Федеральное государственное автономное образовательное учреждение
высшего образования
«Новосибирский национальный исследовательский государственный
университет»

На правах рукописи

Быков Игорь Сергеевич

КОНСТРУКЦИИ ГАМИЛЬТОНОВЫХ ЦИКЛОВ И 2-ФАКТОРОВ С ЛОКАЛЬНЫМИ ОГРАНИЧЕНИЯМИ В БУЛЕВОМ n-КУБЕ

Специальность 01.01.09 —
«Дискретная математика и математическая кибернетика»

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научные руководители:
кандидат физико-математических наук
Евдокимов Александр Андреевич
кандидат физико-математических наук
Пережогин Алексей Львович

Новосибирск — 2021

Оглавление

Введение

Актуальность и степень разработанности темы исследования. Основной объект исследования в данной работе — граф n-мерного гиперкуба. Этот граф является важнейшим объектом изучения в дискретном анализе, теории графов, теории кодирования. Множество вершин это графа может быть интерпретировано как множество всех подмножеств заданного множества мощности n. Такая интерепретация делает изучение этого графа актуальным для многих теоретических областей знаний. Помимо этого, в настоящее время появляются и прикладные задачи, в которых граф n-мерного гиперкуба находит своё применение. Например, широкое распространение получили параллельные суперкомпьютеры, структура сети в которых представляет собой гиперкубы различной размерности [19]. Новые области применения не только предоставляют пространство для использования уже имеющихся теоретических результатов по данной теме, но и ставят новые задачи, которые нуждаются в исследовании. Из-зи актуальности и обширной области применения данного графа, особый интерес представляют разнообразные фундаментальные свойства n-мерного гиперкуба, среди которых помимо различных инвариантов теории графов есть и менее очевидные. К таким фундаментальным свойствам, например, может относиться существование путей, обладающих различными локальными свойствами.

Далее приведём основные формальные определения. Булев *n-куб* (*n-мерный гиперкуб*, *n-мерный куб*) — это граф, вершинами которого являются все двоичные слова длины n; две вершины смежны, если расстояние Хэмминга между соответствующими словами равно 1. В работе граф n-мерного куба будет обозначаться Q_n, а $V(Q_n)$ и $E(Q_n)$ — его множества вершин и рёбер соответственно. Равносильно граф n-мерного гиперкуба можно рекурсивно определить через декартово произведение графов [9]:

$$Q_1 = K_2$$
$$Q_n = K_2 \,\square\, Q_{n-1}.$$

Основные свойства данного графа приведены в обзоре Ф. Харари с соавторами [23].

Путём в графе называется чередующаяся последовательность вершин

$$v_0, v_1, v_2, \ldots, v_l,$$

в которой два соседних элемента являются инцидентными. Число l называется *длиной* пути, v_0 называется *начальной* вершиной, а v_l — *конечной.* Таким образом, последовательность $v_0, v_1, v_2, \ldots, v_l$ вершин графа Q_n образует путь, если $d(v_i, v_{i+1}) = 1$ для всех $i \in \{0, \ldots, l-1\}$. *Цепью* называют путь, все рёбра в котором различны, а *простой цепью* — цепь, для которой также различны все вершины. Цепь, в которой начальная вершина совпадает с конечной, называется *циклом.* Соответственно, цикл, в котором все вершины различны (кроме начальной и конечной), называется *простым циклом.*

Одной из наиболее популярных задач при исследовании путей в графе булева n-куба является задача «змея в ящике» («snake-in-the-box»). Эта задача состоит в построении наибольшей простой цепи в Q_n

$$v_0, v_1, v_2, \ldots, v_l,$$

для которой выполняется следующее условие:

$$\forall i,j \in \{0, \ldots, l\} \quad |i - j| > 1 \Rightarrow d(v_i, v_j) > 1.$$

Условие задачи для краткости можно формулировать другими эквивалентными способами: задача построения максимальной цепи без хорд в Q_n или задача построения максимальной порождённой цепи в Q_n. Данные условия впервые возникли в статье У. Каутца [3] при исследовании кодов, исправляющих ошибки. Впоследствии также известность получила задача «цикл в ящике» («coil-in-the-box»), в которой требуется построить максимальный цикл без хорд. Впервые данная задача была сформулирована в работе Ю. Журавлева [4], а первая оценка длины цикла получена в работе Ю. Васильева [6]. В таблице 1 приведены известные точные решения для этих двух задач. Результаты, представленные в этой таблице, опубликованы в работах У. Каутца [3] , Д. Дэвиса [7], В. Кли [11]. Последние результаты представлены П. Остергардом и В. Петтерсоном в 2014 году [50; 51].

Помимо вычисления точных решений задачи «змея в ящике» существует большое количество результатов, в которых получены верхние и конструктивные нижние оценки. Верхние оценки получены, например, в работах Р. Дугласа

Таблица 1 — Известные точные решения для задач «snake-in-the-box» и «coil-in-the-box»

n	«snake-in-the-box»	«coil-in-the-box»
1	1	0
2	2	4
3	4	6
4	6	8
5	13	14
6	26	26
7	50	48
8	98	96

[8], Ф. Соловьёвой [21], Ж. Земора [33], а конструктивные нижние — в статьях А. Евдокимова [10], Е. Войцеховского [24] и совместной статье Х. Эбботта и М. Качальски [27].

Другим фундаментальным свойством графа гиперкуба, связанным с путями, является гамильтоновость. *Гамильтоновым циклом* называется простой цикл графа, проходящий через все его вершины; граф, содержащий гамильтонов цикл, называют *гамильтоновым.*

Для любого $n \geqslant 2$ достаточно легко привести способ построения гамильтонова цикла в Q_n. Одним из таких способов является код Грея, запатентованный Фрэнком Греем в 1953 году [1] (хотя такой код до этого был продемонстрирован французским инженером Э. Бодо ещё в 1878 году [38]). Строго говоря, *n-мерным кодом Грея* называют последовательность

$$v_0, v_1, v_2, \ldots, v_{2^n-1}$$

двоичных слов длины n, в которой

– все двоичные слова попарно различны;
– каждые два соседних слова в последовательности отличаются в одной позиции;
– v_0 и v_{2^n-1} отличаются в одной позиции;
– $v_0 = \tilde{0}$.

Нетрудно видеть, что любому n-мерному коду Грея соответствует гамильтонов цикл в Q_n. Позднее кодами Грея стали называть произвольные гамильтоновы циклы в графе булева n-мерного куба, а способ, непосредственно приведённый Ф. Греем, в силу своей конструкции получил более точное название — *двоично-отражённый код Грея.* Далее в работе понятия код Грея и гамильтонов цикл в Q_n будут синонимичны и взаимозаменяемы.

Коды Грея имеют многочисленные практические приложения. В силу того, что множество вершин гиперкуба можно интерпретировать как множество всех подмножеств конечного множества, коды Грея находят применение во всех областях математики, где есть потребность в быстром переборе всех подмножеств. Одной из наиболее ранних проблем, связанных с областью комбинаторных алгоритмов, является эффективное перечисление элементов заданного класса комбинаторных объектов, при которой каждый элемент порождается ровно один раз. Однако, чтобы такое перечисление было возможно (даже для множеств умеренной мощности) методы генерации элементов должны быть предельно эффективными. Общий подход состоит в том, чтобы попытаться перечислить элементы комбинаторного класса так, чтобы последовательные элементы отличались «малым» образом, так как это позволит тратить меньше времени на генерацию каждого следующего элемента. Как раз такое перечисление и порождают коды Грея для множества всех подмножеств. В связи с этим гамильтоновы циклы в Q_n применяются при разработке комбинаторных алгоритмов [13].

Другая естественная область приложения кодов Грея — теория кодирования (например, работа А. ван Зантена [29]). Благодаря своей структуре, коды Грея могут исправлять ошибки и устранять шум при коммуникации через канал связи [22]. Также исправление ошибок способствует применению кодов Грея в проектировании жёстких дисков и баз данных [20].

Простое рекурсивное строение некоторых видов кодов Грея позволяет применять их для решения разнообразных математических задач и головоломок, например, таких, как Ханойские Башни [12]. Еще несколько приложений кодов Грея можно найти в других работах и обзорах по данной тематике [32] [39] [46].

Первыми работами, посвященными кодам Грея, были работа Э. Гилберта 1958 года [2], и работа У. Миллса 1963 года [5], в которых выполнялось построение гамильтоновых циклов в Q_n для малых значений n. Достаточно быстро стало понятно, что решение задачи построения кода Грея для произвольного n не составляет труда, и для одной размерности можно построить несколько кодов Грея, причём их число увеличивается с ростом n. Появилась задача подсчёта гамильтоновых циклов в Q_n: сначала в помеченном графе n-мерного гиперкуба (число таких гамильтоновых циклов будем обозначать H_n), а потом и в графе n-мерного гиперкуба с точностью до автоморфизма относительно расстояния Хэмминга (h_n). По этой теме был опубликован ряд работ, последние из которых принадлежат А. Пережогину и В. Потапову [35], И. Дейтеру и А. Дельгадо [42], Ю. Чебиряку и Д. Кронингу [43], Х. Хяянпяя и П. Остергарду [49], Т. Федеру и К. Суби [45]. В последней работе получена асимптотическая оценка на число H_n. Точные известные значения H_n и h_n приведены в таблице 2.

Таблица 2 — Количество кодов Грея

n	h_n	H_n
2	1	1
3	1	6
4	9	1344
5	275065	906545760
6	777739016577752714	35838213722570883870720

В статье Е. Гилберта [2] впервые вводится понятие переходной последовательности пути в Q_n. Будем говорить, что ребро $e = (v,u)$ гиперкуба имеет *направление* i, если двоичные слова v и u отличаются в i-ой позиции. Тогда каждому пути $P = v_0, v_1, v_2, \ldots, v_l$ в Q_n длины l можно сопоставить его *переходную последовательность* $T(P)$:

$$T(P) = t_0, t_1, \ldots t_{l-1},$$

где t_i — направление ребра (v_i,v_{i+1}). Более того, каждой переходной последовательности $T = T(P)$ (а значит и самому пути P) можно сопоставить

– *спектр* $sp(T) = (a_1, a_2, a_3 \ldots, a_n)$, где a_i — количество вхождений символа i в T;
– *набор четности* $Z(T) = \mathtt{z}_1\mathtt{z}_2 \ldots \mathtt{z}_\mathtt{n}$:

$$\mathtt{z_i} = \begin{cases} \mathtt{0}, & \text{если символ } i \text{ встречается четное число раз в } T; \\ \mathtt{1}, & \text{если символ } i \text{ встречается нечетное число раз в } T. \end{cases}$$

В этой же статье Е. Гилберта доказано следующее утверждение.

Утверждение. *Последовательность*

$$T = t_0, t_1, \ldots, t_{l-1}$$

над алфавитом $\{1,2,3,\ldots,n\}$ *является переходной последовательностью кода Грея в* Q_n *тогда и только тогда, когда выполнено каждое из условий:*

- $l = 2^n$;
- $Z(T) = \tilde{0}$;
- *для любого собственного подслова* T' *последовательности* T *выполнено* $Z(T') \neq \tilde{0}$.

Как видно из таблицы 2 и асимптотики для H_n, число кодов Грея очень быстро увеличивается с ростом размерности n гиперкуба. Поэтому появляется задача существования кода Грея, обладающего какими-либо наперёд заданными специальными свойствами. Иногда такие задачи возникают из простого математического интереса, но очень часто такие специальные свойства диктуются многочисленными практическими приложениями кодов Грея. Далее приведём несколько из таких свойств.

Одним из таких свойств является наличие спектра заданного вида. В книге Д. Кнута [46] приведены необходимые условия того, что $(a_1, a_2, a_3 \ldots, a_n)$ является спектром переходной последовательности n-мерного кода Грея:

- a_i — неотрицательное чётное число для любого $i = 1, \ldots, n$;
- $\sum\limits_{i=1}^{n} a_i = 2^n$;
- $\sum\limits_{i=1}^{k} a_{j_i} \geqslant 2^k$ для любого $\{j_1, j_2, \ldots, j_k\} \subseteq \{1,2,\ldots,n\}$ и любого $k = 1, \ldots, n$.

Вопрос, является ли данные условия в совокупности достаточными для существования кода Грея со спектром $(a_1, a_2, a_3 \ldots, a_n)$, остаётся открытым. В работе В. Потапова [48] доказано, что если для некоторого большого N данные необходимые условия являются достаточными, то это верно и для любой большей размерности.

Частным случаем задачи нахождения кода Грея с заданным спектром является задача построения кода Грея, обладающего свойством *сбалансированности спектра.* В гамильтоновых циклах, удовлетворяющих этому свойству, переходная последовательность содержит каждый символ из $\{1,2,\ldots,n\}$ «примерно» одинаковое число раз. В случае, если любые два значения из спектра гамильтонова цикла отличаются не больше чем на 2, говорят, что данный гамильтонов цикл является *сбалансированным*. В этом случае спектр содержит только значения $2\left\lfloor\frac{2^{n-1}}{n}\right\rfloor$ и $2\left\lfloor\frac{2^{n-1}}{n}\right\rfloor+2$. Исследование таких кодов Грея проводилось, например, в статье В. Викерса и Дж. Сильвермана [14] и статье Дж. Лудмана [17]. Завершила эти исследования совместная работа Г. Бхата и К. Сэвэдж [30], в которой они показали, что сбалансированный код Грея существует для любого $n > 1$.

Очевидно, что все значения, входящие в спектр, могут оказаться одинаковыми только если $n = 2^k$ для некоторого k. При этом спектр будет состоять из значений $\frac{2^n}{n}$. Код Грея, все значения спектра в котором одинаковы, называется *абсолютно сбалансированным* кодом Грея. Проблема существования абсолютно сбалансированных гамильтоновых циклов была решена в работе Д. Вагнера и Дж. Веста [28], в которой показано, что такие коды Грея существуют для любого n, являющегося степенью двойки.

Свойство сбалансированности спектра кода Грея является глобальным: оно не накладывает дополнительных ограничений на подслова малой длины в переходной последовательности кода. Одним из локальных свойств кодов Грея является свойство *локальной равномерности*. Рассмотрим переходную последовательность произвольного n-мерного кода Грея C. Пусть $l_1(C)$ — наибольшее число, такое что в каждом подслове длины $l_1(C)$ переходной последовательности кода Грея C все символы различны. Чем больше число $l_1(C)$ тем более равномерную, «хорошо перемешанную» переходную последовательность мы имеем. Пусть $l_1(n)$ — максимальное значение $l_1(C)$ среди всех n-мерных кодов. Коды, достигающие $l_1(n)$ являются самыми равномерными относительно параметра l_1.

Основным направлением при исследовании кодов Грея с параметром l_1 является изучение поведения функции $l_1(n)$ с помощью построения верхних и нижних оценок. К сожалению, на данный момент не известно верхней оценки для $l_1(n)$, отличной от тривиальной. Однако, получен ряд результатов, касающихся нижних оценок для $l_1(n)$. Все они строятся конструктивно, что и проделано в работе А. Евдокимова [15] и работе Л. Годдина, Дж. Лоуренса и Э. Немета [22]. Наилучшая известная нижняя оценка на данный момент получена в работа Л. Годдина и П. Гвоздяка в 2003 году [37]:

$$l_1(n) \geqslant n - \lceil 2.001 \log n \rceil.$$

В работе А. Пережогина [31] представлена оценка на максимальную длину цикла, обладающего оптимальным значением параметра l_1. В четвёртой главе диссертации рассматривается задача построения локально равномерных кодов Грея относительно другого параметра локальной равномерности — l_2.

Еще одним свойством кодов Грея является свойство *антиподальности*. Код Грея размерности n называется $(n{,}t)$ — *антиподальным*, если для любой пары противоположны вершин (v_i, v_j) выполняется $|i-j| = t$ или $|i-j| = 2^n - t$. Из двудольности графа Q_n следует, что для существования $(n{,}t)$-антиподального кода Грея необходимо, чтобы числа n и t были одной чётности. В статье Ч. Киллиана и К. Сэвэдж [36] получены результаты для $(n{,}n)$-антиподальных кодов Грея, а в работе Дж. Чанга, С.-П. Ю и Ч.-Х. Е [41] рассматриваются $(n{,}t)$-антиподальные коды для произвольного t.

Некоторые другие свойства кодов Грея можно найти в обзоре К. Сэвэдж [32]. Во второй главе диссертации рассмотрено новой специальное свойство кодов Грея — свойство дистанционности.

Для построения кодов Грея, обладающих теми или иными специальными свойствами, использовались разнообразные конструкции кодов Грея. Несомненно, простейшей из таких конструкций является двоично-отражённый код Грея, представленный ещё в 1953 году. В дальнейшем было представлено большое количество конструкций кодов Грея: конструкция Бакоша [25], конструкция Робинсона-Кона [18], конструкция Рамраса [26], конструкция Потапова [48]. Обзор и классификация этих и других конструкций представлены в первой главе данной работы. В третьей главе представлена новая конструкция кодов Грея, которая применена для получения основного результата в пятой главе.

Естественным обобщением понятия гамильтонов цикл является 2-фактор. *2-фактором* называется остовный 2-регулярный подграф. Другими словами, 2-фактор представляет собой набор попарно вершинно непересекающихся простых циклов, покрывающих все вершины графа. Гамильтонов цикл является частным случаем 2-фактора — в этом случае 2-фактор содержит единственный цикл, который и является гамильтоновым.

Существует ряд известных результатов, касающихся 2-факторов в Q_n. Так, в работе А. ван Зантена и Л. Харианто [44] решалась задача построения 2-фактора в Q_n, каждый цикл в котором является «циклом в ящике». Новое доказательство гамильтоновости графа средних слоёв гиперкуба от П. Грегора, Т. Мютце и Й. Нумменпало [57] состоит в объединении 2-фактора в единый цикл. Недавний результат И. Финка устанавливает, что любое паросочетание в Q_n может быть расширено до 2-фактора [59]. В пятой главе решается задача построения 2-фактора, не содержащего близких рёбер одного направления, в Q_n.

Целью данной работы является исследование существования и несуществования гамильтоновых циклов и 2-факторов в графе булева n-мерного куба, удовлетворяющих некоторым локальным ограничениям, а также построение таких циклов.

Задачи:

1. Оценить функцию параметра локальной равномерности $l_2(n)$ кодов Грея.
2. Определить, при каких наборах параметров в графе булева n-куба существуют дистанционные коды Грея.
3. Построить 2-фактор, не содержащий близких рёбер в булевом n-кубе.

Научная новизна и значимость работы Все результаты, представленные в работе являются новыми. Работа носит теоретический характер. Полученные конструкции и теоретические результаты могут быть применены в дальнейших исследованиях графа булева n-куба. Также результаты данной работы могут использоваться в спецкурсах для студентов, специализирующихся в области дискретной математики.

Методы исследования. В работе применялись методы комбинаторики, дискретного анализа и теории графов. Для проверки результатов и выдвижения гипотез были использованы компьютерные эксперименты.

Основные результаты диссертации:

1. Найдена конструктивная верхняя оценка $n + 3\log n$ для параметра локальной равномерности кодов Грея.
2. Приведено несколько способов построения дистанционных кодов Грея. Для двух нетривиальных серий параметров доказано несуществование кодов Грея.
3. Предложена новая конструкция 2-факторов и гамильтоновых циклов в булевом кубе.
4. Доказано, что в булевых кубах размерностей $n \geqslant 10$ существуют 2-факторы без близких рёбер с длинами циклов не меньше $2^{n/4}$.

Апробация работы. Основные результаты работы в разные годы докладывались на научных семинарах Института Математики им. С.Л. Соболева

СО РАН: «Комбинаторика и символьные последовательности» под руководством к.ф.-м.н. А.А. Евдокимова, «Дискретный анализ» под руководством к.ф.-м.н. А.А. Евдокимова, «Теория кодирования» под руководством д.ф.-м.н. Ф.И. Соловьёвой и к.ф.-м.н. С.В. Августиновича; а также на Международной студенческой конференции МНСК-2015, на Международной конференции «Дискретные модели в теории управляющих систем» (2015 и 2018 гг.), на Международном семинаре «Дискретная математика и её приложения» (2016 г.), на Международной конференции, посвященной 60-летию Института Математики им. Соболева «Математика в современном мире» (2017 г.).

Публикации. Основные результаты по теме диссертации изложены в 7 работах [54; 56; 60; 52; 53; 55; 58], из них 3 статьи опубликованы в журналах из списка ВАК [54; 56; 60], 4 — в тезисах и трудах международных конференций [52; 53; 55; 58]. Результаты работы [56] получены в неразделимом соавторстве с А. Л. Пережогиным.

Структура и объём диссертации. Диссертация состоит из введения, пяти глав, заключения и приложения. Полный объем диссертации 74 страницы текста с 2 рисунками и 15 таблицами. Список литературы содержит 60 наименований.

Глава 1. Определения и обозначения

Сначала приведём еще ряд определений и обозначений, которые будут использоваться в тексте работы помимо тех, что уже были представлены во введении.

Весом двоичного слова v будем называть количество его ненулевых символов. Через $W(v)$ будем обозначать чётность веса вершины v: $W(v) = 0$ для вершин чётного веса, $W(v) = 1$ для вершин нечётного веса. Иногда для краткости вершину v будем называть чётной или нечётной в зависимости от значения $W(v)$.

Записью $supp(v)$ будем обозначать *носитель* двоичного слова $v = \mathtt{x_1x_2x_3\ldots x_n}$ — множество номеров позиций i, для которых $\mathtt{x_i} = \mathtt{1}$. Таким образом, $supp(v) \subseteq \{1{,}2,\ldots,n\}$.

На множестве двоичных слов одинаковой длины естественным образом определяется операция $\oplus$ поразрядного сложения по модулю 2. Символом $\overline{v}$ будем обозначать инверсию двоичного слова v: $\overline{v} = v \oplus \tilde{1}$.

Пусть дан код Грея

$$C = v_0, v_1, \ldots, v_{2^n-1}.$$

Будем говорить, что слова v_i и v_j находятся *на расстоянии k по коду*, если между вхождениями вершин v_i и v_j в C находится $k-1$ других вершин. Таким образом, очевидно, что если v_i и v_j находятся на расстоянии k по коду, то они находятся и на расстоянии $2^n - k$ по коду. В силу двудольности Q_n имеет место следующее утверждение

Утверждение. *Пусть v_i и v_j находятся на расстоянии k по коду в C. Тогда k и $d(v_i, v_j)$ имеют одинаковую четность.*

1.1 Конструкции кодов Грея

Коды Грея, обладающие специальными свойствами, очевидно, имеют разное строение, и в общем случае не могут быть построены одними и теми же способами. Поэтому при решении тех или иных задач, связанных с кодами Грея, необходимо применять различные схемы (или алгоритмы) построения кодов Грея. Такие схемы построения далее в работе мы будем называть *конструкциями.*

Все конструкции можно классифицировать следующим образом

1. Конструкции, позволяющие по n-мерному коду Грея (или какой-либо другой специальной структуре в n-мерном гиперкубе) построить $(n+p)$-мерный код Грея для некоторой константы p. Наиболее распространены конструкции, двигающиеся с шагом 1 или 2: то есть получают $(n+1)$-мерный или $(n+2)$-мерный код Грея из n-мерного. К конструкциям такого типа относятся двоично-отражённый код Грея, конструкции Бакоша, Рамраса и Робинсона-Кона.
2. Конструкции, использующие различные структуры в Q_n и Q_k для построения $(n+k)$-мерного кода Грея. К таким конструкциям можно отнести торическую конструкцию, конструкцию Потапова и потоковую конструкцию, которая будет рассмотрена в главе 3.
3. Прямое построение n-мерного кода Грея. В отдельных случаях гамильтонов цикл, обладающий желаемым свойством можно построить напрямую сразу для размерности n. В качестве примера в последнем разделе настояще главы мы рассмотрим построение v-добавочного кода Грея.

Двоично-отраженный код Грея

Пусть $T = t_0, t_1, t_2, \ldots, t_{2^n-1}$ — переходная последовательность некоторого n-мерного кода Грея, где $t_i \in \{1{,}2, \ldots, n\}$. Тогда нетрудно видеть, что последовательности

$$\varphi(T) = t_0, t_1, t_2, \ldots, t_{2^n-3}, t_{2^n-2}, n+1, t_0, t_1, t_2, \ldots, t_{2^n-3}, t_{2^n-2}, n+1,$$

и

$$\psi(T) = t_0, n+1, t_1, n+1, t_2, \ldots, t_{2^n-2}, n+1, t_{2^n-1}, n+1$$

являются переходными последовательностями $(n+1)$-мерного кода Грея.

При последовательном применении отображения φ к переходной последовательности 2-мерного кода Грея с переходной последовательностью 1,2,1,2 получается *двоично-отраженный код Грея* (результат построения представлен в таблице 3).

Таблица 3 — Построение двоично-отраженных кодов Грея.

$n = 2$	T	1,2,1,2
$n = 3$	$\varphi(T)$	1,2,1,3,1,2,1,3
$n = 4$	$\varphi(\varphi(T))$	1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,4
$n = 5$	$\varphi(\varphi(\varphi(T)))$	...
...	...	...

Те же самые переходные последовательности (с точностью до замены символов) получаются при последовательном применении ψ к переходной последовательности 2-мерного кода Грея.

Эти два простейших преобразования, сохраняющих свойство «быть переходной последовательностью кода Грея» и стали основой первой работы по данной тематике, в которой Ф. Грей установил существование гамильтоновых циклов в Q_n [1]. Полученные коды он и назвал двоично-отраженными. Данная конструкция являются простейшей для реализации среди всех конструкций кодов Грея, поэтому применяется в приложениях во всех случаях, когда на перечисление двоичных слов не накладывается никаких дополнительных свойств. В различных областях приложений нельзя обойтись стандартным двоично-отраженным кодом Грея, так как требуется, чтобы код отвечал определенным требованиям, которые зачастую несовместимы со свойствами двоично-отраженного кода Грея. В этих случаях приходится прибегать к помощи других конструкций кодов Грея, которые обеспечивают широкий простор для построения гамильтоновых циклов в Q_n с различными особенностями.

Конструкция Рамраса

Следующая конструкция является обобщением отображения φ используемого при построении двоично-отраженного кода Грея. Она была приведена Рамрасом в [26] в качестве решения задачи о некомпозитном коде Грея. Код Грея называется *некомпозитным*, если для любого $k \in \{2,3,\ldots,n{-}1\}$ любые 2^k подряд идущих слов не являются гамильтоновой цепью в некотором k-мерном подкубе Q_n. *Конструкция Рамраса* определяется следующей теоремой.

Теорема (Рамрас)**.** *Пусть T — переходная последовательность кодов Грея размерности n, а $(a_1, a_2, \ldots, a_n)$ — его спектр. Положим q — произвольное нечётное число с условием $q < a_i$ для некоторого $1 \leqslant i \leqslant n$. Тогда если T' — последовательность, полученная из T заменой любых q вхождений i-го символа на символ $(n+1)$, то последовательность (T', T') является переходной последовательностью $(n+1)$-мерного кода Грея.*

Важным свойством данной конструкции является тот факт, что она сохраняет свойство некомпозитности, если $3 \leqslant q \leqslant a_i - 3$. Этот результат представляется весьма любопытным: чтобы построить код Грея максимально далёкий от двоично-отраженного кода Грея (можно считать его «максимально композитным»), нужно лишь немного обобщить простейшую конструкцию.

Конструкция Бакоша и конструкция Робинсона-Кона

Теперь рассмотрим конструкцию, впервые упомянутую в [25]. Она использует переходную последовательность кода Грея размерности n для построения $(n+2)$-мерного кода Грея.

Пусть $U = u_0, u_1, \ldots, u_k$ — некоторая последовательность символов. Символом U^R будем обозначать инверсию $U^R = u_k, u_{k-1}, \ldots, u_1, u_0$ последовательности U. Имеет место следующая теорема:

Теорема (Бакош)**.** *Пусть $T = t_0, U_0, t_1, U_1, t_2, \ldots, U_{l-1}, t_l, U_l, t_{l+1}, t_{l+2}$ — переходная последовательность n-мерного кода Грея, где каждое U_i — это* *некоторая последовательность (возможно пустая), а l — чётное число. Тогда последовательность*

$$\begin{aligned}
n+2, n+1, n+2, t_0,\\
U_0, n+2, U_0^R, n+1, U_0, t_1,\\
U_1, n+1, U_1^R, n+2, U_1, t_2,\\
\vdots\\
U_{2i}, n+2, U_{2i}^R, n+1, U_{2i}, t_{2i+1},\\
U_{2i+1}, n+1, U_{2i+1}^R, n+2, U_{2i+1}, t_{2i+2},\\
\vdots\\
U_{l-1}, n+1, U_{l-1}^R, n+2, U_{l-1}^R, t_l,\\
U_l, n+2, U_l^R, n+1, U_l, t_{l+1},\\
n+2, n+1, n+2, t_{l+1}\\
U_l^R, t_l, U_{l-1}^R, \ldots, t_1, U_0^R, t_0
\end{aligned}$$

является переходной последовательностью $(n+2)$-мерного кода Грея.

Конструкция, приведенная в теореме, получила название *конструкция Бакоша*. Самая известная вариация конструкции Бакоша была представлена в работе [18] и получила название *конструкция Робинсона-Кона*. Данная конструкция описывается следующей теоремой:

Теорема (Робинсон, Кон). *Пусть $T = U_1, t_1, t_2, U_2, t_3, U_3 \ldots, t_{l-2}, U_{l-2}, t_{l-1}, t_l, U_l$ — переходная последовательность n-мерного кода Грея, где каждое U_i — это некоторая последовательность (возможно пустая), а l — чётное число. Тогда последовательность*

$$\begin{aligned}
U_2, n+1, U_2^R, n+2, U_2, t_3,\\
U_3, n+2, U_3^R, n+1, U_3, t_4,\\
\vdots\\
U_{2i}, n+1, U_{2i}^R, n+2, U_{2i}, t_{2i+1},\\
U_{2i+1}, n+2, U_{2i+1}^R, n+1, U_{2i+1}, t_{2i+2},\\
\vdots\\
U_{l-2}, n+1, U_{l-2}^R, n+2, U_{l-2}, t_{l-1},\\
n+2, n+1, t_l, U_l,
\end{aligned}$$

$$U_1, n+2, U_1^R, U_l^R,$$
$$t_l, t_{l-1}, t_{l-2}, U_{l-2}^R, t_{l-3}, \ldots, U_2^R, t_2, n+1,$$
$$t_1, U_1^R, U_l^R, n+2,$$
$$U_l, U_1, t_1, n+1, t_2$$

является переходной последовательностью $(n+2)$*-мерного кода Грея.*

Схемы конструкции Бакоша и конструкции Робинсона-Кона изображены на рисунке 1.1.

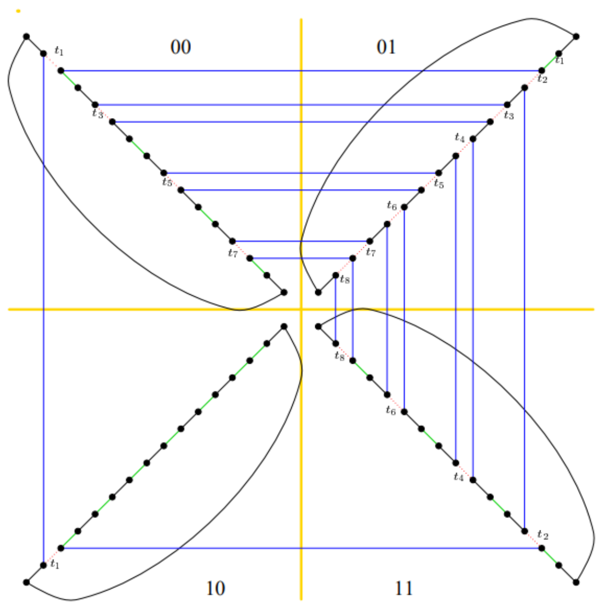

Рисунок 1.1 — Конструкция Робинсона-Кона.

Конструкция Потапова

Рассмотрим произвольный код Грея в Q_k с переходной последовательностью

$$r_0, t_0, r_1, t_1, \ldots, r_{2^{k-1}-1}, t_{2^{k-1}-1}.$$

Рёбра этого цикла очевидным образом разбиваются на два непересекающихся совершенных паросочетания M_1 (с направлениями r_i) и M_2 (с направлениями t_i). Поскольку каждой вершине Q_k в декартовом произведении $Q_n \times Q_k$ соответствует n-мерный гиперкуб, каждому ребру из M_2 можно сопоставить пару параллельных n-мерных кубов, то есть один $(n+1)$-гиперкуб. Заменим каждое ребро $e_i \in M_2$ гамильтоновым циклом в $(n+1)$-гиперкубе, проходящим через это ребро. Очевидно, что переходная последовательность этого гамильтонова цикла может быть представлена в виде t_iT_i, где t_i — направление ребра e_i.

Теорема (Потапов). *Последовательность*

$$r_0, T_0, r_1, T_1, \ldots, r_{2^{k-1}-1}, T_{2^{k-1}-1}$$

является переходной последовательностью $n+k$-мерного кода Грея.

Это построение приведено В. Н. Потаповым в [48]. В данной работе приведенная конструкция используется для доказательства условного покрытия всех наборов, удовлетворяющих необходимым условиям спектров кодов Грея, в случае если покрываются такие наборы в гиперкубах всех размерностей, не превосходящих достаточно большого N.

Торическая конструкция

Достаточно естественной кажется идея построить гамильтонов цикл в Q_{n+k}, используя гамильтоновы циклы в кубах размерности n и k. При декартовом перемножении двух гамильтонов циклов образуется тор, по узлам которого и проходит новый гамильтонов цикл в Q_{n+k} (см рис. 1.2). По этой причине конструкция и получила название *торической*.

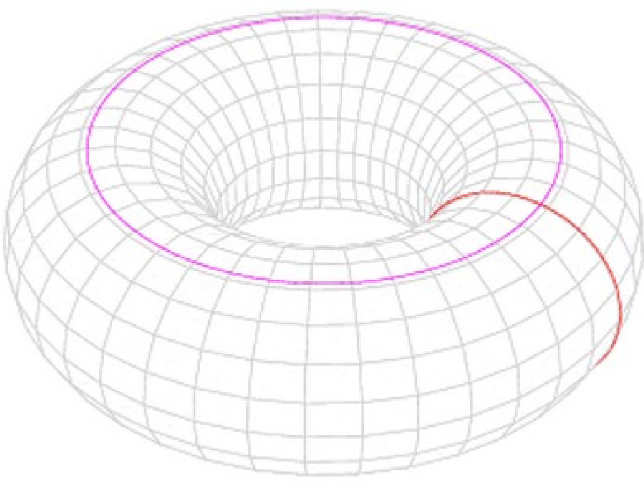

Рисунок 1.2 — Тор в Q_{n+k}.

Пусть R и T — переходные последовательности кодов Грея над алфавитами мощности n и k, не имеющими общих букв. Периодически повторяя слова R и T, получим две последовательности:

$$R, R, R, \dots$$

$$T, T, T, \dots$$

Пусть $P = \{p_i\}_{i=1}^m$ и $Q = \{q_i\}_{i=1}^m$ — последовательности положительных целых чисел такие, что $\sum_{i=1}^m (p_i + q_i) = 2^{n+k}$. Начальный отрезок длины $\sum_{i=1}^m p_i$ последовательности R,R,$R, \dots$ разобьем на блоки длины $p_1, p_2, \dots, p_m$, а начальный отрезок длины $\sum_{i=1}^m q_i$ последовательности T,T,$T, \dots$ разобьем на блоки длины $q_1, q_2, \dots, q_m$, изображая это схематически так:

$$[r_0][r_1]\dots[r_i]\dots[r_t],$$

$$[t_0][t_1]\dots[t_i]\dots[t_t],$$

где $[r_i]$ и $[t_i]$ — блоки длины p_i и q_i соответственно.

Образуем слово X последовательным чередованием $[r_i]$ и $[t_i]$ блоков

$$X = [r_0][t_0][r_1][t_1]\dots[r_i][t_i]\dots[r_m][t_m].$$

По построению, длина слова X равна 2^{n+k}. Для этого слова X справедлива лемма:

Лемма 1.1.1. *Слово X является переходной последовательностью кода Грея размерности $n + k$, тогда и только тогда, когда последовательности P и Q периодические, и $\sum_{i=1}^M p_i$ и $\sum_{i=1}^M q_i$ — нечетные числа, сумма которых равна $2^{\min\{n,k\}}$, где M — наименьшее общее кратное периодов последовательностей P и Q.*

Эта конструкция была первой конструкцией, которую применяли для решения задачи о локально-равномерных кодах Грея [15]. Гамильтонов цикл, полученный в результате применения этой конструкции, существенно ограничен в выборе рёбер: он может использовать только рёбра получившегося тора, количество которых намного меньше количества рёбер Q_{n+k}.

Конструкция v-добавочного кода Грея

Наконец, рассмотрим пример кода Грея, построение которого осуществляется напрямую для любой размерности n. Этот вид кода будет использоваться для доказательства основного результата главы 4.

Код Грея назовём *v-добавочным*, если для любых двух слов u_1 и u_2, находящихся на расстоянии 2^{n-1} по коду, выполнено

$$u_1 \oplus v = u_2.$$

Для доказательства нам понадобится утверждение, приведенное в работе [16]:

Теорема (Чен, Куимпо). *В Q_n между любыми двумя вершинами различной четности существует гамильтонова цепь.*

Теперь мы можем доказать лемму, устанавливающую критерий существования v-добавочных кодов.

Лемма 1.1.2. *При $n \geqslant 2$ v-добавочный код Грея существует тогда и только тогда, когда $W(v) = 0$.*

Доказательство. При $n \geqslant 2$ число 2^{n-1} чётное, а значит, в силу двудольности графа Q_n v-добавочный код Грея не существует, если $W(v) = 1$.

Пусть теперь $W(v) = 0$. Построим переходную последовательность v-добавочного кода Грея. Выберем произвольное $i \in supp(v)$. Пусть вершина u получена из вершины v заменой $\mathtt{1}$ на $\mathtt{0}$ в i-ой позиции. Тогда u — вершина нечётного веса. Вершины $(\tilde{\mathtt{0}})$ и u разной чётности и лежат в подкубе размерности $n-1$, образованном вершинами с $\mathtt{0}$ в i-ой позиции. Пусть T — переходная последовательность гамильтоновой цепи из $(\tilde{\mathtt{0}})$ в u в этом подкубе. Теперь легко убедиться, что последовательность T, i, T, i является переходной последовательностью кода Грея, обладающего желаемым свойством. $\square$

Таким образом, для построения v-добавочного кода Грея необходимо лишь соединить две одинаковые гамильтоновы цепи в подкубах размерности $n-1$ в единый цикл. Гамильтонов цикл, имеющий такую структуру, будем называть *2-композитным.* Так как при чётном n вершина $\tilde{\mathtt{1}}$ является чётной, то имеет место следующее следствие.

Следствие 1.1.1. *Для любого чётного n существует 2-композитный $(n, 2^{n-1})$-антиподальный код Грея.*

Глава 2. Дистанционные коды Грея

2.1 Определение и простейшие свойства

Назовем n-мерный код $\langle d{,}k\rangle_n$-*дистанционным кодом Грея*, если расстояние Хэмминга между словами, находящимися в коде на расстоянии k, равно d. Далее для краткости такой код будем называть $\langle d{,}k\rangle_n$-кодом, а параметры $d{,}k$ — параметрами дистанционности данного кода.

Пример 2.1.1. *Код Грея с переходной последовательностью*

$$T = 1, 2, 1, 3, 1, 2, 1, 3$$

является $\langle 2{,}4\rangle_3$-кодом. Действительно, любое подслово T длины 4 дважды содержит символ 1, а символы 2, 3 — по одному разу. Значит, расстояние Хэмминга между словами, расположенными в коде на расстоянии 4 равно 2. То есть, этот код Грея является $\langle 2{,}4\rangle_3$-кодом.

Пример 2.1.2. *Код Грея с переходной последовательностью*

$$T = 1, 2, 3, 4, 1, 2, 3, 5, 1, 4, 3, 2, 1, 4, 3, 5, 1, 2, 3, 4, 1, 2, 3, 5, 1, 4, 3, 2, 1, 4, 3, 5$$

является $\langle 4{,}4\rangle_5$-кодом. Любое подслово T длины 4 содержит 4 различных символа. Следовательно, расстояние Хэмминга между словами, расположенными в коде на расстоянии 4, равно 4. То есть, этот код Грея является $\langle 4{,}4\rangle_5$-кодом.

В таблице 4 приведены все наборы значений параметров $1 < d < 5$ и k, для которых существует $\langle d{,}k\rangle_5$-код. Для малых значений можно привести и несколько нетривиальных наборов параметров, когда дистанционного кода Грея не существует. Например, не существует $\langle 3{,}3\rangle_3$-, $\langle 3{,}3\rangle_4$- и $\langle 3{,}5\rangle_4$-дистанционных кодов Грея.

Далее докажем простейшие свойства кодов Грея, касающиеся дистанционности.

Таблица 4 — $\langle d,k\rangle_5$-коды

n	d	k	Пример переходной последовательности кода
5	2	2	(1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5,1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5)
5	2	4	(1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5,1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5)
5	2	6	(1,2,1,3,1,2,4,2,1,3,1,2,1,3,5,2,1,2,3,1,2,1,4,3,2,3,1,2,3,2,5,3)
5	2	8	(1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5,1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5)
5	2	10	(1,2,1,3,1,2,1,4,1,3,2,5,1,3,4,2,1,4,1,3,1,4,1,2,1,3,4,5,1,3,2,4)
5	2	12	(1,2,1,3,1,2,1,4,1,2,1,3,1,5,1,3,1,2,1,4,1,2,1,3,1,2,1,4,1,5,1,4)
5	2	14	(1,2,1,3,1,2,1,4,1,2,1,3,1,2,5,2,1,4,1,2,1,3,1,2,1,4,1,2,1,3,5,4)
5	2	16	(1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5,1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5)
5	3	3	(1,2,3,1,2,4,3,1,5,3,1,4,2,1,4,3,5,1,4,5,1,2,3,5,4,2,1,5,3,2,4,5)
5	3	5	(1,2,1,3,1,4,5,1,2,1,4,3,4,5,2,5,1,4,1,3,1,2,5,1,4,1,2,3,2,5,4,5)
5	3	7	(1,2,1,3,1,2,4,1,4,5,4,2,4,1,4,5,1,3,1,5,1,2,5,1,5,3,4,3,2,1,2,5)
5	3	9	(1,2,1,3,1,2,1,4,1,5,2,5,3,2,5,4,3,2,1,2,4,2,5,3,2,5,2,1,4,1,2,5)
5	3	11	(1,2,1,3,1,2,1,4,1,2,1,3,5,1,5,2,5,3,2,1,2,4,2,1,2,3,2,1,2,4,5,4)
5	3	13	(1,2,1,3,1,2,1,4,1,2,1,3,1,5,1,2,5,1,5,3,2,1,2,4,2,1,2,3,2,1,2,5)
5	3	15	(1,2,1,3,1,2,1,4,1,2,1,3,2,1,2,5,2,1,2,3,2,1,2,4,2,1,2,3,1,2,1,5)
5	4	4	(1,2,3,4,1,2,3,5,1,4,3,2,1,4,3,5,1,2,3,4,1,2,3,5,1,4,3,2,1,4,3,5)
5	4	8	(1,2,1,3,2,1,2,4,1,2,1,3,2,1,2,5,1,2,1,3,2,1,2,4,1,2,1,3,2,1,2,5)
5	4	12	(1,2,1,3,1,2,4,3,1,2,1,3,1,2,5,3,1,2,1,3,1,2,4,3,1,2,1,3,1,2,5,3)
5	4	14	(1,2,1,3,1,2,1,4,1,3,1,2,1,3,1,5,1,2,1,3,1,2,1,4,1,3,1,2,1,3,1,5)
5	4	16	(1,2,1,3,1,2,1,4,1,2,1,3,1,5,3,1,2,1,3,5,1,5,2,4,1,2,3,2,1,2,3,5)

Утверждение 2.1.1. *Любой n-мерный код Грея является $\langle 1,1\rangle_n$- и $\langle 2,2\rangle_n$-кодом при $n \geqslant 2$.*

Доказательство. В любом коде Грея слова, находящиеся на расстоянии 1 по коду, очевидно отличаются ровно в одной позиции; следовательно, любой код Грея является $\langle 1,1\rangle_n$-кодом.

Аналогично, в n-мерном коде Грея (при $n \geqslant 2$) слова, находящиеся на расстоянии 2 по коду, отличаются ровно в двух позициях. Значит, любой код Грея является $\langle 2,2\rangle_n$-кодом при $n \geqslant 2$. $\square$

Утверждение 2.1.2. *Если существует $\langle d,k\rangle_n$-код, то d и k одной четности.*

Доказательство. Пусть v и u — произвольные двоичные слова длины n, и расстояние по коду между ними равно k'. В силу двудольности Q_n, четность расстояния Хэмминга $d(u,v)$ совпадает с четностью k'. Отсюда, если код Грея является $\langle d,k\rangle_n$-кодом, то параметры дистанционности должны быть одной четности. □

Утверждение 2.1.3. *Если существует $\langle d,k\rangle_n$-код, то он является $\langle d, 2^n - k\rangle_n$-кодом, и при этом $d \leqslant \min(k, 2^n - k)$.*

Доказательство. Очевидно, если два слова находятся на расстоянии k по коду в n-мерном коде Грея, то эти два слова в тоже время находятся на расстоянии $2^n - k$ по коду (для этого достаточно двигаться по списку слов кода в обратном порядке). Значит, любой $\langle d,k\rangle_n$-код является $\langle d, 2^n - k\rangle_n$-кодом.

Ясно, что если расстояние между двумя словами по коду k, то расстояние Хэмминга между этими словами не может быть больше k. Следовательно, $d \leqslant \min(k, 2^n - k)$. □

При изучении дистанционных кодов Грея возникают традиционные задачи, связанные со специальными кодами Грея: установить существование или несуществования кодов Грея с заданными параметрами дистанционности, и, если код существует, привести способ его построения.

Свойство дистанционности можно рассматривать не только для кодов Грея, но и для произвольных циклов и даже незамкнутых маршрутов в Q_n. В случае, если кода Грея с данными параметрами дистанционности не существует, интересной представляется задача построения цикла (маршрута) максимальной длины, с такими параметрами. Однако исследование этой задачи остается за рамками данной работы.

Дистанционные коды Грея связаны с некоторыми другими специальными классами кодов Грея. Например, дистанционные коды Грея имеют отношение к (n,t)-антиподальным кодам Грея. Как был сказано ранее, в [41] показано, что для любого четного n существует $(n,2^{n-1})$-антиподальный код Грея. Таким образом, любые два слова, находящиеся на расстоянии 2^{n-1} в таком коде являются противоположными — то есть расстояние Хэмминга между ними равно n. Значит, любой $(n,2^{n-1})$-антиподальный код Грея является $\langle n,2^{n-1}\rangle_n$-кодом. Имеет место более сильное утверждение.

Утверждение 2.1.4. *$\langle n,k\rangle_n$-код существует тогда и только тогда, когда n — четное число и $k = 2^{n-1}$.*

Доказательство. Пусть $v_0, v_1, \ldots, v_{2^n-1}$ — $\langle n,k\rangle_n$-код. Отсюда, для любого i: $v_i = \overline{v_{i+k}} = \overline{v_{i-k}}$. Значит, $i + k \equiv i - k \mod 2^n$, что возможно тогда и только тогда, когда $k = 2^{n-1}$, а, следовательно, n — четное по предложению 2.1.2. В этом случае $(n,2^{n-1})$-антиподальный код Грея является искомым дистанционным кодом Грея. □

Заметим, что если в n-мерном коде Грея расстояние между словами v и u по коду равно 2^{n-1}, а $d(v,u) = n$, то любое из соседних с u слов по коду отличается от v в $n - 1$ позиции. То есть имеет место следующее следствие.

Следствие 2.1.1. *Если n— четное число, то существует $\langle n-1,2^{n-1}-1\rangle_n$-код Грея.*

Также дистанционные коды Грея связаны с равномерными кодами Грея. Утверждения 2.1.5, 2.1.6 устанавливают связь дистанционных кодов Грея с равномерными кодами Грея относительно параметров l_1 и l_2 соответственно.

Утверждение 2.1.5. *Код Грея C является $\langle d,d\rangle_n$-кодом тогда и только тогда, когда $l_1(C) \geqslant d$. В частности, код C является $\langle n-1,n-1\rangle_n$-кодом тогда и только тогда, когда $l_1(C) = n - 1$ для $n \geqslant 3$.*

Доказательство. Пусть C — $\langle d,d\rangle_n$-код. Это выполнено тогда и только тогда, когда в любом подслове длины d переходной последовательности кода C все символы различны. Что и означает, что $l_1(C) \geqslant d$.

Так как при $n \geqslant 3$ параметр равномерности ограничен сверху $l_1(C) \leqslant n - 1$, то утверждения $l_1(C) = n-1$ и C является $\langle n-1,n-1\rangle_n$-кодом эквивалентны при $n \geqslant 3$. □

Утверждение 2.1.6. *Если для кода C выполнено $l_2(C) = n + 1$, то код C является $\langle n-1,n+1\rangle_n$-кодом.*

Доказательство. Пусть для кода C выполнено $l_2(C) = n + 1$. Тогда в любом подслове T длины $n + 1$ его переходной последовательности некоторый символ содержится два раза, а остальные $n - 1$ символов — по одному. Отсюда расстояние Хэмминга между любой парой слов, расположенной на расстоянии $n + 1$ по коду C, равно $n - 1$. □

2.2 Индуктивные конструкции дистанционных кодов Грея

В данном разделе приводятся несколько способов построения дистанционных кодов Грея.

Утверждение 2.2.1. *Пусть $t_0, t_1, \ldots, t_{2^n-1}$ — переходная последовательность $\langle d{,}k\rangle_n$-кода Грея. Если существует такая позиция i, что $t_i = a$ и в каждом из подслов*

$$\begin{aligned} t_{i-k+1}, t_{i-k+2}, \ldots, t_{i-1}, t_i;\\ t_{i-k+2}, t_{i-k+3}, \ldots, t_i, t_{i+1};\\ \ldots\\ t_{i-1}, t_i, \ldots, t_{i+k-3}, t_{i+k-2};\\ t_i, t_{i+1}, \ldots, t_{i+k-2}, t_{i+k-1} \end{aligned}$$

символ a содержится нечетное число раз, то существует $\langle d{,}k\rangle_{n+1}$-код Грея.

Доказательство. Легко убедиться, что последовательность

$$t_0, t_1, \ldots, t_{i-1}, (n+1), t_{i+1}, \ldots, t_{2^n-1}, t_0, t_1, \ldots, t_{i-1}, (n+1), t_{i+1}, \ldots, t_{2^n-1}.$$

является переходной последовательностью $(n+1)$-мерного кода Грея. Покажем, что этот код Грея является $\langle d{,}k\rangle_{n+1}$-кодом. Рассмотрим подслово длины k полученной переходной последовательности: $T = t_j, t_{j+1}, \ldots, t_{j+k-1}$. Если эта последовательность не содержит символа $(n+1)$, то $|supp(Z(T))| = d$, в силу того, что эта последовательность является подсловом переходной последовательности исходного $\langle d{,}k\rangle_n$-кода.

Пусть, в противном случае, это подслово содержит символ $(n+1)$:

$$T' = t_j, t_{j+1}, \ldots, t_{i-1}, (n+1), t_{i+1}, \ldots t_{j+k-1}.$$

Заметим, что для всех $1 \leqslant i \leqslant n+1$, кроме $i = a$ и $i = n+1$ выполнено $Z_i(T) = Z_i(T')$. Для $i = a$ и $i = n+1$ имеем

$$\begin{aligned} Z_a(T) = Z_{n+1}(T') = 1;\\ Z_{n+1}(T) = Z_a(T') = 0. \end{aligned}$$

Отсюда, $|supp(Z(T))| = |supp(Z(T'))| = d$. Значит, построенная переходная последовательность является переходной последовательностью $\langle d{,}k\rangle_{n+1}$-кода. $\square$

Следствие 2.2.1. *Если в каждом подслове длины k переходной последовательности $\langle d,k\rangle_n$-кода некоторый символ содержится нечетное число раз, то существует $\langle d,k\rangle_{n+1}$-код Грея.*

Заметим, что n-мерный двоично-отраженный код Грея удовлетворяет условию следствия 2.2.1 при следующих значениях d и k: он является $\langle 2,2^t\rangle_n$-кодом и $\langle 2,2^n-2^t\rangle_n$-кодом при $1 \leqslant t \leqslant n-1$.

Следствие 2.2.2. *Если в переходной последовательности $\langle d,k\rangle_n$-кода существует вхождение некоторого символа такое, что расстояние до ближайшего вхождения этого же символа в переходной последовательности не меньше k, то существует $\langle d,k\rangle_{n+1}$-код Грея.*

Нетрудно видеть, что следствие 2.2.2 можно применять к 2-композитным $\langle d,k\rangle_n$-кодам, получая $\langle d,k\rangle_{n+1}$-коды (при $1 \leqslant k \leqslant 2^{n-1}$).

Другой класс кодов, к которым можно применять следствие 2.2.2 — это равномерные коды с высоким значением $l_1(C)$. Пусть для кода C выполнено $l_1(C) = d$, тогда C — $\langle d,d\rangle_n$-код по утверждению 2.1.5. В переходной последовательности такого кода одинаковые символы находятся друг от друга на расстоянии по крайней мере d.

Утверждение 2.2.2. *Если существует (2-композитный) $\langle d,k\rangle_n$-код Грея, то существует (2-композитный) $\langle d',2k\rangle_{n+1}$-код Грея, где*

$$d' = \begin{cases} d, & \text{если } k \text{ — четное;} \\ d+1, & \text{если } k \text{ — нечетное.} \end{cases}$$

Доказательство. Пусть $t_0,t_1,t_2,\ldots,t_{2^n-1}$ — переходная последовательность $\langle d,k\rangle_n$-кода Грея. Тогда очевидно, что $t_0,(n+1),t_1,(n+1),t_2,(n+1),\ldots,t_{2^n-1},(n+1)$ — переходная последовательность $\langle d',2k\rangle_{n+1}$-кода Грея. При этом свойство 2-композитности сохраняется. $\square$

Утверждение 2.2.2 предоставляет рекурсивную конструкцию построения дистанционных кодов Грея:

Теорема 2.2.1 ([56]). *Следующие дистанционные коды Грея существуют:*

1. $\langle 2,2^k-2^t\rangle_n$ *при* $t < k \leqslant n$;
2. $\langle d,2^{t+d-1}\rangle_n$ *при четном* d *и* $n \geqslant d+t$;

3. $\langle d, 2^{t+d-1} - 2^t\rangle_n$ *при четном* d *и* $n \geqslant d + t$*;*

4. $\langle d, 2^t d\rangle_n$ *при четном* d *и* $d \leqslant l_1(n - t)$*;*

5. $\langle d + 1, 2^t d\rangle_n$ *при нечетном* d *и* $d \leqslant l_1(n - t)$*.*

Доказательство.

1. k-мерный двоично-отраженный код Грея является $\langle 2{,}2^k - 2^t\rangle_k$-кодом. Заметим при этом, что этот код является 2-композитным. По следствию 2.2.1 существует и $\langle 2{,}2^k - 2^t\rangle_{k+1}$-код (2-композитность кода сохраняется). Теперь по следствию 2.2.2 можем увеличивать размерность кода с сохранением расстояний.
2. По следствию 1.1.1 при четном d существует $(d, 2^{d-1})$-антиподальный 2-композитный код Грея, который в то же время является $\langle d{,}2^{d-1}\rangle_d$-кодом. Применяя к нему t раз утверждение 2.2.2, получаем $\langle d{,}2^{t+d-1}\rangle_{d+t}$-код (по прежнему 2-композитный). Теперь по следствию 2.2.2 можем увеличивать размерность кода с сохранением расстояний.
3. По следствию 2.1.1 при четном d существует $\langle d - 1{,}2^{d-1} - 1\rangle_d$-код, который является 2-композитным. Применяя к нему t раз утверждение 2.2.2, получаем $\langle d{,}2^{t+d-1} - 2^t\rangle_{d+t}$-код (по-прежнему 2-композитный). Теперь по следствию 2.2.2 можем увеличивать размерность кода с сохранением расстояний.
4. Пусть d — четное и $d \leqslant l_1(n - t)$. По утверждению 2.1.5 существует $\langle d{,}d\rangle_{n-t}$-код. Применяя к нему t раз утверждение 2.2.2, получаем $\langle d, 2^t d\rangle_n$-код.
5. Пусть d — нечетное и $d \leqslant l_1(n - t)$. По утверждению 2.1.5 существует $\langle d{,}d\rangle_{n-t}$-код. Применяя к нему t раз утверждение 2.2.2, получаем $\langle d + 1, 2^t d\rangle_n$-код.

$\square$

2.3 Наборы параметров, для которых не существует дистанционных кодов Грея

Как и в случае с другими классами специальных кодов Грея, получение нетривиальных результатов о несуществовании дистанционных кодов Грея с заданными параметрами дистанционности представляет сложную задачу. В данном разделе речь пойдет о наборах параметров дистанционности, при которых не существует дистанционных кодов Грея.

Как следует из утверждения 2.1.2, если параметры дистанционности d и k имеют разную четность, то $\langle d,k\rangle_n$-кодов не существует. Аналогично, не существует $\langle d,k\rangle_n$-кодов, если $d > \min(k, 2^n - k)$. Далее везде полагаем, что d и k одной четности и $d \leqslant \min(k, 2^n - k)$.

Для дистанционных кодов Грея при $d = 1$ имеет место следующие утверждения:

Утверждение 2.3.1. *При* $1 < k < 2^n - 1$ *не существует* $\langle 1,k\rangle_n$*-кода Грея.*

Доказательство. Пусть C — $\langle 1,k\rangle_n$-код Грея. Рассмотрим часть его переходной последовательности:

$$T = t_{j+1}, t_{j+2}, \ldots, t_{j+k-1}.$$

Без ограничения общности можно положить, что $supp(Z(t_jT)) = \{a\}$. Тогда $supp(Z(T)) = \{a,b\}$. В силу того, что C — $\langle 1,k\rangle_n$-код Грея, имеем $t_{j+k} = a$ или $t_{j+k} = b$. При $t_{j+k} = b$ получаем $supp(Z(t_jTt_{j+k})) = \varnothing$, что противоречит тому, что C — код Грея. Значит $t_j = t_{j+k} = a$. Продолжив, получим $t_j = t_{j+k} = t_{j+2k} = t_{j+3k} = \ldots$. Двигаясь по переходной последовательности с шагом k мы целиком замостим ее элементом a, так как k — нечетное. Противоречие, следовательно $\langle 1,k\rangle_n$-кода Грея не существует. $\square$

Этот результат можно интерпретировать в терминах теории графов. Граф-циркулянт $G_n^{1,r_1,\ldots,r_s}$ — это цикл длины n, в котором проведены дополнительные ребра: две вершины соединяются ребром, если расстояние между ними по циклу равно r_i. Заметим, что $\langle 1,k\rangle_n$-коду Грея соответствует гамильтонов цикл в n-мерном гиперкубе $v_0, v_1, \ldots, v_{2^n-1}$, причем вершины v_i и v_{i+k} смежны для любого $0 \leqslant i \leqslant 2^n - 1$. Такой цикл и образует граф $G_{2^n}^{1,k}$. Таким образом, утверждение 2.3.1 дает следующий результат

Следствие 2.3.1. *Для любого* $1 < k < 2^n$ *граф* $G_{2^n}^{1,k}$ *не является подграфом графа* Q_n.

Для некоторых наборов параметров дистанционности со значением d близким к n удаётся получить результаты о несуществовании дистанционных кодов Грея.

Теорема 2.3.1 ([56]). *Для любого четного $n \geqslant 4$ дистанционный $\langle n-1,k \rangle_n$-код Грея существует тогда и только тогда, когда существует $\langle n-1,k' \rangle_n$-код Грея, где k и k' — пара взаимнообратных элементов в мультипликативной группе кольца вычетов по модулю 2^n.*

Доказательство. Пусть $Q_n^{(n-1)}$ — граф на множестве двоичных слов длины n, в котором ребром соединены два слова, расстояние Хэмминга между которыми равно $n-1$. Заметим, что при четном n существует изоморфизм $\varphi : Q_n^{(n-1)} \to Q_n$:

$$\varphi(v) = \begin{cases} v, \text{если вес } v \text{ четный} \\ \overline{v}, \text{иначе.} \end{cases}$$

Пусть $C = v_0,v_1,v_2,\ldots,v_{2^n-1}$ — $\langle n-1,k \rangle_n$-код Грея. Нетрудно видеть, что

$$C^{(n-1)} = v_0, v_k, v_{2k}, \ldots, v_{(2^n-1)k}$$

— это гамильтонов цикл в $Q_n^{(n-1)}$. При этом заметим, что расстояние в этом цикле между вершиной v_0 и v_1 равно k' (так как $k \cdot k' \equiv 1(\mod 2^n)$). Так как φ — изоморфизм, то цикл

$$C' = \varphi(v_0), \varphi(v_k), \varphi(v_{2k}), \ldots, \varphi(v_{(2^n-1)k})$$

является n-мерным кодом Грея. Рассмотрим расстояние Хэмминга между словами $\varphi(v_0)$ и $\varphi(v_1)$. Так как веса слов v_0 и v_1 разной четности, то $d(\varphi(v_0),\varphi(v_1)) = n-1$. Получили, что C' — $\langle n-1,k' \rangle_n$-код Грея. $\square$

Таким образом, при фиксированном n, нечётном k и при $d = n-1$ все наборы параметров $\langle d,k \rangle_n$ разбиваются на пары (кроме таких значений k, что $k^2 \equiv 1 \mod 2^n$), для которых дистанционные коды Грея с этими параметрами либо одновременно существуют, либо одновременно не существуют. Отсюда, используя тривиальные результаты о несуществовании дистанционных кодов Грея, можно получить новые негативные результаты.

Следствие 2.3.2 ([56]). *Пусть для чётного $n \geqslant 6$ существует пара взаимнообратных чисел k_i и $(2i+1)$ в мультипликативной группе кольца вычетов по модулю 2^n, при этом $n-1 \leqslant k_i \leqslant 2^n-(n-1)$, $1 \leqslant i \leqslant \frac{n-4}{2}$. Тогда $\langle n-1,k_i \rangle_n$-кода Грея не существует.*

Доказательство. Так как k_i — обратный к $(2i+1)$ элемент в мультипликативной группе кольца вычетов по модулю 2^n, то $(2i+1)k_i = 2^n m + 1$ для некотрого $m \geqslant 1$. Значит, $k_i \geqslant \frac{2^n m+1}{(2i+1)} \geqslant \frac{2^n m+1}{n-3} \geqslant n-1$ при $n \geqslant 6$.

Пусть теперь $k_i = (2^n - \overline{k_i})$. Тогда $(2i+1)(2^n - \overline{k_i}) = 2^n m + 1$ для некотрого $m \geqslant 1$. Отсюда, $\overline{k_i}(2i+1) \geqslant 2^n - 1$. При $n \geqslant 6$ имеем: $\overline{k_i} \geqslant \frac{2^n-1}{2i+1} \geqslant \frac{2^n-1}{n-3} \geqslant n-1$. □

Так, например, поскольку $43 \cdot 3 \equiv 1 \mod 64$, то по следствию 2.3.2 и предложению 2.1.3 не существует $\langle 5{,}21\rangle_6$-кода Грея. Все наборы параметров при $6 \leqslant n \leqslant 10$, для которых не существует $\langle n-1{,}k\rangle_n$ кода Грея в силу следствия 2.3.2, приведены в таблице 5.

Таблица 5 — Наборы параметров при $6 \leqslant n \leqslant 10$, для которых не существует $\langle d{,}k\rangle_n$-кодов по следствию 2.3.2

n	d	k	2^n	$(2i+1)$	k_i
6	5	21	64	3	43
8	7	85	256	3	171
8	7	51	256	5	205
10	9	341	1024	3	683
10	9	205	1024	5	205
10	9	439	1024	7	439

Применяя идею из теоремы 2.3.1 для значений n произвольной четности и более далеких от n значений d можно получить обобщение следствия 2.3.2:

Теорема 2.3.2 ([56]). *Пусть $k = 2^p(2m+1)$ и k' — обратный к $(2m+1)$ элемент в мультипликативной группе кольца вычетов по модулю 2^{n-p}. Если $\frac{n-2^p}{d} > k'$, то $\langle d{,}k\rangle_n$-код Грея не существует.*

Доказательство. Пусть $C = v_0{,}v_1{,}v_2{,}\ldots{,}v_{2^n-1}$ — $\langle d{,}k\rangle_n$-код Грея. Нетрудно видеть, что

$$v_0, v_k, v_{2k}, \ldots, v_{k\cdot k'}$$

— это простая цепь в $Q_n^{(n-d)}$, причем $v_{k\cdot k'} = v_{2^p}$. Отсюда

$$v_0, \overline{v_k}, v_{2k}, \ldots, \overline{v_{2^p}}$$

— это цепь в $Q_n^{(d)}$. Теперь нетрудно видеть, что $d(v_0,\overline{v_{2^p}}) \leqslant dk'$. С другой стороны, $d(v_0,v_{2^p}) \leqslant 2^p$, а следовательно $d(v_0,\overline{v_{2^p}}) \geqslant n - 2^p$. Получили, что если $n - 2^p > dk'$, то исходный $\langle d,k\rangle_n$-дистанционный код Грея не существует. $\square$

В таблице 6 приведены некоторые наборы значений n, k и d, для которых несуществование $\langle d,k\rangle_n$-кода Грея устанавливается с помощью теоремы 2.3.2.

Таблица 6 — Примеры наборов параметров, для которых не существует $\langle d,k\rangle_n$-кодов по теореме 2.3.2

n	d	k	p	2^{n-p}	$(2m+1)$	k'
9	7	171	0	512	171	3
9	8	172	2	128	43	3
10	8	342	1	512	171	3
11	9	683	0	2048	683	3
11	10	410	1	1024	205	5
11	10	684	2	512	171	3
11	10	820	2	512	205	5
11	10	878	1	1024	439	7

Глава 3. Обобщенная потоковая конструкция

3.1 Вспомогательные определения

Для введения обобщенной потоковой конструкции кодов Грея понадобится ряд вспомогательных понятий, основные из которых — смежные перестановки и разбиения на цепи.

Смежной перестановкой в Q_n называется такая перестановка φ на множестве $V(Q_n)$, что $(v, \varphi(v)) \in E(Q_n)$ для любой вершины v гиперкуба Q_n. Приведём примеры смежных перестановок.

Пример 3.1.1. *Пусть M — совершенное паросочетание в Q_n. Тогда перестановка μ, переводящая вершину в смежную с ней в M является смежной перестановкой вершин Q_n.*

$$\mu(v) = u, \text{ если} (v,u) \in M.$$

Пример 3.1.2. *Пусть $C = v_0, v_1, v_2, \ldots, v_k$ — простой цикл в Q_n. Обозначим через σ_C перестановку вершин $V(C)$, сдвигающую вершины по циклу:*

$$\sigma_C(v_i) = \begin{cases} v_{i+1}, & i \in \{0, 1, 2, \ldots, k\}; \\ v_0, & i = k. \end{cases}$$

Нетрудно видеть, что если C — гамильтонов цикл в Q_n, то σ_C — смежная перестановка в Q_n.

Пример 3.1.3. *Пусть $\mathfrak{C} = \{C_1, C_2, \ldots, C_t\}$ — 2-фактор в Q_n. Тогда перестановка $\sigma_{\mathfrak{C}}$:*

$$\sigma_{\mathfrak{C}}(v) = \begin{cases} \sigma_{C_1}, & v \in V(C_1); \\ \sigma_{C_2}, & v \in V(C_2); \\ \ldots \\ \sigma_{C_i}, & v \in V(C_i); \\ \ldots \\ \sigma_{C_t}, & v \in V(C_t). \end{cases}$$

является смежной перестановкой в Q_n.

Теперь возьмём произвольную вершину v из Q_n и набор произвольных смежных перестановок φ_1, φ_2, …, φ_t в Q_n. Обозначим $v_0 = v$, и $v_i = \varphi_i(v_{i-1})$ для всех $i \in 1, 2, \ldots, t$.

$$\begin{aligned} v_0 &= v, \\ v_1 &= \varphi_1(v_0), \\ v_2 &= \varphi_2(v_1), \\ &\ldots, \\ v_t &= \varphi_t(v_{t-1}). \end{aligned}$$

Очевидно, что последовательность вершин v_0, v_1, v_2, …, v_t является путём в Q_n в силу определения смежной перестановки. Такой путь будем обозначать $P_v(\varphi_1, \varphi_2, \ldots, \varphi_t)$. Полезное свойство путей, построенных таким образом, устанавливает следующее утверждение:

Утверждение 3.1.1. *Пусть $P_v(\varphi_1, \ldots, \varphi_t) = v_0, \ldots, v_l$, а $P_{v'}(\varphi_1, \ldots, \varphi_t) = v'_0$, …, v'_t для двух различных вершин v и v' гиперкуба Q_n. Тогда $v_i \neq v'_i$ для любого $i \in \{0, \ldots, t\}$.*

Доказательство. Пусть i — такое минимальное число, что $v_i = v'_i$. Поскольку $v \neq v'$, то $i > 0$. Значит существуют v_{i-1} и v'_{i-1} такие, что

$$\begin{aligned} v_i &= \varphi_i(v_{i-1}), \\ v'_i &= \varphi_i(v'_{i-1}). \end{aligned}$$

Так как φ_i — перестановка на множестве $V(Q_n)$, то из $v_i = v'_i$ следует, что $v_{i-1} = v'_{i-1}$. Противоречие с минимальностью i. □

Перестановку φ на множестве $V(Q_n)$ будем называть *результирующей* перестановкой для последовательности смежных перестановок φ_1, φ_2, …, φ_t, если

$$\varphi = \varphi_1 \circ \varphi_2 \circ \ldots \varphi_t.$$

Ясно, что в общем случае результирующая перестановка смежной не является.

Пусть P_1, P_2, …, P_t — пути в Q_n. Будем называть $\mathcal{H} = \{P_1, P_2, \ldots, P_t\}$ *набором путей* в Q_n. Множество начальных вершин всех путей, входящих в $\mathcal{H}$, будем обозначать $S(\mathcal{H})$, а множество конечных вершин — $F(\mathcal{H})$. Совокупность всех рёбер, принадлежащих путям из $\mathcal{H}$, будет обозначаться $E(\mathcal{H})$.

В случае, если все пути, входящие в набор $\mathcal{H}$, имеют одинаковую длину, то набор путей $\mathcal{H}$ будем называть *однородным.* В частности, если каждый из путей P_i имеет длину r, то $\mathcal{H}$ будем называть однородным набором путей *длины* r.

Набор путей $\mathcal{H} = \{P_1, P_2, \ldots, P_t\}$ будем называть *разделимым*, если для него выполнено

$$|S(\mathcal{H})| = |F(\mathcal{H})| = t.$$

Разделимый набор путей $\mathcal{H}$ естественным образом определяет взаимо-однозначное отображение $\alpha_{\mathcal{H}} : S(\mathcal{H}) \to F(\mathcal{H})$, переводящее начальную вершину пути в конечную вершину этого же пути.

Заметим, что некоторые разделимые наборы путей можно задать с помощью последовательности смежных перестановок. Пусть $U \subseteq V(Q_n)$ и φ_1, φ_2, $\ldots$, φ_t — последовательность смежных перестановок в Q_n.

$$\mathcal{H}(U, \varphi_1, \varphi_2, \ldots, \varphi_t) = \{P_v(\varphi_1, \varphi_2, \ldots, \varphi_t) \mid v \in U\}.$$

В силу утверждения 3.1.1 построенный таким образом набор путей действительно будет разделимым, а отображение $\alpha_{\mathcal{H}}$ будет являться сужением результирующей перестановки φ_1, φ_2, $\ldots$, φ_t на множество U. Очевидно, такой набор путей будет однородным набором путей длины t.

Далее мы определим операцию соединения для путей и для наборов путей. Пусть $P = v_0, v_1, \ldots, v_t$ и $R = u_0, u_1, \ldots, u_s$, при этом $v_t = u_0$. Тогда соединение $(\circ)$ путей P и R — это путь

$$P \circ R = v_0, v_1, \ldots, v_t, u_1, u_2, \ldots, u_s.$$

Пусть теперь $\mathcal{H} = \{P_1,\ P_2,\ \ldots,\ P_t\}$ и $\mathcal{I} = \{R_1,\ R_2,\ \ldots,\ R_t\}$ — два разделимых набора путей, при этом $F(\mathcal{H}) = S(\mathcal{I})$. Без ограничения общности полагаем, что конец пути P_i совпадает с началом пути R_i (в противном случае пути внутри наборов можно перенумеровать). Тогда для них тоже можно определить операцию соединения:

$$\mathcal{H} \circ \mathcal{I} = \{P_1 \circ R_1, P_2 \circ R_2, \ldots, P_t \circ R_t\}.$$

В случае, если $F(\mathcal{H}) = S(\mathcal{H})$, записью $\mathcal{H}^t$ будем обозначать $\mathcal{H} \circ \cdots \circ \mathcal{H}$ — последовательное соединение t экземпляров набора путей $\mathcal{H}$.

Также для вершин, путей и наборов путей определим операцию *конкатенации с вершиной*. Пусть v — вершина Q_n, а u — вершина Q_k. Записью vu, будем обозначать вершину Q_{n+k}, соответствующую результату конкатенации двоичного слова v длины n и двоичного слова u длины k. Пусть теперь $P = u_0$, u_1, $\ldots$, u_t — путь в Q_k. Тогда результатом конкатенации v и P, будет путь

$$vP = vu_0, vu_1, \ldots, vu_t$$

в Q_{n+k}. Результатом конкатенации v и набора путей $\mathcal{H} = \{P_1, P_2, \ldots, P_t\}$ в Q_k будет являться набор путей

$$v\mathcal{H} = \{vP_1, vP_2, \ldots, vP_t\}$$

в Q_{n+k}.

Теперь можно определить специальный класс наборов путей. Пусть v_1, v_2 — смежные вершины Q_n, и $U \subseteq V(Q_k)$, тогда определим следующий набор путей в Q_{n+k}:

$$\mathcal{E}(v_1, v_2, U) = \{v_1u, v_2u \mid u \in U\}.$$

Таким образом $\mathcal{E}(v_1, v_2, U)$ — это набор путей в Q_{n+k}, каждый путь в котором является путём длины 1 (ребром). Понятно, что $\mathcal{E}(v_1, v_2, U)$ является разделимым набором путей.

Набор путей $\mathcal{H}$ будем называть *разбиением* Q_n *на цепи* (или просто *разбиением*), если каждая вершина из Q_n встречается ровно один раз в списке всех вершин всех путей из $\mathcal{H}$ (то есть покрывается всей совокупностью путей из набора ровно один раз). Очевидно, что любое разбиение является разделимым, а все пути в этом наборе являются простыми цепями.

Нетрудно видеть, что набор путей $\mathcal{H}(U, \varphi)$, где $U \in \{V_0(Q_n), V_1(Q_n)\}$, а φ — смежная перестановка в Q_n, является разбиением Q_n на цепи. В таком разбиении все цепи имеют длину 1: то есть множество рёбер данного разбиения образует совершенное паросочетание в Q_n.

Пример 3.1.4. *Набор путей* $\mathcal{H} = \{P_1, P_2, P_3\}$, *где*

$$P_1 = \mathtt{000}, \mathtt{001}, \mathtt{101}, \mathtt{111};$$
$$P_2 = \mathtt{010}, \mathtt{011};$$
$$P_3 = \mathtt{110}, \mathtt{100},$$

является разбиением Q_3*. Для этого разбиения имеем* $S(\mathcal{H}) = \{\mathsf{000}, \mathsf{010}, \mathsf{110}\}$*, а* $F(\mathcal{H}) = \{\mathsf{111}, \mathsf{011}, \mathsf{100}\}$*.*

Пример 3.1.5. *Любое совершенное паросочетание, в котором для рёбер определена ориентация является разбиением. Так, набор путей* $\mathcal{H} = \{P_1, P_2, P_3, P_4\}$*, где*

$$P_1 = \mathsf{000}, \mathsf{001};$$
$$P_2 = \mathsf{010}, \mathsf{011};$$
$$P_3 = \mathsf{110}, \mathsf{100};$$
$$P_4 = \mathsf{101}, \mathsf{111}$$

является разбиением Q_3*.*

Разделимый набор путей $\mathcal{H}$, для которого выполнено $S(\mathcal{H}) = F(\mathcal{H})$, будем называть *потоком.* В силу определения потока отображение $\alpha_{\mathcal{H}}$ будет являться перестановкой на множестве вершин $S(\mathcal{H})$. Как известно, каждая перестановка может быть разложена в произведение независимых циклов. Эти циклы будем называть *орбитами* данной перестановки.

Рассмотрим поток $\mathcal{H} = \{P_1, P_2, \ldots P_t\}$, где путь P_i имеет длину r_i. Пусть $[P_{i_1}(0), P_{i_2}(0), \ldots, P_{i_s}(0)]$ — одна из орбит перестановки $\alpha_{\mathcal{H}}$. Тогда нетрудно видеть, что путь

$$\begin{gathered} P_{i_1}(0), P_{i_1}(1), \ldots, P_{i_1}(r_{i_1} - 1), \\ P_{i_2}(0), P_{i_2}(1), \ldots, P_{i_2}(r_{i_2} - 1), \\ \ldots, \\ P_{i_s}(0), P_{i_s}(1), \ldots, P_{i_s}(r_{i_s} - 1) \end{gathered}$$

является циклом. Будем говорить, что совокупность $\mathfrak{C}$ таких циклов для каждой из орбит перестановки $\alpha_{\mathcal{H}}$ *порождается* потоком $\mathcal{H}$. Для краткости будем записывать это как:

$$\mathfrak{C} =< \mathcal{H} > .$$

Говоря неформально, речь идёт о наборе циклов, возникающем при "склеивании" всех концов путей потока с соответствующими им началами путей этого потока. Ясно, что эта операция корректна, так как каждая вершина $P_i(0)$ является начальной ровно для одного пути из потока и конечной ровно для одного пути (возможно, другого) из потока.

Разбиение $\mathcal{H}$ будем называть *замкнутым разбиением* Q_n на цепи (или просто замкнутым разбиением), если существует взаимооднозначное отображение $\beta : F(\mathcal{H}) \to S(\mathcal{H})$ такое, что

$$\forall v \in F(\mathcal{H}) \text{ выполнено } (v, \beta(v)) \in E(Q_n).$$

Отображение β в этом случае будем называть замыканием разбиения $\mathcal{H}$. Нетрудно видеть, что отображение $(\alpha_{\mathcal{H}} \circ \beta)$ является перестановкой на множестве $S(\mathcal{H})$.

Пример 3.1.6. *Набор путей* $\mathcal{H} = \{P_1, P_2, P_3\}$, *где*

$$P_1 = \mathtt{111}, \mathtt{101}, \mathtt{001}, \mathtt{000};$$
$$P_2 = \mathtt{100}, \mathtt{110};$$
$$P_3 = \mathtt{010}, \mathtt{011}$$

является замкнутым разбиением Q_3 *с замыканием:*

$$\mathtt{011} \longrightarrow \mathtt{111},$$
$$\mathtt{000} \longrightarrow \mathtt{100},$$
$$\mathtt{110} \longrightarrow \mathtt{010}.$$

Нетрудно видеть, что любое замкнутое разбиение (в совокупности с некоторым его замыканием β) порождает множество циклов, которое является 2-фактором в Q_n. Действительно, пусть $\mathcal{H} = \{P_1, P_2, \ldots P_t\}$ — замкнутое разбиение с замыканием β, где путь P_i имеет длину r_i. Тогда легко видеть, что набор путей

$$\begin{array}{ll}
P_1(0), P_1(1), & \ldots P_1(r_1), \beta(P_1(r_1)) \\
P_2(0), P_2(1), & \ldots P_2(r_2), \beta(P_2(r_2)) \\
\ldots & \\
P_t(0), P_t(1), & \ldots P_t(r_t), \beta(P_t(r_t))
\end{array}$$

является потоком. Для множества циклов $\mathfrak{C}$, порожденного таким образом из замкнутого разбиения $\mathcal{H}$ и замыкания β будем использовать запись

$$\mathfrak{C} =< \mathcal{H}, \beta > .$$

Но в отличие от потока, множество циклов, порождённое таким образом всегда будет являться 2-фактором. Количество циклов в построенном 2-факторе равно числу орбит перестановки $(\alpha_{\mathcal{H}} \circ \beta)$.

Фактически замкнутое разбиение — это не что иное, как набор цепей, возникающий при разрезании ориентированных циклов некоторого 2-фактора Q_n по нескольким рёбрам. При порождении множества циклов из замкнутого разбиения мы совершаем обратную операцию — соединяем вершины рёбрами, по которым был совершен разрез, и получаем 2-фактор.

Пример 3.1.7. *Для замкнутого разбиения $\mathcal{H}$ из примера 3.1.6 мы имеем следующий порождённый 2-фактор.*

$$\mathtt{111}, \mathtt{101}, \mathtt{001}, \mathtt{000}, \mathtt{100}, \mathtt{110}, \mathtt{010}, \mathtt{011}$$

который является гамильтоновым циклом в Q_3 в силу единственности орбиты $(\alpha_{\mathcal{H}} \circ \beta)$.

3.2 Конструкция

Теперь мы приступаем непосредственно к описанию обобщенной потоковой конструкции. Данная конструкция строит 2-фактор в Q_{n+k} из гамильтонова цикла в Q_n и набора разбиений со специальными свойствами в Q_k.

Сначала рассмотрим $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2$, ..., $\mathcal{H}_{t-1}$ — разбиения Q_k с условиями:

$$\begin{gathered} F(\mathcal{H}_i) = S(\mathcal{H}_{i+1}),\ \forall i \in \{0, \ldots, t-2\}, \\ F(\mathcal{H}_{t-1}) = S(\mathcal{H}_0). \end{gathered} \tag{3.1}$$

Последовательность разбиений $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2$, ..., $\mathcal{H}_{t-1}$, удовлетворяющих указанным выше условиям 3.1, будем называть *согласованным набором разбиений (СНР) в Q_k длины t*. Дополнительно, будем говорить, что согласованный набор разбиений является *СНР для цикла C*, если длина этого набора разбиений совпадает с длиной цикла C.

Итак, пусть $C = v_0, v_1, v_2, \ldots, v_{2^n-1}$ — гамильтонов цикл в Q_n, а $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2$, $\ldots$, $\mathcal{H}_{2^n-1}$, — СНР в Q_k для C . Рассмотрим набор путей

$$\begin{aligned}
&v_0\mathcal{H}_0 \circ \mathcal{E}(v_0, v_1, F(\mathcal{H}_0))\circ \\
&\circ\, v_1\mathcal{H}_1 \circ \mathcal{E}(v_1, v_2, F(\mathcal{H}_1))\circ \\
&\ldots \\
&\circ\, v_i\mathcal{H}_i \circ \mathcal{E}(v_i, v_{i+1}, F(\mathcal{H}_i))\circ \\
&\ldots \\
&\circ\, v_{2^n-2}\mathcal{H}_{2^n-2} \circ \mathcal{E}(v_{2^n-2}, v_{2^n-1}, F(\mathcal{H}_{2^n-2}))\circ \\
&\circ\, v_{2^n-1}\mathcal{H}_{2^n-1}.
\end{aligned} \tag{3.2}$$

Поскольку этот набор путей очевидно зависит только от C и $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2$, $\ldots$, $\mathcal{H}_{2^n-1}$, то для краткости представленный выше набор путей будем записывать как $C * (\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{2^n-1})$. Докажем два утверждения относительно $C * (\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{2^n-1})$.

Лемма 3.2.1. *$C*(\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{2^n-1})$ определён корректно и является набором путей в Q_{n+k}.*

Доказательство. Поскольку любое разбиение является разделимым набором путей, то $v_i\mathcal{H}_i$ — тоже разделимый набор путей.

Нетрудно видеть, что множество $\{v_iu \mid u \in F(\mathcal{H}_i)\}$ одновременно является множеством конечных вершин для набора путей $v_i\mathcal{H}_i$ и множеством начальных вершин для набора путей $\mathcal{E}(v_i, v_{i+1}, F(\mathcal{H}_i))$, поэтому все соединения $v_i\mathcal{H}_i \circ \mathcal{E}(v_i, v_{i+1}, F(\mathcal{H}_i))$ корректны.

В силу того, что $F(\mathcal{H}_{i-1}) = S(\mathcal{H}_i)$, множество вершин $\{v_iu \mid u \in F(\mathcal{H}_{i-1})\}$ одновременно является множеством конечных вершин для набора путей $\mathcal{E}(v_{i-1}, v_i, F(\mathcal{H}_i))$ и множеством начальных вершин для набора путей $v_i\mathcal{H}_i$. Отсюда следует, что и все соединения $\mathcal{E}(v_{i-1}, v_i, F(\mathcal{H}_{i-1})) \circ v_i\mathcal{H}_i$ корректны.

Все операции соединения применены корректно, значит, $C * (\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{2^n-1})$ действительно является набором путей в Q_{n+k}. $\square$

Лемма 3.2.2. *Набор путей $C * (\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{2^n-1})$ является замкнутым разбиением в Q_{n+k} с замыканием β_C:*

$$v_{2^n-1}u \longrightarrow v_0u$$

для всех $u \in F(\mathcal{H}_{2^n-1})$..

Доказательство. Заметим, что любая вершина vu ровно один раз содержится ровно в одном наборе цепей из $v_0\mathcal{H}_0$, $v_1\mathcal{H}_1$, $\dots$, $v_{2^n-1}\mathcal{H}_{2^n-1}$. Отсюда следует, что $C * (\mathcal{H}_0, \mathcal{H}_1, \dots, \mathcal{H}_{2^n-1})$ — это разбиение Q_{n+k}. Легко понять, что указанное отображение β_C является замыканием этого разбиения. Значит, $C * (\mathcal{H}_0, \mathcal{H}_1, \dots, \mathcal{H}_{2^n-1})$ — замкнутое разбиение. □

Очевидно для каждого СНР $\mathcal{H}_0$, $\mathcal{H}_1$, $\dots$, $\mathcal{H}_{t-1}$ такое отображение β_C однозначно опреляется циклом C (точнее, его "первой" и "последней" вершиной). Поэтому далее, под β_C мы будем везде иметь ввиду замыкание, построенное аналогичным образом для данного цикла C.

Будем говорить, что 2-фактор

$$< C * (\mathcal{H}_0, \mathcal{H}_1, \dots, \mathcal{H}_{2^n-1}), \beta_C >$$

получен с помощью *обобщённой потоковой конструкции* из гамильтонова цикла C в Q_n и согласованного набора разбиений $\mathcal{H}_0$, $\mathcal{H}_1$, $\dots$, $\mathcal{H}_{2^n-1}$. Количество циклов в получившемся 2-факторе, очевидно, зависит от замкнутого разбиения $C * (\mathcal{H}_0, \mathcal{H}_1, \dots, \mathcal{H}_{2^n-1})$. Имеют место следующие следствия:

Следствие 3.2.1. *Количество циклов в 2-факторе, построенном с помощью обобщённой потоковой конструкции, равно количеству орбит перестановки* $(\alpha_{C*(\mathcal{H}_0,\mathcal{H}_1,\dots,\mathcal{H}_{2^n-1})} \circ \beta_C)$.

Следствие 3.2.2. *Если перестановка* $(\alpha_{C*(\mathcal{H}_0,\mathcal{H}_1,\dots,\mathcal{H}_{2^n-1})} \circ \beta_C)$ *имеет единственную орбиту, то обобщённая потоковая конструкция строит гамильтонов цикл в* Q_{n+k}.

Заметим, что цикл C, используемый в обобщенной потоковой конструкции, не обязан быть гамильтоновым. В случае, если C является простым циклом длины t в Q_n, замкнутое разбиение $C * (\mathcal{H}_0, \mathcal{H}_1, \dots, \mathcal{H}_{t-1})$ будет порождать набор вершинно непересекающихся циклов, покрывающих $2^k t$ вершин в Q_{n+k}.

Поскольку для согласованного набора разбиений $\mathcal{H}_0$, $\mathcal{H}_1$, $\dots$, $\mathcal{H}_{t-1}$ выполнены условия 3.1, то можно рассмотреть набор путей

$$\mathcal{S} = \mathcal{H}_0 \circ \mathcal{H}_1 \circ \dots \circ \mathcal{H}_{t-1},$$

который будет являться потоком. Такой поток будем называть *результирующим потоком СНР* $\mathcal{H}_0$, $\mathcal{H}_1$, $\dots$, $\mathcal{H}_{t-1}$. Легко заметить, что действие перестановки $(\alpha_{C*(\mathcal{H}_0,\mathcal{H}_1,\ldots,\mathcal{H}_{2^n-1})} \circ \beta_C)$ на множестве $S(C * (\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{2^n-1}))$ совпадает с действием перестановки $\alpha_{\mathcal{S}}$ на множестве $S(\mathcal{S})$. Действительно, имеем:

$$\begin{gathered} S(C * (\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{2^n-1})) = S(v_0\mathcal{H}_0), \\ S(\mathcal{S}) = S(\mathcal{H}_0). \end{gathered} \tag{3.3}$$

То есть множества начальных вершин отличаются только конкатенацией вершины v_0. Таким образом, при исследовании количества орбит перестановки $(\alpha_{C*(\mathcal{H}_0,\mathcal{H}_1,\ldots,\mathcal{H}_{2^n-1})} \circ \beta_C)$ можно ограничиться рассмотрением перестановки $\alpha_{\mathcal{S}}$, которая вычисляется как

$$\alpha_{\mathcal{S}} = \alpha_{\mathcal{H}_0} \circ \alpha_{\mathcal{H}_1} \circ \cdots \circ \alpha_{\mathcal{H}_{2^n-1}}.$$

Пример 3.2.1. *Приведём пример построения 2-фактора в Q_5 с помощью обобщенной потоковой конструкции. Пусть $C = \mathtt{00}, \mathtt{01}, \mathtt{11}, \mathtt{10}, \mathtt{00}$ — гамильтонов цикл в Q_2, а $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$ — согласованный набор разбиений в Q_3:*

$$\begin{aligned} \mathcal{H}_0 &= \{(\mathtt{000}, \mathtt{001}, \mathtt{101}, \mathtt{100}), (\mathtt{010}, \mathtt{110}, \mathtt{111}, \mathtt{011})\}, \\ \mathcal{H}_1 &= \{(\mathtt{100}, \mathtt{110}, \mathtt{111}, \mathtt{101}), (\mathtt{011}, \mathtt{010}, \mathtt{000}, \mathtt{001})\}, \\ \mathcal{H}_2 &= \{(\mathtt{101}, \mathtt{111}, \mathtt{110}, \mathtt{100}), (\mathtt{001}, \mathtt{000}, \mathtt{010}, \mathtt{011})\}, \\ \mathcal{H}_3 &= \{(\mathtt{100}, \mathtt{101}, \mathtt{001}, \mathtt{000}), (\mathtt{011}, \mathtt{111}, \mathtt{110}, \mathtt{010})\}. \end{aligned}$$

Для наглядности будем пользоваться таблицей 7. В первом столбце таблицы приведены вершины гамильтонова цикла C. Остальные столбцы содержат цепи из разбиений $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$ следующим образом: в i-ой секции (напротив вершины v_i из C) находятся цепи из $\mathcal{H}_i$; его цепи идут в таком порядке, чтобы цепь из $\mathcal{H}_i$ с начальной вершиной u, располагалось под цепью из $\mathcal{H}_{i-1}$ с конечной вершиной u. С помощью этой таблицы удобно строить 2-фактор, получаемый из обобщенной потоковой конструкции. Выбираем произвольный столбец из Q_3. Двигаясь по этому столбцу вниз, выписываем конкатенацию текущей вершины и соответствующей вершины первого столбца. Так для первого столбца из Q_3 получим:

$$\begin{gathered} \mathtt{00000}, \mathtt{00001}, \mathtt{00101}, \mathtt{00100}, \mathtt{01100}, \mathtt{01110}, \mathtt{01111}, \mathtt{01101}, \\ \mathtt{11101}, \mathtt{11111}, \mathtt{11110}, \mathtt{11100}, \mathtt{10100}, \mathtt{10101}, \mathtt{10001}, \mathtt{10000}, \end{gathered}$$

Дойдя до конца столбца, переходим к началу столбца, первая вершина которого совпадает с последней вершиной текущего и продолжаем те же действия.

Если текущий столбец уже "посещался", то цикл закончен, и мы начинаем строить новый цикл 2-фактора со следующего не "посещённого" столбца. Таким образом для данного примера мы получаем 2-фактор состоящий из двух циклов:

$$C_1 = \mathtt{00000}, \mathtt{00001}, \mathtt{00101}, \mathtt{00100}, \mathtt{01100}, \mathtt{01110}, \mathtt{01111}, \mathtt{01101},$$
$$\mathtt{11101}, \mathtt{11111}, \mathtt{11110}, \mathtt{11100}, \mathtt{10100}, \mathtt{10101}, \mathtt{10001}, \mathtt{10000},$$

$$C_2 = \mathtt{00010}, \mathtt{00110}, \mathtt{00111}, \mathtt{00011}, \mathtt{01011}, \mathtt{01010}, \mathtt{01000}, \mathtt{01001},$$
$$\mathtt{11001}, \mathtt{11000}, \mathtt{11010}, \mathtt{11011}, \mathtt{10011}, \mathtt{10111}, \mathtt{10110}, \mathtt{10010}.$$

Легко заметить, что путям, входящим в обобщенный поток данного согласованного набора разбиений соответствуют столбцы таблицы 7.

Таблица 7 — Обобщение потоковой конструкции (Пример 3.2.1)

Q_2	Q_3	
00	000	010
	001	110
	101	111
	100	011
01	100	011
	110	010
	111	000
	101	001
11	101	001
	111	000
	110	010
	100	011
10	100	011
	101	111
	001	110
	000	010

3.3 Потоковая конструкция

Частным случаем обобщенной потоковой конструкции является классическая потоковая конструкция, впервые использованная в [37]. Приведем описание этой конструкции на языке разбиений и смежных перестановок.

Пусть $\varphi_0, \varphi_1, \ldots, \varphi_{2^n-1}$ — последовательность смежных перестановок в Q_k. Рассмотрим набор разбиений $\mathcal{M}_0, \mathcal{M}_1, \ldots, \mathcal{M}_{2^n-1}$ в Q_k:

$$\mathcal{M}_i = \begin{cases} \mathcal{M}(V_0(Q_k), \varphi_i), & i \text{ — чётное;} \\ \mathcal{M}(V_1(Q_k), \varphi_i), & i \text{ — нечётное.} \end{cases}$$

Утверждение 3.3.1. $\mathcal{M}_0, \mathcal{M}_1, \ldots, \mathcal{M}_{2^n-1}$ *является согласованным набором разбиений длины* 2^n.

Доказательство. Для чётных i имеем: $S(\mathcal{M}_i) = V_0(Q_k)$, $F(\mathcal{M}_i) = V_1(Q_k)$; для нечётных i — $S(\mathcal{M}_i) = V_1(Q_k)$, $F(\mathcal{M}_i) = V_0(Q_k)$. Откуда следует, что $\mathcal{M}_0, \mathcal{M}_1, \ldots, \mathcal{M}_{2^n-1}$ — согласованный набор разбиений. $\square$

Так как рассмотренная последовательность $\mathcal{M}_0, \mathcal{M}_1, \ldots, \mathcal{M}_{2^n-1}$ является согласованным набором разбиений, то её можно использовать для обобщенной потоковой конструкции: для гамильтонова цикла C в Q_n замкнутое разбиение $C * (\mathcal{M}_0, \mathcal{M}_1, \ldots, \mathcal{M}_{2^n-1})$ будет порождать 2-фактор в Q_{n+k}.

Теперь рассмотрим результирующий поток

$$\mathcal{S} = \mathcal{M}_0 \circ \mathcal{M}_1 \circ \cdots \circ \mathcal{M}_{2^n-1}.$$

Данный поток имеет длину 2^n. По этому потоку $\mathcal{S}$ можно однозначно восстановить СНР длины 2^n, для которого $\mathcal{S}$ является результирующим (здесь мы предполагаем, что длины всех путей в разбиениях, составляющих данный СНР, больше 0): действительно, отсюда следует, что каждое из разбиений, входящих в СНР — это совершенное паросочетание в Q_k, и их порядок определится однозначно. В связи с этим для записи $C*(\mathcal{M}_0, \mathcal{M}_1, \ldots, \mathcal{M}_{2^n-1})$ будем использовать сокращенную форму:

$$C * \mathcal{S},$$

где под символом $\mathcal{S}$ имеется ввиду результирующий поток некоторого СНР, построенного указанным выше образом из последовательности смежных перестановок $\varphi_0, \varphi_1, \ldots, \varphi_{2^n-1}$. Поскольку такая последовательность однозначно определяет СНР (а значит и результирующий поток $\mathcal{S}$), то в таком случае мы будем использовать краткую запись $\mathcal{S} = \varphi_0, \varphi_1, \ldots, \varphi_{2^n-1}$, что более формально означает

$$\mathcal{S} = \{P_v(\varphi_0, \varphi_1, \ldots, \varphi_{2^n-1}) \mid v \in V_0(Q_k)\}$$

Очевидно, для такого $\mathcal{S}$ перестановка $\alpha_{\mathcal{S}}$ будет совпадать с сужением результирующей перестановки последовательности $\varphi_0, \varphi_1, \ldots, \varphi_{2^n-1}$ на множество $V_0(Q_k)$.

2-факторы, построенные таким образом из гамильтонова цикла в Q_n и последовательности смежных перестановок в Q_k впервые рассматривались в работе [37]. Способ построения таких 2-факторов получил название *потоковая конструкция*, поскольку одним из компонентов итогового 2-фактора является поток длины 2^n. Таким образом, конструкцию из [37] описывает следующая теорема.

Теорема 3.3.1. *Пусть C — гамильтонов цикл в Q_n, а S — поток в Q_k такой, что*

$$\mathcal{S} = \varphi_0, \varphi_1, \ldots, \varphi_{2^n-1},$$

где $\varphi_0, \varphi_1, \ldots, \varphi_{2^n-1}$ — последовательность смежных перестановок в Q_k с результирующей перестановкой φ. Тогда $< C * \mathcal{S}, \beta_C >$ — 2-фактор в Q_{n+k}, причём количество циклов в этом 2-факторе равно количеству орбит перестановки φ на множестве $V_0(Q_k)$.

В частном случае, когда орбита результирующей перестановки единственна, мы получаем гамильтонов цикл:

Следствие 3.3.1. *Пусть C — гамильтонов цикл в Q_n, а S — поток в Q_k такой, что*

$$\mathcal{S} = \varphi_0, \varphi_1, \ldots, \varphi_{2^n-1},$$

где $\varphi_0, \varphi_1, \ldots, \varphi_{2^n-1}$ — последовательность смежных перестановок в Q_k с результирующей перестановкой φ, имеющей единственную орбиту на $V_0(Q_k)$. Тогда $< C * \mathcal{S}, \beta_C >$ — гамильтонов цикл в Q_{n+k}.

Пример 3.3.1. *Вновь для примера рассмотрим гамильтонов цикл $C = \mathtt{00}, \mathtt{01}, \mathtt{11}, \mathtt{10}, \mathtt{00}$ — в Q_2, и $\mathcal{M}_0$, $\mathcal{M}_1$, $\mathcal{M}_2$, $\mathcal{M}_3$ — согласованный набор разбиений в Q_3:*

$$\mathcal{M}_0 = \{(\mathtt{000}, \mathtt{001}), (\mathtt{011}, \mathtt{010}), (\mathtt{110}, \mathtt{100}), (\mathtt{101}, \mathtt{111})\},$$

$$\mathcal{M}_1 = \{(\mathsf{001}, \mathsf{011}), (\mathsf{010}, \mathsf{000}), (\mathsf{100}, \mathsf{101}), (\mathsf{111}, \mathsf{110})\},$$
$$\mathcal{M}_2 = \{(\mathsf{000}, \mathsf{100}), (\mathsf{011}, \mathsf{001}), (\mathsf{110}, \mathsf{111}), (\mathsf{101}, \mathsf{010})\},$$
$$\mathcal{M}_3 = \{(\mathsf{001}, \mathsf{101}), (\mathsf{010}, \mathsf{110}), (\mathsf{100}, \mathsf{000}), (\mathsf{111}, \mathsf{011})\}.$$

Таблица 8 — Потоковая конструкция (Пример 3.3.1)

Q_2	Q_3			
00	000	011	110	101
	001	010	100	111
01	001	010	100	111
	011	000	101	110
11	011	000	101	110
	001	100	010	111
10	001	100	010	111
	101	000	110	011

Теперь построим таблицу 8, аналогичную таблице из примера 3.2.1. В данном примере потоковая конструкция строит 2-фактор в Q_5 состоящий из двух циклов:

$$C_1 = \mathsf{00000}, \mathsf{00001}, \mathsf{01001}, \mathsf{01011}, \mathsf{11011}, \mathsf{11001}, \mathsf{10001}, \mathsf{10101},$$
$$\mathsf{00101}, \mathsf{00111}, \mathsf{01111}, \mathsf{01110}, \mathsf{11110}, \mathsf{11111}, \mathsf{10111}, \mathsf{10011},$$
$$\mathsf{00011}, \mathsf{00010}, \mathsf{01010}, \mathsf{01000}, \mathsf{11000}, \mathsf{11100}, \mathsf{10100}, \mathsf{10000}.$$

$$C_2 = \mathsf{00110}, \mathsf{00100}, \mathsf{01100}, \mathsf{01101}, \mathsf{11101}, \mathsf{11010}, \mathsf{10010}, \mathsf{10110}.$$

Классическая потоковая конструкция естественным образом вкладывается в новую обобщенную конструкцию как частный случай, в котором все разбиения на цепи в согласованном наборе разбиений являются совершенными паросочетаниями в Q_k.

Глава 4. Локально-равномерные коды Грея

4.1 Постановка задачи и основной результат

Рассмотрим переходную последовательность произвольного n-мерного кода Грея C. $l_2(C)$ — наименьшее число такое, что в каждом подслове длины $l_2(C)$ переходной последовательности кода Грея C содержатся все символы $\{1,2,\ldots,n\}$. Таким образом, фиксированный размер величины $l_2(C)$ запрещает символам в переходной последовательности находиться слишком далеко друг от друга, что способствует его локальной равномерности. Чем меньше число $l_2(C)$ тем более равномерный код Грея мы имеем. Пусть $l_2(n)$ — минимальное значение $l_2(C)$ среди всех n-мерных кодов. Коды, достигающие $l_2(n)$ являются самыми равномерными с точки зрения параметра l_2. А число $l_2(n)$ показывает, насколько равномерными могут быть самые равномерные коды Грея. Заметим, что параметр l_2 можно рассматривать для произвольных замкнутых и незамкнутых маршрутов в Q_n, поскольку каждому маршруту в Q_n можно сопоставить ее переходную последовательность.

Задача оценки параметра $l_2(n)$ является в некотором смысле двойственной к задаче оценки параметра $l_1(n)$. В [37] показано, что справедлива оценка

$$l_1(n) \geqslant n - \lceil 2.001 \log n \rceil,$$

а следовательно, справедливо и

$$\lim_{n\to\infty} \tfrac{l_1(n)}{n} = 1.$$

Везде далее "log" обозначает логарифм по основанию 2. Более раняя конструкция, приведенная в [15], дает результат $\frac{l_1(n)}{n} \geqslant \frac{1}{2}$.

Основным результатом этой главы является

Теорема 4.1.1 ([54]). *Для всех $n \geqslant 3$ справедлива верхняя оценка*

$$l_2(n) \leqslant n + 3\lfloor \log n \rfloor.$$

Отсюда, в силу того, что $l_2(n) \geqslant n$, несложно понять, что

$$\lim_{n\to\infty} \tfrac{l_2(n)}{n} = 1.$$

4.2 Доказательство теоремы 4.1.1

Доказательство теоремы проведем конструктивно, построив для каждого $n \geqslant 3$ n-мерный код Грея со значением параметра l_2 не превосходящим $n + 3\lfloor \log n \rfloor$. Строить код Грея в Q_n будем с помощью классической потоковой конструкции, используя следствие 3.3.1.

Сначала обобщим параметр l_2 для потока $\mathcal{S}$:

$$l_2(\mathcal{S}) = \max_{C \in <\mathcal{S}>} l_2(C).$$

То есть значение параметра l_2 для потока равно максимальному значению $l_2(C)$ среди всех циклов C в 2-факторе, порожденном данным потоком.

Возьмем целые числа a,$b > 0$ такие, что $a + b = n$. Теперь пусть C — гамильтонов в Q_a, а φ_0, φ_1, ..., φ_{2^a-1} — последовательность смежных перестановок в Q_b, с результирующей перестановкой φ, имеет единственную орбиту не множестве $V_0(Q_b)$. Рассмотрим поток $\mathcal{S} = \varphi_0, \varphi_1, \ldots, \varphi_{2^n-1}$. Для C и $\mathcal{S}$ выполнены условия следствия 3.3.1. Значит $< C * \mathcal{S} >$ — гамильтонов цикл. Обозначим его через $C' =< C * \mathcal{S} >$. Для построенного цикла C' имеет место следующая лемма.

Лемма 4.2.1.

$$l_2(C') \leqslant 2\max\{l_2(C), l_2(\mathcal{S})\}.$$

Доказательство. По построению результирующая перестановка φ имеет единственную орбиту на $V_0(Q_b)$. А значит $\alpha_{\mathcal{S}}$ имеет единственную орбиту. Следовательно $< \mathcal{S} >$ — это цикл, длина которого равна

$$2^a \cdot 2^{b-1} = 2^{a+b-1}.$$

Пусть переходная последовательность этого цикла —

$$b_0, b_1, b_2, \ldots, b_{2^{a+b-1}-2}, b_{2^{a+b-1}-1},$$

а переходная последовательность цикла C —

$$a_0, a_1, a_2, \ldots, a_{2^a-2}, a_{2^a-1}.$$

Тогда переходная последовательность итогового цикла C' будет выглядеть так:

$$
\begin{array}{cccccccc}
b_0, & a_0, & b_1, & a_1, & \dots, & b_{2^a-2}, & a_{2^a-2}, & b_{2^a-1}, & a_{2^a-1}, \\
b_{2^a}, & a_0, & b_{2^a+1}, & a_1, & \dots, & b_{2^{2a}-2}, & a_{2^a-2}, & b_{2^{2a}-1}, & a_{2^a-1}, \\
b_{2^{2a}}, & a_0, & b_{2^{2a}+1}, & a_1, & \dots, & b_{2^{3a}-2}, & a_{2^a-2}, & b_{2^{3a}-1}, & a_{2^a-1}, \\
\dots \\
b_{2^{a+b-2}}, & a_0, & b_{2^{a+b-2}+1}, & a_1, & \dots, & b_{2^{a+b-1}-2}, & a_{2^a-2}, & b_{2^{a+b-1}-1}, & a_{2^a-1}.
\end{array}
$$

Теперь очевидно, что значение $l_2(C')$ не может быть больше чем удвоенное $\max\{l_2(C), l_2(\mathcal{S})\}$. □

Построение искомого потока

Сперва построим поток в Q_b, обладающий необходимыми свойствами: длина 2^a и "хорошее" значение $l_2(\mathcal{S})$. Сначала докажем лемму:

Лемма 4.2.2. *Существует поток $\mathcal{S}_b$ в Q_b длины $2b+2$ такой, что $V_0(Q_b)$ — орбита $\alpha_{\mathcal{S}_b}$, и $l_2(\mathcal{S}_b) \leqslant b+2$.*

Доказательство. Пусть C_1 — произвольный гамильтонов цикл в Q_b:

$$v_0, u_0, v_1, u_2, \dots, v_{2^b-2}, u_{2^b-2}, v_{2^b-1}, u_{2^b-1},$$

причем $v_i \in V_0(Q_b)$, а $u_i \in V_1(Q_b)$. Рассмотрим поток $\mathcal{S}_b$:

$$\mathcal{S}_b = \sigma_{C_1}, \sigma_{C_1}, \tau_1, \tau_2, \dots, \tau_{b-1}, \tau_b, \tau_1, \tau_2, \dots, \tau_{b-1}\tau_b.$$

Очевидно, что длина потока $\mathcal{S}_b$ равна $2b+2$. Также легко заметить, $l_2(\mathcal{S}_b) \leqslant b+2$. Осталось показать, что $V_0(Q_b)$ — орбита $\alpha_{\mathcal{S}_b}$. Действие перестановки $\alpha_{\mathcal{S}_b}$ на $v_i \in V(Q_b)$:

$$
\begin{aligned}
\alpha_{\mathcal{S}_b}(v_i) &= \tau_b(\dots\tau_1(\tau_b(\dots\tau_1(\sigma_{C_1}(\sigma_{C_1}(v_i))\dots) \\
&= \tau_b(\dots\tau_1(\tau_b(\dots\tau_1(\sigma_{C_1}(u_i))\dots) \\
&= \tau_b(\dots\tau_1(\tau_b(\dots\tau_1(v_{i+1}))\dots) \\
&= v_{i+1}.
\end{aligned}
$$

Значит, $V_0(Q_b)$ — орбита $\alpha_{\mathcal{S}_b}$. □

Теперь докажем еще одну лемму, с помощью которой мы сможем увеличивать длину полученного потока с сохранением значения параметра l_2 этого потока.

Лемма 4.2.3. *Для любого четного целого* $b' \geqslant 2b + 2 + 2\left\lfloor \frac{b^2}{2} \right\rfloor$, *существует поток* $\mathcal{S}'$ *в* Q_b *длины* b' *такой, что* $V_0(Q_b)$ *— орбита* $\alpha_{\mathcal{S}'}$, *и* $l_2(\mathcal{S}') \leqslant b + 2$.

Доказательство. Рассмотрим поток $\mathcal{S}' = \mathcal{S}_b \circ \mathcal{T}^{2x} \circ \mathcal{R}^{2y} \circ \mathcal{P}^{2z}$, где $\mathcal{S}_a$ — поток, построенный в предыдущей лемме,

$$\mathcal{T} = \tau_1, \tau_2, \ldots, \tau_{b-1}, \tau_b;$$
$$\mathcal{R} = \tau_b, \tau_1, \tau_2, \ldots, \tau_{b-1}, \tau_b;$$
$$\mathcal{P} = \tau_{b-1}, \tau_b, \tau_1, \tau_2, \ldots, \tau_{b-1}, \tau_b.$$

Очевидно, $\mathcal{T}$, $\mathcal{R}$, $\mathcal{P}$ и $\mathcal{S}'$ являются потоками. Пусть $b' = 2b + 2 + 2w$ — длина потока S', где

$$w = xb + y(b+1) + z(b+2).$$

В [40] показано, что такое диофантово уравнение относительно x, y и z будет иметь неотрицательные решения для всех $w \geqslant \left\lfloor \frac{b^2}{2} \right\rfloor$. Значит, для любых целых четных $b' \geqslant 2b + 2 + 2\left\lfloor \frac{b^2}{2} \right\rfloor$ мы сможем построить такой поток $\mathcal{S}'$ длины b'.

Легко заметить, что перестановки $\alpha_{\mathcal{T}^{2x}}, \alpha_{\mathcal{R}^{2y}}$ и $\alpha_{\mathcal{P}^{2z}}$ оставляют вершины на местах при любых значениях x,y,z. Значит, $V_0(Q_b)$ — орбита $\alpha_{\mathcal{S}'}$, так как

$$\alpha_{\mathcal{S}'} = \alpha_{\mathcal{S}_b \mathcal{T}^{2x} \mathcal{R}^{2y} \mathcal{P}^{2z}} = \alpha_{\mathcal{S}_b}.$$

Для того, чтобы показать, что $l_2(\mathcal{S}') \leqslant b + 2$, нужно рассмотреть все значения $l_2(\mathcal{S}_1 \circ \mathcal{S}_2 \circ \mathcal{S}_3)$, где $\mathcal{S}_1$,$\mathcal{S}_2, \mathcal{S}_3 \in \{\mathcal{S}_a, \mathcal{T}, \mathcal{R}, \mathcal{P}\}$. Рассмотрев все случаи, легко убедиться, что каждое из этих значений не превосходит $b + 2$. □

В итоге из лемм 4.2.2 и 4.2.3 имеем

Следствие 4.2.1. *Если*

$$2^a \geqslant 2b + 2 + 2\left\lfloor \frac{b^2}{2} \right\rfloor,$$

то

$$l_2(a + b) \leqslant 2\max\{l_2(a), b + 2\}.$$

Теперь вернемся к доказательству основной теоремы. Его доказательство проведем по индукции. Сначала необходимо определить значение N, для которого любое целое $n \geqslant N$ можно представить в виде суммы двух слагаемых $n = a + b$ таких, что выполняются два условия:

$$2^a \geqslant 2b + 2 + 2\left\lfloor \frac{b^2}{2} \right\rfloor. \tag{4.1}$$

$$n + 3\lfloor\log n\rfloor \geqslant \max\{2a + 6\lfloor\log a\rfloor,\, 2(b+2)\}. \tag{4.2}$$

Поясним каждое из них:

– Мы можем построить поток необходимой длины с требуемым параметром равномерности l_2 (а значит и построить код Грея с использованием потоковой конструкции), если выполнено неравенство 4.1 из следствия 4.2.1.
– Выполнение неравенства 4.2 обеспечивает получение нового кода Грея C' размерности n, для которого справедлива верхняя оценка $l_2(C') \leqslant n + 3\lfloor\log n\rfloor$, если эта оценка справедлива для всех чисел, меньших n (в том числе и a).

4.2.1 Шаг индукции

Рассмотрим множество $M = \{2m + 3\lfloor\log m\rfloor \mid m \in \mathbb{N}\}$. Очевидно, что натуральные числа можно разбить на пять непересекающихся множеств:

1. $M_0 = M$;
2. $M_1 = \{n \in \mathbb{N} \mid (n+1) \in M\}$;
3. $M_2 = \{n \in (\mathbb{N} \setminus M_0) \mid (n+2) \in M\}$;
4. $M_3 = \{n \in (\mathbb{N} \setminus M_1) \mid (n+3) \in M\}$;
5. $M_4 = \{n \in (\mathbb{N} \setminus (M_0 \cup M_2) \mid (n+4) \in M\}$.

Таблица 9 — Разбиение N на множества M_0, M_1, M_2, M_3, M_4

n	4	5	6	7	8	9	10	11	12	13	14
	M_3	M_2	M_1	M_0	M_1	M_0	M_4	M_3	M_2	M_1	M_0

n	15	16	17	18	19	20	21	22	23	24	25
	M_1	M_0	M_1	M_0	M_1	M_0	M_4	M_3	M_2	M_1	M_0

Для каждого из этих множеств приведем разбиение его элементов в сумму слагаемых a и b и определим для каких элементов при данном разбиении выполняются условия 4.1 и 4.2. Подробно рассмотрим множество M_0 — остальные множества рассматриваются аналогично.

Если $n \in M_0$, то $n = 2m+3\lfloor \log m \rfloor$ для некоторого m. Положим $a = m+1$, а $b = m+3\lfloor \log m \rfloor - 1$. При таком разбиении n неравенство 4.1 приобретает вид

$$2^{m+1} \geqslant 2(m+3\lfloor \log m \rfloor - 1) + 2 + 2\left\lfloor \frac{(m+3\lfloor \log m \rfloor - 1)^2}{2} \right\rfloor.$$

Оно выполняется для всех целых $m \geqslant 7$.

Подставляя значения a и b, получаем

$$\begin{aligned} n + 3\lfloor \log n \rfloor &= 2m + 3\lfloor \log m \rfloor + 3\lfloor \log(2m + 3\lfloor \log m \rfloor) \rfloor; \\ 2a + 6\lfloor \log a \rfloor &= 2m + 6\lfloor \log(m+1) \rfloor + 2; \\ 2(b+2) &= 2m + 6\lfloor \log m \rfloor + 2. \end{aligned}$$

Выполнение условия 4.2 эквивалентно выполнению двух неравенств, каждое из которых выполняется для всех $m \geqslant 1$. Результаты для всех множеств представлены в таблице 10.

Таблица 10 — Выполнение неравенств 4.1, 4.2 для множеств M_0, M_1, M_2, M_3, M_4

	a	b	Неравенство 4.1 выполняется для всех m, больших либо равных	Неравенство 4.2 выполняется для всех m, больших либо равных
M_0	$m+1$	$m+3\lfloor \log m \rfloor - 1$	7	1
M_1	m	$m+3\lfloor \log m \rfloor - 1$	9	2
M_2	m	$m+3\lfloor \log m \rfloor - 2$	6	2
M_3	$m-1$	$m+3\lfloor \log m \rfloor - 2$	10	2
M_4	$m-1$	$m+3\lfloor \log m \rfloor - 3$	9	3

Рассмотрев все множества можно заключить, что индукционный переход (построение кодов большей размерности с использованием потоковой конструкции с сохранением верхней оценки) справедлив для всех $n \geqslant 25$, а также для $n = 20$ и для $n = 23$. Имеем:

Для доказательства теоремы осталось доказать базу индукции, то есть доказать, что неравенство $l_2(n) \leqslant n + 3\lfloor \log n \rfloor$ выполняется для всех $n \leqslant 24$, кроме $n = 20$ и $n = 23$.

База индукции

В работе [47] приведены верхние оценки функции $l_2(n)$ для $n \leqslant 7$. Переходные последовательности кодов Грея этих размерностей приведены также в приложении А. Получим оценки для всех остальных значений $n \leqslant 24$, используя торическую конструкцию, приведённую ранее в главе 1:

Лемма 4.2.4. *Если $l_2(n_1), l_2(n_2) \leqslant 2^{n_1-1} - 1$ и $n_1 \leqslant n_2$, тогда $l_2(n_1+n_2) \leqslant 2\max\{l_2(n_1), l_2(n_2)\} + 2$.*

Доказательство. Пусть $X = T(C_1)$ и $Y = T(C_2)$ — переходные последовательности кодов Грея C_1 и C_2 размерности n_1 и n_2 соответственно над непересекающимися алфавитами такие, что $l_2(C_1) = l_2(n_1)$, $l_2(C_2) = l_2(n_2)$, и выполнены условия леммы.

Воспользуемся торической конструкцией из леммы 1.1.1 со следующими параметрами:

$$
\begin{aligned}
&M = 2^{n_1-1} - 1; && \\
&p_i = 1, && i = 1, \dots, 2^{n_1-1} - 1; \\
&q_i = \begin{cases} 2, & \text{при } i \equiv 0,1 (\operatorname{mod} 2^{n_1-1}) \\ 1, & \text{иначе.} \end{cases}, && i = 1, \dots, 2^{n_1-1} - 1,
\end{aligned}
$$

если $l_2(n_1) \leqslant l_2(n_2)$, и

$$
\begin{aligned}
&M = 2^{n_1-1} - 1; && \\
&p_i = \begin{cases} 2, & \text{при } i \equiv 0,1 (\operatorname{mod} 2^{n_1-1}) \\ 1, & \text{иначе.} \end{cases}, && i = 1, \dots, 2^{n_1-1} - 1; \\
&q_i = 1, && i = 1, \dots, 2^{n_1-1} - 1,
\end{aligned}
$$

иначе.

Пусть $l_2(n_1) \leqslant l_2(n_2)$, в противном случае, рассуждения аналогичны. Теперь покажем, что в любом подслове длины $2l_2(n_2) + 2$ слова T, полученного с помощью торической конструкции из X и Y встречаются все буквы.

Так как $l_2(n_2) \leqslant 2^{n_1-1}$, то по построению, в отрезок длины $2l_2(n_2)+2$ полностью могут попасть только два блока длины 2 из q_i. Проезжая окном длины $2l_2(n_2)+2$ по слову T, рассмотрев все случаи, легко убедиться, что в это окно попадают все буквы. □

Лемма 4.2.5. *Если* $l_2(n_1) < l_2(n_2) \leqslant 2^{n_1-1}$, *тогда* $l_2(n_1+n_2) \leqslant 2l_2(n_2)$.

Доказательство проводится аналогично доказательству предыдущей леммы.

С помощью лемм 4.2.4 и 4.2.5 удаётся получить верхние оценки для l_2, представленные в таблице 11. Так как для $n = 23$ можно применить потоковую конструкцию (то есть индукционный переход), то для завершения проверки базы индукции достаточно улучшить верхние оценки для $n = 15,17,21$.

Таблица 11 — Верхние оценки l_2 для $4 \leqslant n \leqslant 24$. Жирным шрифтом выделены значения n, для которых $l_2(n) > n + 3\lfloor \log n \rfloor$

n	4	5	6	7	8	9	10	11	12	13	14
$l_2(n) \leqslant$	6	7	8	9	14	14	16	16	18	18	20

n	**15**	16	**17**	18	19	20	**21**	22	**23**	24
$l_2(n) \leqslant$	**28**	28	**30**	30	32	32	**34**	34	**36**	36

База. Случай $n = 15, n = 21$

Рассмотрим сначала случай $n = 15$. Представим $n = a + b$, где $a = 5$, а $b = 10$. Используя потоковую конструкцию, построим код Грея в Q_{a+b} из кода Грея в Q_a и потока в Q_b.

В качестве требуемого потока в Q_b возьмем поток

$$\mathcal{S} = \sigma_{C_v}, \sigma_{C_v}, \tau_1, \tau_2, \ldots, \tau_b, \tau_1, \tau_2, \ldots, \tau_a, \tau_1, \tau_2, \ldots, \tau_b,$$

где $v = \tilde{1}$. Очевидно, длина потока равна $3b + 2 = 32 = 2^a$, а $l_2(\mathcal{S}) \leqslant b + 2$. Осталось показать, что $V_0(Q_b)$ — орбита $\alpha_{\mathcal{S}}$. Легко видеть, что $V_0(Q_b)$ —

орбита $\sigma_{C_v}\sigma_{C_v}$. Пусть $u_0,u_1,\ldots,u_{2^{b-1}-1}$ — вершины четного веса в Q_b, причем $\sigma_{C_v}\sigma_{C_v}(u_i) = u_{i+1}$ (по циклу). Рассмотрим действие $\alpha_{\mathcal{S}}$ на u_i:

$$\alpha_{\mathcal{S}}(u_i) = \tau_a\tau_{a-1}\ldots\tau_1\sigma_{C_v}\sigma_{C_v}(u_i) = \tau_a\tau_{a-1}\ldots\tau_1(u_{i+1}).$$

Так как C_v — $\tilde{1}$-добавочный код, то $u_{i+1} \oplus (\tilde{1}) = u_{i+2^{b-2}+1}$. Таким образом

$$\alpha_{\mathcal{S}}(u_i) = u_{i+2^{a-2}+1}.$$

Число $2^{b-2}+1$ взаимно просто с числом 2^{b-1}, следовательно $V_0(Q_b)$ — орбита $\alpha_{\mathcal{S}}$.

Стало быть, полученный поток $\mathcal{S}$, удовлетворяет условиям применения потоковой конструкции. В качестве кода Грея в Q_a можно взять код C, для которого $l_2(C) = 7$. Согласно таблице 11, такой код существует.

В результате применения конструкции получим код C'. Для него справедливо

$$l_2(C') \leqslant 2\max\{l_2(a), b+2\} = 2\max\{7, 12\} = 24.$$

Получили новую оценку сверху: $l_2(15) \leqslant 24 \leqslant 15 + 3\lfloor \log 15 \rfloor$.

Аналогичные рассуждения можно провести для $n = 21$. Представим $n = a + b$, где $a = 7$, а $b = 14$. В качестве требуемого потока в Q_a возьмем поток

$$\mathcal{S} = \sigma_{C_v}, \sigma_{C_v}, \overbrace{\overbrace{\tau_1, \tau_2, \ldots, \tau_b}, \overbrace{\tau_1, \tau_2, \ldots, \tau_b}, \ldots, \overbrace{\tau_1, \tau_2, \ldots, \tau_b}, \overbrace{\tau_1, \tau_2, \ldots, \tau_b}}^{9\ \text{раз}},$$

где $v = (\tilde{1})$.

Заметим, что $9b + 2 = 128 = 2^a$. В итоге получаем

$$l_2(C') \leqslant 2\max\{l_2(a), b+2\} = 2\max\{9, 16\} = 32.$$

Получили новую оценку сверху: $l_2(21) \leqslant 32 \leqslant 21 + 3\lfloor \log 21 \rfloor$.

База. Случай $n = 17$

Пусть $n = 17$. Представим $n = a + b$, где $a = 6$, а $b = 11$. Используя потоковую конструкцию, построим код Грея в Q_{a+b} из кода Грея в Q_a и потока в Q_b.

В качестве требуемого потока в Q_b возьмем поток

$$\mathcal{S} = \overbrace{\sigma_{C_v}, \sigma_{C_v}, \tau_1, \tau_2, \ldots, \tau_b}^{13}, \overbrace{\tau_1, \tau_2, \tau_1, \tau_2, \ldots, \tau_b}^{13}, \overbrace{\tau_1, \tau_2, \tau_1, \tau_2, \ldots, \tau_b}^{13},$$

$$\overbrace{\tau_1, \tau_2, \tau_1, \tau_2, \ldots, \tau_b}^{13}, \overbrace{\tau_2, \tau_1, \tau_2, \ldots, \tau_b}^{12}.$$

где $v = (0,1,1,1,1,1,1,1,1,1,1,1)$.

Длина потока равна $4(b+2)+(b+1) = 64 = 2^a$, а $l_2(\mathcal{S}) \leqslant b+2$. Осталось показать, что $V_0(Q_b)$ — орбита $\alpha_\mathcal{S}$. Вновь замечаем, что $V_0(Q_b)$ — орбита $\sigma_{C_v}\sigma_{C_v}$. Пусть $u_0, u_1, \ldots, u_{2^{a-1}-1}$ — вершины четного веса в Q_b, причем $\sigma_{C_v}\sigma_{C_v}(u_i) = u_{i+1}$ (по циклу). Рассмотрим действие $\alpha_\mathcal{S}$ на u_i:

$$\alpha_\mathcal{S}(x_i) = \tau_b\tau_{b-1}\ldots\tau_2\sigma_{G_v}\sigma_{G_v}(u_i) = \tau_b\tau_{b-1}\ldots\tau_2(u_{i+1}).$$

Так как C_v — v-добавочный код, то $u_{i+1} + v = u_{i+2^{b-2}+1}$. Таким образом

$$\alpha_\mathcal{S}(u_i) = u_{i+2^{b-2}+1}.$$

Число $2^{b-2}+1$ взаимнопросто с числом 2^{a-1}, следовательно $V_0(Q_b)$ — орбита $\alpha_\mathcal{S}$.

Стало быть полученный поток S, удовлетворяет условиям применения потоковой конструкции. В качестве кода Грея в Q_b можно взять код C, для которого $l_2(C) = 8$. Согласно таблице 11, такой код существует.

В результате применения конструкции получим код C'. Для него справедливо

$$l_2(C') \leqslant 2\max\{l_2(a), b+2\} = 2\max\{8, 13\} = 26.$$

Получили новую оценку сверху: $l_2(17) \leqslant 26 \leqslant 17 + 3\lfloor\log 17\rfloor$.

Таким образом, база индукции доказана, что и завершает доказательство теоремы.

Глава 5. 2-факторы без близких ребер

5.1 Постановка задачи

Для рёбер гиперкуба введём функцию чётности веса $W'(e)$ и расстояния $d'(e_1, e_2)$. Пусть ребро e образовано словами v_1 и v_2, которые отличаются в i-ой позиции. Тогда $W'(e) = W(v)$, где v — та из вершин v_1 и v_2, которая имеет `0` в i-ой позиции.

Далее также будем пользоваться записью $W'(v_1,v_2)$ для двух вершин, образующих ребро гиперкуба. Для двух рёбер одного направления $e_1 = (v_1, v_2)$ и $e_2 = (u_1, u_2)$ в Q_n определим расстояние между ребрами d':

$$d'(e_1, e_2) = \min\{d(v_1, u_1),\, d(v_1, u_2)\}.$$

Очевидно, что если $W'(e_1) = W'(e_2)$, то $d'(e_1, e_2)$ чётно. Пару рёбер e_1 и e_2 одного направления будем называть *близкими*, если $d'(e_1, e_2) = 1$. Нетрудно видеть, что два ребра являются близкими тогда и только тогда, когда они образуют грань гиперкуба размерности 2.

Утвердительный ответ на вопрос о существовании совершенного паросочетания без близких рёбер даётся в работе [34]. В ней были представлены паросочетания M_1, M_2, M_3, M_4 в Q_4, в которых рёбра одного направления находятся на расстоянии 3 (таблица 12). С помощью построения, представленного в данной статье достаточно легко получать совершенные паросочетания без близких рёбер в Q_n для всех $n \geqslant 4$.

Как продолжение исследования свойств совершенных паросочетаний возникает вопрос, существуют ли два непересекающихся совершенных паросочетания, не имеющих в совокупности близких рёбер. Так как объединение двух непересекающихся совершенных паросочетаний образует 2-фактор, то данная задача может быть сформулирована как задача построения 2-фактора в Q_n без близких рёбер.

В личной беседе Кротов предложил следующий способ построения таких 2-факторов для любого $n \geqslant 8$. Пусть

$$E_1 = \{vM_1 \mid W(v) = 0,\, v \in Q_{n-4}\} \cup \{vM_2 \mid W(v) = 1,\, v \in Q_{n-4}\},$$

$$E_2 = \{M_1 v \mid W(v) = 0,\ v \in Q_{n-4}\} \cup \{M_2 v \mid W(v) = 1,\ v \in Q_{n-4}\}.$$

Тогда нетрудно видеть, что паросочетания E_1 и E_2 не пересекаются, а множество $E_1 \cup E_2$ не содержит близких рёбер. Для любого $n \geqslant 8$ получающийся таким образом 2-фактор состоит из циклов длины 8. Далее в работе мы приведём способ построения 2-фактора, длины циклов в котором увеличиваются с ростом размерности гиперкуба.

Таблица 12 — Паросочетания $\boldsymbol{M_1}$, $\boldsymbol{M_2}$, $\boldsymbol{M_3}$, $\boldsymbol{M_4}$

$$\begin{array}{rlrl}
M_1 = & \{(\mathsf{0000{,}0001}), & M_3 = & \{(\mathsf{0000{,}0100}), \\
& (\mathsf{0011{,}1011}), & & (\mathsf{0011{,}0001}), \\
& (\mathsf{0101{,}0111}), & & (\mathsf{0101{,}1101}), \\
& (\mathsf{0110{,}0010}), & & (\mathsf{0110{,}0111}), \\
& (\mathsf{1001{,}1101}), & & (\mathsf{1001{,}1000}), \\
& (\mathsf{1010{,}1000}), & & (\mathsf{1010{,}0010}), \\
& (\mathsf{1100{,}0100}), & & (\mathsf{1100{,}1110}), \\
& (\mathsf{1111{,}1110})\} & & (\mathsf{1111{,}1011})\} \\
M_2 = & \{(\mathsf{0000{,}0010}), & M_4 = & \{(\mathsf{0000{,}1000}), \\
& (\mathsf{0011{,}0111}), & & (\mathsf{0011{,}0010}), \\
& (\mathsf{0101{,}0100}), & & (\mathsf{0101{,}0001}), \\
& (\mathsf{0110{,}1110}), & & (\mathsf{0110{,}0100}), \\
& (\mathsf{1001{,}0001}), & & (\mathsf{1001{,}1011}), \\
& (\mathsf{1010{,}1011}), & & (\mathsf{1010{,}1110}), \\
& (\mathsf{1100{,}1000}), & & (\mathsf{1100{,}1101}), \\
& (\mathsf{1111{,}1101})\} & & (\mathsf{1111{,}0111})\}
\end{array}$$

В некотором смысле 2-фактор, не содержащий близких рёбер, является оптимальным, так как имеет место следующее утверждение:

Лемма 5.1.1. *В Q_n не существует 2-фактора, в котором любые два ребра одного направления находятся на расстоянии не менее* 3.

Доказательство. Пусть искомый 2-фактор $\mathfrak{F}$ существует.

Любой 2-фактор в Q_n содержит 2^n рёбер, поэтому очевидно, что найдется направление i такое, что рёбер этого направления в 2-факторе не менее $\lceil \frac{2^n}{n} \rceil$.

Обозначим E_i — множество рёбер i-го направления в Q_n. Для каждого ребра e направления i определим множество $B_e = \{e' \in E_i \mid d'(e,e') \leqslant 1\}$. Ясно, что $|B_e| = n$ для любого ребра e. Так как все ребра одного направления в $\mathfrak{F}$ находятся на расстоянии не менее 3, то для двух различных рёбер этого 2-фактора e_1 и e_2 имеем: $B_{e_1} \cap B_{e_2} = \varnothing$. Отсюда

$$\sum_{e \in E(\mathfrak{F}) \cap E_i} |B_e| \geqslant n \left\lceil \frac{2^n}{n} \right\rceil \geqslant 2^n.$$

Но с другой стороны, всего рёбер i-го направления в Q_n — 2^{n-1}. Получаем неравенство:

$$\sum_{e \in E(\mathfrak{F}) \cap E_i} |B_e| \leqslant 2^{n-1}.$$

Противоречие. $\square$

5.2 Построение 2-фактора без близких рёбер

Для того, чтобы 2-фактор без близких рёбер мог быть построен с помощью обобщённой потоковой конструкции, согласованный набор разбиений $\mathcal{H}_0$, $\mathcal{H}_1$, …, $\mathcal{H}_{2^n-1}$ должен удовлетворять ряду условий. Достаточные условия устанавливает следующая теорема:

Теорема 5.2.1. *Пусть $C = v_0, v_1, v_2, \ldots, v_{2^n-1}$ — гамильтонов цикл в Q_n, а $\mathcal{H}_0$, $\mathcal{H}_1$, …, $\mathcal{H}_{2^n-1}$ — согласованный набор разбиений в Q_k для C. Положим, для любых $i,j \in \{0,\ldots,2^a-1\}, i \neq j$ следующие условия выполнены:*

(i) $F(\mathcal{H}_i) \cap F(\mathcal{H}_j) = \varnothing$;

(ii) $\forall u,w \in F(\mathcal{H}_i)$ выполнено $d(u,w) > 1$;

(iii) если $d(v_i, v_j) = 1$, то $E(\mathcal{H}_i) \cap E(\mathcal{H}_j) = \varnothing$;

(iv) $E(\mathcal{H}_i)$ не содержит близких рёбер,

тогда обобщённая потоковая конструкция строит 2-фактор без близких рёбер.

Доказательство. Пусть в получившемся 2-факторе существует пара близких рёбер $e_1 = (v_{i_1}u_1, v_{i_2}u_2)$ и $e_2 = (v_{i_3}u_3, v_{i_4}u_4)$. Возможно четыре случая:

- $d(v_{i_1}, v_{i_2}) = 1$, $d(v_{i_1}, v_{i_3}) = 1$. Следовательно, рёбра имеют вид $e_1 = (v_{i_1}u, v_{i_2}u)$ и $e_2 = (v_{i_3}u, v_{i_4}u)$. Ребро $(v_{i_1}u, v_{i_2}u)$ может принадлежать 2-фактору только если $u \in F(\mathcal{H}_{i_1})$ (или $u \in F(\mathcal{H}_{i_2})$), а ребро $(v_{i_3}u, v_{i_4}u)$, только если $u \in F(\mathcal{H}_{i_3})$ (или $u \in F(\mathcal{H}_{i_4})$). Очевидно, все v_{i_1}, v_{i_2}, v_{i_3}, v_{i_4} попарно различны между собой: в противном случае e_1 и e_2 не могут оказаться близкими. Но вершина u может принадлежать не более чем одному из множеств $F(\mathcal{H}_{i_1})$, $F(\mathcal{H}_{i_2})$, $F(\mathcal{H}_{i_3})$, $F(\mathcal{H}_{i_4})$ по (i). Противоречие.
- $d(v_{i_1}, v_{i_2}) = 1$, $d(u_1, u_3) = 1$. Следовательно, рёбра имеют вид $e_1 = (v_{i_1}u_1, v_{i_2}u_1)$ и $e_2 = (v_{i_1}u_3, v_{i_2}u_3)$. Без ограничения общности положим, что $i_2 = i_1 + 1$. Ребро $(v_{i_1}u_1, v_{i_2}u_1)$ может принадлежать итоговому 2-фактору, только если $u_1 \in F(\mathcal{H}_{i_1})$, а ребро $(v_{i_1}u_3, v_{i_2}u_3)$ — только если $u_3 \in F(\mathcal{H}_{i_1})$. Но по (ii) в $F(\mathcal{H}_{i_1})$ не может оказаться вершин, находящихся на расстоянии 1. Противоречие.
- $d(v_{i_1}, v_{i_3}) = 1$, $d(u_1, u_2) = 1$. Следовательно, рёбра имеют вид $e_1 = (v_{i_1}u_1, v_{i_1}u_2)$ и $e_2 = (v_{i_3}u_1, v_{i_3}u_2)$. Заметим, что ребро (u_1,u_2) принадлежит и $E(\mathcal{H}_{i_1})$, и $E(\mathcal{H}_{i_3})$. Но по (iii) множества $E(\mathcal{H}_{i_1})$ и $E(\mathcal{H}_{i_3})$ не могут содержать одинаковых рёбер, так как $d(v_{i_1}, v_{i_3}) = 1$. Противоречие.
- $d(u_1, u_2) = 1$, $d(u_1, u_3) = 1$. Следовательно, рёбра имеют вид $e_1 = (v_{i_1}u_1, v_{i_1}u_2)$ и $e_2 = (v_{i_1}u_3, v_{i_1}u_4)$. Заметим, что тогда рёбра (u_1,u_2) и (u_3,u_4) являются близкими в Q_k, при этом (u_1,u_2), $(u_3,u_4) \in E(\mathcal{H}_{i_1})$. Но по (iv) множество $E(\mathcal{H}_{i_1})$ не может содержать близких рёбер. Противоречие.

Получили, что при существовании пары близких рёбер в каждом из четырех возможных вариантов получается противоречие с одним из условий. Значит, одновременное выполнение всех четырех условий теоремы является достаточным для того, чтобы построенный 2-фактор не имел близких рёбер. □

Теперь необходимо установить совместность условий, установленных теоремой 5.2.1 — то есть убедиться, что такие согласованные наборы разбиений действительно существуют для гамильтоновых циклов по крайней мере в гиперкубах некоторых размерностей. Далее приведем способ построения таких наборов.

5.3 Построение согласованного набора разбиений

Пусть $C = v_0,\ v_1,\ v_2,\ \ldots,\ v_{2^n-1}$ — гамильтонов цикл в Q_n, при $n \geqslant 2$. Будем строить согласованный набор разбиений для C в Q_k, где $k = 4(n+a)$ при $a \geqslant 0$. Число $n+a$ будем обозначать b.

Любую вершину u из Q_k можно представить в виде $u = q_0q_1q_2\ldots q_{b-1}$ (здесь и далее везде символ q_i обозначают вершину Q_4). Определим отображение f, сопоставляющее каждой вершине u из Q_k вершину из Q_b по следующему правилу:

$$f(u) = W(q_0)\ W(q_1)\ \ldots\ W(q_{b-1}).$$

Теперь имеем $V(Q_k) = \bigsqcup_{w \in V(Q_b)} X_w$, где $X_w = \{u \in Q_k | f(u) = w\}$. Ясно, что мощность множества X_w для любого $w \in V(Q_b)$ равна 2^{3b}.

Будем строить согласованный набор $\mathcal{H}_0,\mathcal{H}_1,\ \ldots,\ \mathcal{H}_{2^n-1}$ разбиений в Q_k для гамильтонова цикла C. Приведём метод построения разбиения $\mathcal{H}_i$ для $i \in \{0,\ldots,2^n-1\}$.

Вершину гиперкуба Q_b вида $v_i\mathtt{00}\ldots\mathtt{00}$ будем обозначать v'_i. Возьмем произвольную гамильтонову цепь R в Q_b, ведущую из вершины в v'_i в вершину v'_{i+1}. Пусть $t_0,\ t_1,\ t_2,\ \ldots,\ t_{2^b-2}$ — переходная последовательность этой гамильтоновой цепи. Для произвольной вершины $u = q_0q_1\ldots q_{b-1}$ из Q_k определим смежную перестановку φ_r^j, где $j \in \{0,\ldots,b-1\}$, а $r \in \{1,2,3,4\}$ следующим образом:

$$\varphi_r^j(u) = q_0q_1\ldots q_{j-1}\ \mu_r(q_j)\ q_{j+1}\ldots q_{b-1}.$$

Для вершины u из $V(Q_k)$ введём обозначение

$$P_u(R) = P_u(\varphi_{r_0}^{t_0}, \varphi_{r_1}^{t_1}, \varphi_{r_2}^{t_2}, \ldots, \varphi_{r_{2^b-3}}^{t_{2^b-3}}, \varphi_{r_{2^b-2}}^{t_{2^b-2}}) = u_0, u_1, u_2, \ldots u_{2^b-2}, u_{2^b-1}.$$

Далее рассмотрим набор путей $\{P_u(R) \mid u \in X_{v'_i}\}$ мощности 2^{3b}.

Лемма 5.3.1. *Построенный набор путей $\{P_u(R) \mid u \in X_{v'_i}\}$ является разбиением Q_k при любых значениях $r_s \in \{1,2,3,4\}$. При этом вершины, стоящие в путях на s-ых местах, образуют множество X_{w_s}, где $R = w_0,\ w_1,\ w_2,\ldots,w_{2^b-1}$.*

Доказательство. Из построения следует, что начальные вершины всех путей из набора образуют множество $X_{v'}$, то есть X_{w_0}.

Нетрудно видеть, что $\varphi_{r_0}^{t_0}(u_s) \in X_{w_{s+1}}$ для любого $u_s \in X_{w_s}$. В силу утверждения 3.1.1 все вершины, стоящие на s-ых местах в путях набора $\{P_u(R) \mid u \in X_{v'_i}\}$, различны. Отсюда, так как мощность всех X_{w_s} одинакова, получаем, что совокупность всех вершин, стоящих на s-ых местах в путях образует в точности множества X_{w_s} для всех $s \in 0, \ldots, 2^b - 1$.

Поскольку множества X_{w_s} разбивают множество $V(Q_k)$, то набор путей $\{P_u(R) \mid u \in X_{v'_i}\}$ является разбиением в независимости от значений r_s. □

Желаемое разбиение $\mathcal{H}_i$ — это разбиение $\{P_u(R) \mid u \in X_{v'_i}\}$ при следующих значениях r_s:

$$r_s = \begin{cases} 1, & \text{если } i \text{ — четное и } W'(f(u_s),f(u_{s+1})) = 0; \\ 2, & \text{если } i \text{ — четное и } W'(f(u_s),f(u_{s+1})) = 1; \\ 3, & \text{если } i \text{ — нечетное и } W'(f(u_s),f(u_{s+1})) = 0; \\ 4, & \text{если } i \text{ — нечетное и } W'(f(u_s),f(u_{s+1})) = 1. \end{cases}$$

r_s определено корректно, поскольку значение $f(u_s)$ не зависит от выбора пути из набора (так как все $u_s \in X_{w_s}$ по предыдущей лемме).

Лемма 5.3.2. *Набор разбиений $\mathcal{H}_0$, $\mathcal{H}_1$, $\ldots$,$\mathcal{H}_{2^a-1}$ является согласованным набором разбиений для цикла C.*

Доказательство. Для каждой из $\mathcal{H}_i$ имеем: $S(\mathcal{H}_i) = X_{v'_i}$, $S(\mathcal{H}_i) = X_{v'_{i+1}}$. Отсюда следует, что указанный набор разбиений является согласованным. □

Теорема 5.3.1. *Согласованный набор разбиений $\mathcal{H}_0$,$\mathcal{H}_1$, $\ldots$, $\mathcal{H}_{2^a-1}$ удовлетворяет всем условиям из теоремы 5.2.1.*

Доказательство. Последовательно докажем, что полученный согласованный набор разбиений удовлетворяет каждому из условий теоремы 5.2.1.

1. Так как $X_{v'_i} \cap X_{v'_j} = \varnothing$ для разных $v_i, v_j \in V(Q_n)$, то и $F(\mathcal{H}_i) \cap F(\mathcal{H}_j) = \varnothing$ выполнено;
2. Очевидно что внутри одного множества $X_{v'}$ могут находиться только вершины одной чётности. Отсюда расстояние Хэмминга между любыми двумя вершинами из $F(\mathcal{H}_i)$ не меньше 2;
3. Пусть v_i и v_j такие, что $d(v_i, v_j) = 1$. Значит i и j разной чётности. Предположим, что существуют совпадающие рёбра $e_1 = (u_{l_1}, \varphi_{r_{l_1}}^{t_{l_1}}(u_1)) \in$

$E(\mathcal{H}_i)$ и $e_2 = (u_{l_2}, \varphi^{t_{l_2}}_{r_{l_2}}(u_2)) \in E(\mathcal{H}_j)$. В этом случае необходимо, чтобы $r_{l_1} = r_{l_2}$, $t_{l_1} = t_{l_2}$. Но это невозможно в силу определения r_i, так как i и j разной чётности. Противоречие;

4. Предположим, что $e_1 = (u_{l_1}, \varphi^{t_{l_1}}_{r_{l_1}}(u_1)))$ и $e_2 = (u_{l_2}, \varphi^{t_{l_2}}_{r_{l_2}}(u_2))$ — пара близких рёбер из $E(\mathcal{H}_i)$. Чтобы эти рёбра оказались близкими нужно, чтобы $r_{l_1} = r_{l_2}$, $t_{l_1} = t_{l_2}$. Но для близких рёбер e_1 и e_2 имеем $W'(e_1) \neq W'(e_2)$. Значит $r_{l_1} \neq r_{l_2}$ Противоречие.

□

Таким образом для любого гамильтонова цикла в Q_n мы можем построить согласованный набор разбиений в $Q_{4(n+a)}$, удовлетворяющий условиям теоремы 5.2.1. Это позволяет построить 2-фактор без близких рёбер в Q_{5n+4a} с помощью обобщённой потоковой конструкции.

Минимальной размерностью, для которой удаётся построить 2-фактор без близких рёбер с помощью обобщенной потоковой конструкции, является размерность $N = 10$. В этом случае параметры принимают следующие значения: $n = 2$, $k = 8$, $b = 2$, $a = 0$. Приведём результат этого построения.

Пусть $C =$ `00,10,11,01` — гамильтонов цикл в Q_2. Согласованный набор разбиений $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$ для C будет задаваться четырьмя гамильтоновыми цепями:

- R_0 — гамильтонова цепь в Q_2 из `00` в `10`. Её переходная последовательность — 1,0,1.
- R_1 — гамильтонова цепь в Q_2 из `10` в `11`. Её переходная последовательность — 0,1,0.
- R_2 — гамильтонова цепь в Q_2 из `11` в `01`. Её переходная последовательность — 1,0,1.
- R_3 — гамильтонова цепь в Q_2 из `01` в `00`. Её переходная последовательность — 0,1,0.

Для примера рассмотрим пути из $\mathcal{H}_0$, начальные вершины которых начинаются на `0000`. Всего таких путей 8, все они имеют длину 4 (см. таблицу 13). На первом шаге вторая четверка позиций вершины из каждого пути меняется в соответствии с паросочетанием M_1. На втором шаге первая четверка позиций вершины из каждого пути меняется в соответствии с паросочетанием M_1. На третьем шаге вторая четверка позиций вершины из каждого пути меняется в соответствии с паросочетанием M_2.

Таблица 13 — Пути из разбиения $\mathcal{H}_0$

Q_8			
00000000	00001100	00000110	00000011
00000001	00000100	00000010	00001011
00010001	00010100	00010010	00011011
00011001	00010101	00010000	00011010

Q_8			
00001010	00001001	00000101	00001111
00001000	00001101	00000111	00001110
00011000	00011101	00010111	00011110
00011100	00011111	00010011	00010110

5.4 Анализ полученного решения

Количество циклов

По следствию 3.2.1 количество циклов в 2-факторе, полученном с помощью обобщённой потоковой конструкции равно количеству орбит перестановки $\alpha_{\mathcal{H}'}$, являющейся суперпозицией перестановок $\alpha_{\mathcal{H}_0}$, $\alpha_{\mathcal{H}_1}$, $\ldots$, $\alpha_{\mathcal{H}_{2^n-1}}$.

Рассмотрим действие перестановки $\alpha_{\mathcal{H}'}$ на вершину $u = q_0, q_1, q_2, \ldots, q_{b-1}$ гиперкуба Q_{4b}. Нетрудно видеть, что

$$\alpha_{\mathcal{H}'}(u) = \gamma_0(q_0), \gamma_1(q_1), \gamma_2(q_2), \ldots, \gamma_{n+a-1}(q_{b-1}),$$

где каждое из γ_i — это суперпозиция чётного числа перестановок из μ_1, μ_2, μ_3, μ_4, являющаяся перестановкой всех вершин одной чётности из $V(Q_4)$. Отсюда получаем, что длина орбиты $\alpha_{\mathcal{H}'}$ равна наименьшему общему кратному длины орбит γ_i. Из симметричности перестановок μ_i следует, что каждая из γ_i имеет орбиты одинаковой длины. Значит, возможная длина орбит γ_i — 1, 2, 4, 8. Таким образом, минимально возможная длина циклов в полученно 2-факторе равна $2^b \cdot 2^n = 2^{2n+a}$, а максимальная — $8 \cdot 2^b \cdot 2^n = 2^{2n+a+3}$.

Покрываемые размерности

Применяя указанный выше способ построения, можно построить 2-фактор с желаемым свойством в Q_{5n+4a}, где $n \geqslant 2$, а $a \geqslant 0$. Значит, минимальная размерность гиперкуба N, для которой можно применить построение — $N = 10$. В Q_{10} удаётся построить 2-фактор, в котором все циклы имеют длину 64.

Теперь необходимо узнать, начиная с какого N, любое число может быть представлено в виде $5n + 4a$, где $n \geqslant 2$, а $a \geqslant 0$. Для этого воспользуемся решением задачи Фробениуса для двух чисел. Напомним, что задача Фробениуса состоит в нахождении максимального целого числа N такого, что уравнение

$$N = ax + by$$

не имеет решения в целых неотрицательных числах относительно x и y при фиксированных значениях a и b. Решение этой задачи было найдено ещё Сильвестром в 1882 году: $N = ab - a - b$.

Отсюда легко получаем, что $N = 21$ — самое большое целое число, которое не может быть представлено в виде $5n + 4a$, где $n \geqslant 2$, а $a \geqslant 0$. Следовательно, приведенная конструкция строит 2-факторы в гиперкубах всех размерностей $N \geqslant 22$ при подходящих значениях n и a. Очевидно, что для всех целых неотрицательных n и a мы имеем:

$$2n + a \geqslant \frac{1}{4}(5n + 4a) = \frac{N}{4}.$$

Следовательно, для всех $N \geqslant 22$ с помощью представленной выше конструкции можно строить 2-факторы, длины циклов в которых не меньше, чем $2^{N/4}$.

Таблица 14 демонстрирует, какие значения размерности N покрываются конструкцией при соответствующих n и a в интервале от 10 до 22 (жирным выделены непокрытые значения).

Таблица 14 — Покрываемые размерности

N	10	**11**	**12**	**13**	14	15	**16**	**17**	18	19	20	**21**	22
n	2				2	3			2	3	4		2
a	0				1	0			2	1	0		3

Заметим, что построенный таким образом 2-фактор без близких рёбер в Q_N может быть "расширен"до 2-фактора без близких рёбер в Q_{N+1}. Пусть C — гамильтонов цикл в Q_n, а $\mathcal{H}_0$, $\mathcal{H}_1$, ..., $\mathcal{H}_{2^n-1}$ — согласованный набор разбиений в Q_k для C, построенный способом, приведённым в предыдущем разделе.

Пусть $\mathfrak{F}_1$ — 2-фактор в Q_{n+k}, построенный с помощью обобщённой потоковой конструкции из C и согласованного набора разбиений $\mathcal{H}_0$, $\mathcal{H}_1$, ..., $\mathcal{H}_{2^n-1}$. А $\mathfrak{F}_2$ — 2-фактор в Q_{n+k}, построенный с помощью обобщённой потоковой конструкции из C и согласованного набора разбиений $\mathcal{H}_1$, $\mathcal{H}_2$, ..., $\mathcal{H}_{2^n-1}$, $\mathcal{H}_0$. Ясно, что $\mathfrak{F}_2$ также не содержит близких рёбер.

Лемма 5.4.1. *Два множества рёбер $\mathfrak{F}_1$ и $\mathfrak{F}_2$ не пересекаются.*

Доказательство. Пусть существует ребро $e = (v_{i_1}u_{j_1}, v_{i_2}u_{j_2})$, принадлежащее обоим 2-факторам.

Если $i_1 = i_2$, то это означает, что $(u_{j_1},u_{j_2}) \in E(\mathcal{H}_{i_1})$ из $\mathfrak{F}_1$. Также $(u_{j_1},u_{j_2}) \in E(\mathcal{H}_{i_1+1})$ из $\mathfrak{F}_2$. Но согласованный набор разбиений $\mathcal{H}_0$, $\mathcal{H}_1$, ..., $\mathcal{H}_{2^n-1}$ удовлетворяет условию (iii) теоремы 5.3.1. Противоречие.

Если $u_{j_1} = u_{j_2}$, то v_{i_1} и v_{i_2} — две соседние вершины в C. Без ограничения общности полагаем $i_2 = i_1+1$. Тогда $u_{j_1} \in F(\mathcal{H}_{i_1})$ из $\mathfrak{F}_1$. Также $u_{j_1} \in F(\mathcal{H}_{i_1+1})$ из $\mathfrak{F}_2$. Но согласованный набор разбиений $\mathcal{H}_0$,$\mathcal{H}_1$,...,$\mathcal{H}_{2^n-1}$ удовлетворяет условию (i) теоремы 5.3.1. Противоречие. □

Поместив теперь каждый из этих 2-факторов в подкуб Q_{n+k+1} размерности $n+k$ получим 2-фактор в Q_{n+k+1}. Этот 2-фактор не будет содержать близких рёбер по лемме 5.4.1 и в силу того, что каждый из $\mathfrak{F}_1$ и $\mathfrak{F}_2$ не содержит близких рёбер. Очевидно, такой подход можно обобщить для построения 2-факторов при увеличении размерности на произвольное число, размещая в "чётных" подкубах $\mathfrak{F}_1$, а в "нечётных" — $\mathfrak{F}_2$.

Заметим, что для всех $10 \leqslant N \leqslant 21$ выполняется:

$$2^{N/4} \leqslant 64.$$

Значит, "расширяя" указанным выше способом 2-фактор без близких рёбер в Q_{10} в к кубах размерности $10 \leqslant N \leqslant 21$, можно будет получить 2-факторы без близких рёбер с длинами циклов не менее $2^{N/4}$. Следовательно, справедлива следующая теорема:

Теорема 5.4.1 ([60]). *Для любого $N \geqslant 10$ в Q_N существует 2-фактор без близких рёбер с длинами циклов не менее $2^{N/4}$.*

Заключение

Основные результаты работы заключаются в следующем.

1. Найдена конструктивная верхняя оценка $n + 3\log n$ для параметра локальной равномерности кодов Грея.
2. Приведено несколько способов построения дистанционных кодов Грея. Для двух нетривиальных серий параметров доказано несуществование кодов Грея.
3. Предложена новая конструкция 2-факторов и гамильтоновых циклов в булевом кубе.
4. Доказано, что в булевых кубах размерностей $n \geqslant 10$ существуют 2-факторы без близких рёбер с длинами циклов не меньше $2^{n/4}$.

Список литературы

1. *Gray F.* Pulse code communications : patent no. 2632058 US. — 1953.
2. *Gilbert E. N.* Gray codes and paths on the n-cube // The bell system technical journal. — 1958. — Vol. 37, no. 3. — P. 815—826.
3. *Kautz W. H.* Unit-Distance Error-Checking Codes // IRE Transactions on Electronic Computers. — 1958. — Vol. EC—7, no. 2. — P. 179—180.
4. *Журавлев Ю. А.* Алгоритмы упрощения дизъюнктивных нормальных форм конечного индекса // Докл. АН СССР, — 1961. — т. 139, № 6. — с. 1329—1331.
5. *Mills W. H.* Some Complete Cycles on the n-Cube // Proceedings of the American Mathematical Society. — 1963. — Vol. 14, no. 4. — P. 640—643.
6. *Васильев Ю. Л.* О длине цикла в n-мерном единичном кубе // Докл. АН СССР, — 1963. — т. 148, № 4. — с. 753—756.
7. *Davies D. W.* Longest "separated" paths and loops in an N-cube // IEE Trans. Electron. Comput. — 1965. — Vol. EC—14. — P. 261.
8. *Douglas R. J.* Upper bounds on the length of circuits of even spread in the d-cube // Journal of Combinatorial Theory. — 1969. — Vol. 7. — P. 206—214.
9. *Harary F.* Graph theory. — Addison-Wesley Pub. Co., 1969.
10. *Евдокимов А. А.* О максимальной длине цепи в единичном n-мерном кубе // Математические заметки. — 1969. — т. 4, № 3. — с. 309—319.
11. *Klee V. L.* What is the maximum length of the n-dimensional snake? // Am. Math. Mon. — 1970. — Vol. 77. — P. 63—65.
12. *Gardner M.* The curious properties of the Gray code and how it can be used to solve puzzles // Scientific American. Mathematical Games. — 1972. — Vol. 227, no. 2. — P. 106.
13. *Reingold E. M.*, *Nievergelt J.*, *Deo N.* Combinatorial Algorithms: Theory and Practice. — Prentice Hall College Div, 1977.
14. *Vickers V. E.*, *Silverman J.* A Technique for Generating Specialized Gray Codes // IEEE Trans. Comput. — 1980. — Vol. 29, no. 4. — P. 329—331.

15. *Евдокимов А. А.* О нумерации подмножеств конечного множества // Методы дискретного анализа в решении комбинаторных задач. — 1980. — т. 34. — с. 8—26.

16. *Chen C. C.*, *Quimpo N. F.* On strongly hamiltonian abelian group graphs // Combinatorial Mathematics VIII. — 1981. — P. 23—34.

17. *Ludman J.* Gray Code Generation for MPSK Signals // Communications, IEEE Transactions on. — 1981. — Vol. 29. — P. 1519—1522.

18. *Robinson J. P.*, *Cohn M.* Counting sequences // IEEE Trans. Computers. — 1981. — Vol. C—30. — P. 17—23.

19. Architecture of a Hypercube Supercomputer. / J. P. Hayes [et al.] // Proceedings of the International Conference on Parallel Processing. — 1986. — P. 653—660.

20. *Faloutsos C.* Multiattribute Hashing Using Gray Codes. — 1986.

21. *Solovyeva F. I.* An upper bound for the length of a cycle in an n-dimensional unit cube // Diskretnyi Analiz. — 1987. — Vol. 45. — P. 71—76.

22. *Goddyn L.*, *Lawrence G. M.*, *Nemeth E.* Gray codes with optimized run lengths // Utilitas Mathematica. — 1988. — Vol. 34. — P. 179—192.

23. *Harary F.*, *Hayes J. P.*, *Wu H.-J.* A survey of the theory of hypercube graphs // Computers & Mathematics with Applications. — 1988. — Vol. 15. — P. 277—289.

24. *Wojciechowski J.* A new lower bound for Snake-in-the-Box Codes // Combinatorica. — 1989. — Vol. 9. — P. 91—99.

25. *Adam A.* Truth Functions and the Problem of their Realization by Two-Terminal Graphs // Discrete Mathematics. — 1990. — Vol. 85. — P. 329—331.

26. *Ramras M.* A new method of generating Hamiltonian cycle on the n-cube // Discrete Mathematics. — 1990. — Vol. 85. — P. 329—331.

27. *Abbott H.*, *Kachalski M.* On the construction of snake-in-the-box codes // Utilitas Math. — 1991. — Vol. 40. — P. 97—116.

28. *Wagner D. J.*, *West J.* Constructions of uniform Gray codes // Congressus Numerantium. — 1991. — Vol. 80. — P. 217—223.

29. *Zanten A. van.* Minimal-Change Order and Separability in Linear Codes // Information Theory, IEEE Transactions on. — 1993. — Vol. 39. — P. 1988—1989.

30. *Bhat G. S.*, *Savage C. D.* Balanced Gray Codes // Electronic Journal of Combinatorics. — 1996. — Vol. 3.

31. *Пережогин А. Л.* О локально изометрическом кодировании натуральных чисел // Дискретный анализ и исследование операций. — 1996. — т. 3, № 4. — с. 69—76.

32. *Savage C.* A survey of combinatorial Gray codes // SIAM Rev. — 1997. — Vol. 39, no. 4. — P. 605—629.

33. *Zemor G.* An upper bound on the size of the snake-in-the-box problem // Combinatorica. — 1997. — Vol. 17, no. 2. — P. 287—298.

34. *Кротов Д. С.* Индуктивные конструкции совершенных троичных равновесных кодов с расстоянием 3 // Пробл. передачи информ. — 2001. — т. 37, № 1. — с. 3—11.

35. *Пережогин А. Л.*, *Потапов В. Н.* О числе гамильтоновых циклов в булевом кубе // Дискретный анализ и исследование операций. — 2001. — т. 8, № 2. — с. 52—62.

36. *Killian C.*, *Savage C.* Antipodal Gray Codes // Discrete Mathematics. — 2002. — Vol. 281. — P. 221—236.

37. *Goddyn L.*, *Gvozdjak P.* Binary Gray codes with long bit runs // The Electron. J. Comb. — 2003. — Vol. 10. — R27.

38. *He M. X.*, *Petoukhov S. V.*, *Ricci P. E.* Genetic code, hamming distance and stochastic matrices // Bulletin of Mathematical Biology. — 2004. — Vol. 66, no. 5. — P. 1405—1421.

39. On the optimality of the binary reflected Gray code / E. Agrell [et al.] // IEEE Transactions on Information Theory. — 2004. — Vol. 50. — P. 3170—3182.

40. *Aguilo F.*, *Mirallas A.* On the Frobenius' Problem of three numbers // Proc. 2005 Eur. Conf. Comb., Graph Theory Appl. Nancy: DMTCS. — 2005. — P. 317—322.

41. *Chang G. J.*, *Eu S.-P.*, *C.-H. Y.* On the (n,t)-antipodal Gray codes // Theoretical Computer Science. — 2007. — Vol. 374, no. 1—3. — P. 82—90.

42. *Dejter I.*, *Delgado A. A.* Classes of Hamiltonian Circuits in the 5-cube // Journal of Combinatorial Mathematics and Combinatorial Computing. — 2007. — Vol. 61. — P. 87—95.

43. *Chebiryak Y.*, *Kroening D.* Towards a Classification of Hamiltonian Cycles in 6-Cube // Journal of Satisfiability, Boolean Modelling and Computation. — 2008. — Vol. 4, no. 1. — P. 57—74.

44. *Zanten A. J. van*, *Haryanto L.* Sets of disjoint snakes based on Reed-Muller code and covering hypercube. — 2008. — URL: https://link.springer.com/article/10.1007%2Fs10623-008-9202-x.

45. *Feder T.*, *Subi C.* Nearly Tight Bounds on the Number of Hamiltonian Circuits of the Hypercube and Generalizations // Inform. Process. Lett. — 2009. — Vol. 109, no. 5. — P. 267—272.

46. *Knuth D. E.* The Art of Computer Programming, Volume 4, Fascicle 1: Bitwise Tricks & Techniques; Binary Decision Diagrams. — 12th. — Addison-Wesley Professional, 2009.

47. *Годовых О. П.* Равномерные коды Грея : Выпускная квалификационная работа бакалавра / Годовых О. П. — Новосибирский Государственный Университет, 2012.

48. *Потапов В. Н.* Построение гамильтоновых циклов с заданным спектром направлений рёбер в булевом n-мерном кубе // Дискретный анализ и исследование операций. — 2012. — т. 19, № 2. — с. 75—83.

49. *Haanpaa H.*, *Östergard P. R. J.* Counting Hamiltonian cycles in bipartite graphs // Math. Comp. — 2014. — Vol. 23. — P. 979—995.

50. *Östergård P. R. J.*, *Pettersson V.* Exhaustive Search for Snake-in-the-Box Codes // Graphs and Combinatorics. — 2014. — Vol. 31.

51. *Östergård P. R. J.*, *Pettersson V.* On the maximum length of coil-in-the-box codes in dimension 8 // Discrete Applied Mathematics. — 2014. — Vol. 179. — P. 193—200.

52. *Быков И. С.* О равномерных кодах Грея // 53-я Международная Студенческая Конференция. Материалы. НГУ, Новосибирск. — 2015. — с. 102.

53. *Быков И. С.* О равномерных кодах Грея // Труды 9-ой международной конференции "Дискретные модели в теории управляющих систем". МГУ, Москва. — 2015. — с. 42—44.

54. *Быков И. С.* О локально равномерных кодах Грея // Дискретный анализ и исследование операций. — 2016. — т. 23, № 1. — с. 51—64.

55. *Быков И. С.*, *Пережогин А. Л.* О дистанционных кодах Грея // XII-й Международный семинар "Дискретная математика и её приложения". Материалы. МГУ, Москва. — 2016. — с. 281—283.

56. *Быков И. С.*, *Пережогин А. Л.* О дистанционных кодах Грея // Дискретный анализ и исследование операций. — 2017. — т. 24, № 2. — с. 5—17.

57. *Gregor P.*, *Mutze T.*, *Nummenpalo J.* A short proof of middle levels theorem. — 2018. — URL: https://discreteanalysisjournal.com/article/3659-a-short-proof-of-the-middle-levels-theorem.

58. *Быков И. С.* Об одной задаче поиска 2-фактора в гиперкубе // Труды X международной конференции "Дискретные модели в теории управляющих систем". МГУ, Москва. — 2018. — с. 62—64.

59. *Fink J.* Matchings Extend into 2-Factors in Hypercubes // Combinatorica. — 2019. — Vol. 39, no. 1. — P. 77—84.

60. *Быков И. С.* 2-факторы без близких рёбер в гиперкубе // Дискретный анализ и исследование операций. — 2019. — т. 26, № 3. — с. 5—25.

Приложение А

Локально-равномерные коды Грея малых размерностей

В данном приложении приводятся переходные последовательности кодов Грея малых размерностей, достигающих наилучших известных значений параметров равномерности l_2, для всех размерностей $n \leqslant 7$.

n	$T(C)$
1	1,1
2	1,2,1,2
3	1,2,1,3,1,2,1,3
4	1,2,1,3,1,4,3,2,3,4,1,4,2,3,2,4
5	1,2,1,3,4,5,4,3,2,1,2,3,5,4,5,3, 1,2,1,3,4,5,4,3,2,1,2,3,5,4,5,3
6	1,2,1,3,1,4,5,6,1,2,1,3,4,5,4,6, 2,1,2,3,2,5,4,6,2,1,2,3,5,4,5,6, 1,2,1,3,1,4,5,6,1,2,1,3,4,5,4,6, 2,1,2,3,2,5,4,6,2,1,2,3,5,4,5,6
7	1,2,3,4,5,6,7,3,5,1,2,6,4,5,7,3, 2,1,6,5,4,2,7,3,6,2,1,4,5,1,7,2, 3,6,1,5,4,2,7,1,4,3,6,2,5,4,7,1, 6,3,2,4,5,6,7,1,2,6,3,5,4,3,7,6, 1,2,3,4,5,6,7,3,5,1,2,6,4,5,7,3, 2,1,6,5,4,2,7,3,6,2,1,4,5,1,7,2, 3,6,1,5,4,2,7,1,4,3,6,2,5,4,7,1, 6,3,2,4,5,6,7,1,2,6,3,5,4,3,7,6