,049, эффективность – 100 %.

Таблица Г.16. Результаты выч. экспериментов $n = 20$

ЧД	420	458
Частота	999 100	900
Доля	99,9100 %	0,0900 %

Для $n = 20$: среднее число действий – 420,034, эффективность – 100 %.

Таблица Г.17. Статистика выч. экспериментов $n = 21$

ВК	1		2		3	
ЧД	462	502	462	502	462	502
Частота	333 240	96	333 216	120	333 072	264
Доля	99,9712 %	0,0288 %	99,9640 %	0,0360 %	99,9208 %	0,0792 %

Таблица Г.18. Результаты выч. экспериментов $n = 21$

ЧД	462	502
Частота	999 528	480
Доля	99,9520 %	0,0480 %

Для $n = 21$: среднее число действий – 462,019, эффективность – 100 %.

Таблица Г.19. Статистика выч. экспериментов $n = 22$

ВК	1		2		3	
ЧД	506	548	506	548	506	548
Частота	333 096	240	333 168	168	333 264	72
Доля	99,9280 %	0,0720 %	99,9496 %	0,0504 %	99,9784 %	0,0216 %

Таблица Г.20. Результаты выч. экспериментов $n = 22$

ЧД	506	548
Частота	999 528	480
Доля	99,9520 %	0,0480 %

Для $n = 22$: среднее число действий – 506,020, эффективность – 100 %.

Таблица Г.21. Статистика выч. экспериментов $n = 23$

ВК	1		2		3	
ЧД	552	596	552	596	552	596
Частота	333 288	48	333 288	48	333 312	24
Доля	0,999856 %	0,000144 %	0,999856 %	0,000144 %	0,999928 %	0,000072 %

Таблица Г.22. Результаты выч. экспериментов $n = 23$

ЧД	552	596
Частота	999 888	120
Доля	99,9880 %	0,0120 %

Для $n = 23$: среднее число действий – 552,005, эффективность – 100 %.