Федеральное государственное бюджетное образовательное учреждение
высшего образования «Московский государственный университет имени М.В.
Ломоносова»

На правах рукописи

Ефимов Алексей Андреевич

Оценки энергопотребления объёмных схем

Специальность 1.1.5 —
«Математическая логика, алгебра, теория чисел и дискретная математика»

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научные руководители:
доктор физико-математических наук, профессор
Гасанов Эльяр Эльдарович
кандидат физико-математических наук
Калачев Глеб Вячеславович

Москва — 2023

Оглавление

Стр.

Введение

Одним из разделов математической кибернетики является теория управляющих систем. Интенсивное развитие науки и вычислительной техники в XX веке породило одно из интереснейших направлений в этой области — задачу синтеза схем, вычисляющих булевы функции и операторы. Автор решает эту задачу, разрабатывая универсальные методы синтеза схем и получая фундаментальные нижние оценки сложности схем, показывающие оптимальность применяемых методов.

Одной из основных моделей схем является схема из функциональных элементов (СФЭ). В качестве характеристики оптимальности СФЭ можно рассматривать сложность — количество функциональных элементов, содержащихся в схеме. Под сложностью булевой функции или оператора будем понимать минимальную сложность схемы, реализующую данную функцию или оператор. В 1956 году Д. Маллер [1] посчитал сложность любой булевой функции, равную $\Theta\left(2^n/n\right)$. В 1958 году О.Б. Лупанов [2] нашёл сложность почти всех булевых функций для любого конечного базиса $\{E\}$, которая асимптотически равна $\min\limits_{e\in E} P(e)\cdot 2^n/n$, где $P(e)$ — приведённый вес элемента e. В 1963 году [3] О.Б. Лупанов в качестве следствия установил, что в стандартном базисе $(\wedge,\vee,\neg)$ сложность почти всех булевых функций асимптотически равна $2^n/n$.

Отметим, что в 1961 году М.Н. Вайнцвайг [4] определил другую меру сложности СФЭ — мощность. Мощность или активность СФЭ — это максимальное количество элементов схемы, выдающих на выходе единицу, где максимум берётся по всем входным наборам. О.М. Касим-Заде [5] исследовал мощность в различных базисах и установил порядок функции Шеннона для произвольного конечного базиса.

В качестве альтернативной модели СФЭ рассматриваются контактные схемы (КС). Сложностью КС считается количество её контактов. Ю.С. Шуткин [6] ввёл понятие временной сложности КС, являющиеся некоторым аналогом мощности СФЭ. Им было установлено, что функция Шеннона сложности моделирования КС для функций от n переменных равна $2n-1$.

Существенным недостатком модели СФЭ является то, что в ней не учитываются вполне естественные ограничения на размещение элементов схемы в плоскости или пространстве, способы их соединения, разводка проводов и т.п.

В 1967 году С.С. Кравцов [7] впервые рассмотрел модель плоских прямоугольных схем, учитывающую данные ограничения. Им было показано, что порядок функции Шеннона площади плоских схем, реализующих функции от n переменных, равен 2^n. Одновременно с ним А.Д. Коршунов [8] начал рассматривать два класса схем: схемы из объёмных функциональных элементов и объёмные схемы из функциональных элементов. Для обоих классов при ограничении на длину проводов порядок функции Шеннона также равен 2^n.

Интересное обобщение модели клеточных схем — многослойные d-мерные схемы были рассмотрены Т.Р. Сытдыковым [9; 10]. Если k — число слоев в d-мерной схеме, то были получены верхняя и нижняя оценки функции Шеннона сложности прямоугольных многомерных схем равны $\Theta\left(\frac{2^n}{\min(n,d\log k)}\right)$.

Н.А. Шкаликова в работе [11] одной из первых исследовала связь между площадью плоских схем и объёмом трёхмерных схем, реализующих булевы операторы. Было показано, что если оператор можно реализовать объёмной схемой с объёмом V, то его можно реализовать плоской схемой площади $\Theta\left(n^{3/2}\right)$.

Также в работе [12] Н.А. Шкаликова изучила сложность реализации плоскими схемами некоторых классов булевых функций. В частности, было показано, что сложность реализации всех элементарных конъюнкций от n переменных равна $\Theta\left(n\cdot 2^n\right)$, сложность реализации всех булевых функций от n переменных равна $\Theta\left(n\cdot 2^{2^n}\right)$, сложность умножения двух n-разрядных чисел равна $\Theta\left(n^2\right)$.

Что касается одной булевой функции, то в работе [13] Н.А. Шкаликова построила специальную булеву функцию от n переменных, сложность которой равна $\Theta\left(n^{3/2}\right)$. Позднее, С.А. Ложкин и другие авторы в работе [14] ввели понятие коммуникативной сложности и сформулировали общий подход к получению нижних оценок сложности плоской реализации булевых функций. Ими была получена нижняя квадратичная оценка сложности одной специальной булевой функции для плоской реализации, и порядка $\Theta\left(n^{4/3}\right)$ для объёмной реализации.

О.В. Черемисин [15] показал, что в классе прямоугольных схем невозможна одновременная минимизация площади и мощности плоских схем, реализующих систему всех конъюнкций.

Особый интерес представляют работы Г.В. Калачёва [16—23], посвящённые плоским схемам. Автор также, как и Г.В. Калачёв, использует такую меру сложности схемы как потенциал. Он равен значению количества единиц на всех внутренних узлах схемы. Неформально говоря, потенциал играет роль

«энергии» схемы, необходимой для её функционирования. Кроме того, рассматривается и другая мера мощности — переключательная мощность — количество внутренних узлов схемы, изменяющих своё значение при изменении входных наборов схемы.

В статье [16] было показано, что имеют одинаковый порядок функции Шеннона потенциала и переключательной мощности плоских схем, реализующих булевы функции. В частности, для рассматриваемых мер мощности получен одинаковый порядок функции Шеннона, равный $\Theta(2^{n/2})$.

В работе [18] для почти всех частичных булевых операторов с областью определения D и m выходами получена нижняя оценка $\frac{m\sqrt{|D|}}{\sqrt{\min(m, \log_2 |D|)}}$ средней мощности. Отметим, что был применён метод расслоения, непрерывный аналог которого используется в данной диссертационной работе.

Позднее в статье [17] было показано, что при незначительных ограничениях на область определения оператора существует плоская схема, имеющая оптимальный порядок мощности, площади и глубины. В частности, для всюду определённых операторов с n входами и m выходами мощность равна $\Theta\left(\frac{m\sqrt{2^n}}{\min(n, \log_2 m)}\right)$, а глубина равна $\Theta\left(\max(n, \log_2 m)\right)$.

Для класса монотонных функций также был получен порядок функции Шеннона для среднего и максимального потенциала плоских схем. В частности, в работе [19], функция Шеннона для максимального потенциала равна $\Theta\left(\frac{2^{n/2}}{n^{1/4}}\right)$, а для среднего потенциала равна $\Theta\left(\frac{2^{n/2}}{n^{3/4}}\right)$. Также Г.В. Калачёвым в работе [19] были доказаны универсальные нижние оценки функции Шеннона мощности плоских схем. Кроме того, найден порядок роста функции Шеннона мощности схем, реализующих монотонные функции.

В статье [20] исследована функция Шеннона максимального потенциала плоских схем, реализующих функции от n переменных с ограниченным числом единиц. В частности, было показано, что если количество единиц функции ограничено числом N, то при условии $\log_2 N \asymp n$ порядок функции Шеннона равен $\Theta(N(n - \log_2 N))$.

Позднее в статье [22] был исследован порядок функции Шеннона потенциала плоских схем, реализующих частичные булевы операторы при наличии ограничений на количество различных значений, принимаемых оператором. Было показано, что в классе частичных операторов с m выходами, областью

определения мощности d и областью значения мощности не более r как средний, так и максимальный потенциал по порядку равны $\Theta\left(\left(\sqrt{d}+\frac{m\sqrt{r}}{\log_2 r}\right)\sqrt{\log_2 r}\right)$.

Очень интересный результат получен в работе [23]. Исследуется связь между площадью и максимальным потенциалом плоских схем, реализующих булевы операторы. Показано, что для произвольного булева оператора потенциал не меньше, чем $\sqrt{S}/4\sqrt{2}$, где S — площадь минимальной схемы, реализующей данный оператор.

Плоские автоматные схемы были недавно рассмотрены А.С. Воротниковым [24]. В качестве клеточного элемента здесь рассматривается автомат с не более чем двумя состояниями. А.С. Воротников получил верхнюю оценку переключательной мощности реализации периодической последовательности автоматной схемой. В работе приводится схема, реализующая произвольную последовательность длины 2^n с переключательной мощностью не более $\frac{2^{n/2}}{n}$.

Данная диссертационная работа посвящена объёмным схемам [25—28], которые определяются аналогично плоским схемам, но в трёхмерном пространстве. Под объёмной схемой будем понимать укладку схемы из функциональных элементов в пространстве. Объёмная схема состоит из кубических элементов. Каждый кубический элемент реализует булев оператор, у которого в сумме не более 6 входов и выходов.

Диссертационная работа состоит из введения и трёх глав. В введении даются основные понятия и определения. В частности, определяется объёмная схема и потенциал, как мера сложности объёмных схем.

Первая глава диссертационной работы является изложением статей [25; 26] и посвящена верхним оценкам функции Шеннона для булевых функций и операторов, реализуемых объёмными схемами. А именно, приведен универсальный метод синтеза, позволяющий построить для любой булевой функции (оператора) объёмную схему, реализующую данную функцию (оператор) и имеющую оптимальный порядок сложности и потенциала.

Вторая глава диссертационной работы, результаты которой опубликованы в статье [28], полностью посвящена нижней оценке функции Шеннона потенциала для частичных булевых операторов. Для доказательства используется вариация метода расслоения, ранее применявшегося в работах [16; 18] для плоских схем. Отметим, что для всюду определенных операторов нижняя оценка совпадает с верхней оценкой, доказанной в работе [26].

В третьей главе диссертационной работы рассматривается класс объёмных схем с близкими выходами. Для него получены нижняя и верхняя оценка функции Шеннона потенциала объёмных схем, совпадающие по порядку. Результаты опубликованы в статье [27].

Целью работы является исследование модели объёмных схем, реализующих булевы функции и операторы. Необходимо получить порядок функции Шеннона потенциала объёмных схем для класса схем без ограничений и в классе схем с близкими выходами.

Для достижения поставленной цели необходимо было решить следующие **задачи**:

1. Получить верхнюю оценку функции Шеннона потенциала объёмных схем, реализующих булевы функции и операторы.
2. Получить нижнюю оценку функции Шеннона потенциала объёмных схем, реализующих частичные булевы операторы.
3. Получить верхнюю оценку функции Шеннона потенциала объёмных схем, реализующих булевы операторы в классе схем с близкими выходами.
4. Получить нижнюю оценку функции Шеннона потенциала объёмных схем, реализующих булевы операторы в классе схем с ограничениями на расстояние между выходами.

Научная новизна:

1. Впервые была получена нижняя оценка потенциала объёмных схем, реализующих частичные булевы операторы.
2. Впервые была получена верхняя оценка потенциала объёмных схем, реализующих всюду определённые булевы операторы. При этом по порядку она совпадает с нижней оценкой.
3. Впервые был рассмотрен класс объёмных схем с близкими выходами, для которого получены верхняя и нижняя оценка функции Шеннона, совпадающие по порядку.

Практическая значимость Диссертация имеет теоретический характер. Методы, используемые в работе, могут быть использованы в дальнейшем теоретическом исследовании синтеза схем из различных классов. Результаты, полученные в работе, могут быть применены при проектировании различных электронных устройств с целью уменьшения энергопотребления.

Методология и методы исследования. В работе используются методы дискретной математики, теории управляющих систем, теории вероятностей и математического анализа.

Основные положения, выносимые на защиту. На защиту выносятся обоснование актуальности проведенного исследования и его научной новизны, цели и поставленные задачи, методы исследования, применённые для получения результатов, а также следующие положения, которые подтверждаются результатами исследований, представленными в Заключении диссертации.

1. Значение верхней оценки функции Шеннона потенциала объёмных схем, реализующих булевы функции и операторы.
2. Значение нижней оценки функции Шеннона потенциала объёмных схем, реализующих частичные булевы операторы.
3. Значение верхней оценки функции Шеннона потенциала объёмных схем, реализующих булевы операторы в классе схем с близкими выходами.
4. Значение нижней оценки функции Шеннона потенциала объёмных схем, реализующих булевы операторы в классе схем с ограничениями на расстояние между выходами.

Достоверность полученных результатов обеспечивается строгими математическими доказательствами. Работа прошла апробацию на научных семинарах, всероссийских и международных конференциях, и опубликована в рецензируемых научных журналах. Все результаты других авторов, которые используются в тексте диссертации, приводятся с указанием выходных данных публикаций.

Апробация работы. Основные результаты работы докладывались на следующих конференциях:

- Международная конференция студентов, аспирантов и молодых учёных «Ломоносов» (9.04.18 – 13.04.18, 8.04.19 – 12.04.19, 10.11.20 – 27.11.20, 11.04.22 – 22.04.22, Москва)
- Ломоносовские чтения (15.04.19 – 25.04.19, Москва)
- XIII Международный семинар «Дискретная математика и её приложения» имени академика О.Б. Лупанова (17.06.19 – 22.06.19, Москва)
- XIX Международная конференция «Проблемы теоретической кибернетики» (27.09.21 – 1.10.21, Казань)

Также результаты работы докладывались на семинарах механико-математического факультета МГУ имени М.В. Ломоносова:

– Семинар «Теория автоматов» под руководством академика, профессора, д.ф.-м.н. В.Б. Кудрявцева (2021)
– Семинар «Вопросы сложности алгоритмов поиска» под руководством профессора, д.ф.-м.н. Э.Э. Гасанова (2019–2022)
– Семинар «Математические вопросы кибернетики» (2023)

Личный вклад. Все приводимые в работе результаты, за исключением специально выделенных, сформулированы и доказаны автором лично.

Публикации. Основные результаты по теме диссертации изложены автором в 4 работах [25—28]. Все работы опубликованы в рецензируемом научном издании из дополнительного списка, утвержденного учёным советом МГУ, в котором могут быть опубликованы научные результаты диссертаций по направлению физико-математические науки. Работ, написанных в соавторстве, нет.

Краткое содержание работы.

Введение описывает актуальность поднятой проблемы, исследуемой в рамках диссертационной работы. Также проводится обзор научной литературы по данному исследованию, формулируется цель и задачи работы. Далее обосновывается научная новизна и научная значимость данной диссертации.

Также в введении вводятся основные понятия и определения.

Кубическим элементом будем называть булев оператор, у которого в сумме не более шести входов и выходов, причём каждому его входу и выходу сопоставлена некоторая метка из множества $\{l, t, r, b, f, a\}$ и метки не повторяются.

Метки будем называть сторонами элемента:

– l — левая сторона;
– r — правая сторона;
– t — верхняя сторона;
– b — нижняя сторона;
– f — передняя сторона;
– a — задняя сторона.

Кубический элемент будем изображать в виде единичного куба в пространстве. При этом входам и выходам элемента сопоставляются грани куба в соответствии с присвоенными им метками.

Метки, присвоенные входам (выходам) оператора будем называть *входами (выходами)* элемента. Метки, не присвоенные ни входам, ни выходам, будем называть *изоляторами*. Входы и выходы элемента будем называть его *контактами*.

Если на всех выходах элемента реализуются тождественные функции, то будем называть элемент *коммутационным*, иначе — *логическим*.

Описывать элемент можно уравнениями, которые задают его оператор, заменяя все переменные в них на сопоставленные им метки (l, t, r, b, f, a). Тогда в левой части каждого уравнения будет стоять выходная метка, а в правую часть будут входить только входные метки.

Сетью из кубических элементов на множестве $M \subseteq \mathbb{Z}^3$ будем называть отображение $K : M \to E$, где E — множество всех кубических элементов.

Элемент $K(x, y, z)$ будем называть *элементом схемы K с координатами* (x, y, z).

Левой, правой, верхней, нижней, передней и задней стороной элемента e с координатами (x, y, z) будем называть точки с координатами $(x - \frac{1}{2}, y, z), (x + \frac{1}{2}, y, z), (x, y, z + \frac{1}{2}), (x, y, z - \frac{1}{2}), (x, y + \frac{1}{2}, z), (x, y - \frac{1}{2}, z)$ соответственно.

Будем говорить, что сеть K из кубических элементов корректна, если для любых элементов x и y схемы K верно, что если сторона a элемента x совпадает со стороной b элемента y, то выполнено одно из условий:

- один из элементов x,y — изолирующий,
- стороны a и b являются изоляторами,
- среди них одна является входом, другая выходом; если a — выход, а b — вход, то будем говорить, что выход a *подключен* ко входу b.

Введём понятие *графа корректной сети из кубических элементов K* (будем обозначать G_K). G_K — ориентированный граф, вершинами которого являются входы и выходы элементов схемы. Если выход одного элемента подключен ко входу другого, то им будет соответствовать одна и та же вершина графа (будем говорить, что эта вершина является выходом первого элемента и входом второго). Из вершины a в вершину b ведёт ребро в том и только в том случае, когда существует элемент e, такой, что a является его входом, b — выходом, причём функция, реализуемая на выходе b, существенно зависит от входа a.

Объёмной схемой или *схемой из кубических элементов* на множестве $M \subseteq \mathbb{Z}^3$ будем называть корректную сеть из кубических элементов, в графе

которой нет ориентированных циклов. Множество M будем называть *носителем* схемы K.

Длиной схемы K будем называть длину наименьшего прямоугольного параллелепипеда, содержащего все элементы схемы K, обозначается $\ell_1(K)$.

Шириной схемы K будем называть ширину наименьшего прямоугольного параллелепипеда, содержащего все элементы схемы K, обозначается $\ell_2(K)$.

Высотой схемы K будем называть высоту наименьшего прямоугольного параллелепипеда, содержащего все элементы схемы K, обозначается $\ell_3(K)$.

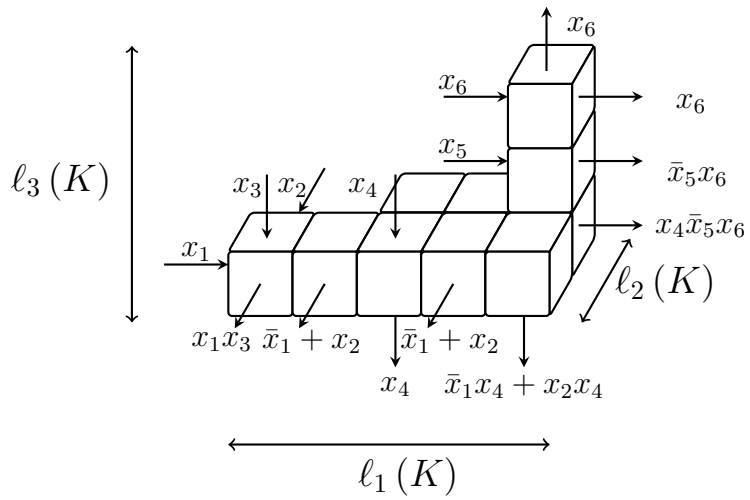


Рисунок 1 — Изображение объёмной схемы K.

Длину схемы мы будем считать по оси Ox, ширину — по оси Oy, высоту — по оси Oz. На примере, изображенном на рис. 1, у схемы K имеется 6 входов, 9 выходов, а характеристики равны: $\ell_1(K) = 5, \ell_2(K) = 2, \ell_3(K) = 3$.

Если вход (выход) элемента не подключен к выходу (входу) другого элемента, будем его называть *входом (выходом)* схемы. *Контактами* схемы K будем называть её входы и выходы, и обозначать их $\mathrm{In}(K), \mathrm{Out}(K)$ соответственно.

Узлами схемы K будем называть вершины графа G_K.

Если M — носитель схемы K, то величину $|M|$, равную количеству элементов в множестве M, будем называть *объёмом* схемы K и обозначать $V(K)$.

Каждой объёмной схеме K можно сопоставить схему их функциональных элементов $\mathrm{Circ}(K)$ следующим образом:

1. каждой функции $f_{s,i}$, которую реализует i-й выход элемента s объёмной схемы, сопоставим функциональный элемент $e_{s,i}$, реализующий $f_{s,i}$; если на i-м и j-м выходе реализуется одна и та же функция, то им будет соответствовать один и тот же функциональный элемент;

2. если i-й выход элемента s_1 подключен к j-му входу элемента s_2, то соединим выход элемента $e_{s_1,i}$ с j-ми входами элементов $e_{s_2,k}$ для всех k, для которых $f_{s_2,k}$ существенно зависит от j-го аргумента.

Будем говорить, что схема K *реализует* булев оператор F, если схема из функциональных элементов $\mathrm{Circ}(K)$ реализует F. Через $\mathrm{Impl}(F)$ обозначим множество всех объёмных схем, реализующих оператор F.

Через $V(F)$ обозначим объём схемы, реализующей оператор F, и обладающей минимальным объёмом среди всех объёмных схем, реализующих F. То есть, $V(F) := \min\limits_{K \in \mathrm{Impl}(F)} V(K)$. Здесь и далее символ $:=$ обозначает «по определению равно».

Будем говорить, что объёмные схемы K_1 и K_2 *равны* и писать $K_1 = K_2$, если существует параллельный перенос пространства π, который позволяет совместить схемы K_1 и K_2 (т.е. $K_1 = K_2 \circ \pi$), иначе будем говорить, что они *различны*.

Для каждой схемы K зафиксируем некоторую нумерацию её узлов. На i-м узле реализуется некоторая функция g_i от входных переменных схемы K (на входах схемы считаем, что реализуются тождественные функции).

Также далее будем считать, что схема K имеет n входов, m выходов и l узлов.

Для вектора $v = (v_1, ..., v_q) \in \{0,1\}^q$ введём обозначение

$$|v| := v_1 + v_2 + ... + v_q.$$

Потенциалом схемы K на входном наборе $x \in \{0,1\}^n$ назовём величину $u_K(x) := |(g_1(x),..., g_l(x))|$.

Средним потенциалом схемы K на множестве входных наборов $D \subseteq \{0,1\}^n$ назовём величину

$$U_D(K) := \frac{1}{|D|} \sum_{x \in D} u_K(x).$$

Через $P_2(D, m)$ обозначим множество частичных булевых операторов $f : D \to \{0,1\}^m$ с m выходами, определённых на множестве D.

Пусть $f \in P_2(D, m)$. Тогда

$$U(f) := \min_{K \in \mathrm{Impl}(f)} U_D(K).$$

Если множество $\mathrm{Impl}(f)$ пусто, то формально полагаем $U(f) = \infty$.

Максимальным потенциалом схемы K на множестве входных наборов $D \subseteq \{0,1\}^n$ назовём величину

$$\hat{U}_D(K) := \max_{x \in D} u_K(x).$$

Пусть $f \in P_2(D,m)$. Тогда

$$\hat{U}(f) := \min_{K \in \mathrm{Impl}(f)} \hat{U}_D(K).$$

Если $\mathrm{Impl}(f)$ пусто, то формально полагаем $\hat{U}(f) = \infty$.

Через $P_2(n,m)$ обозначим множество всюду определённых булевых операторов $f : \{0,1\}^n \to \{0,1\}^m$ с n входами и m выходами.

Введём функцию Шеннона для среднего и максимального потенциала:

$$U(n,m) := \max_{f \in P_2(n,m)} U(f).$$

$$\hat{U}(n,m) := \max_{f \in P_2(n,m)} \hat{U}(f).$$

Мы будем рассматривать случай, когда выходы схемы располагаются достаточно близко. Если мы будем рассматривать лишь схемы из некоторого множества Q, то будем ко всем мерам сложности и мощности добавлять нижний индекс Q.

Пусть $f \in P_2(D,m)$. Тогда

$$U_Q(f) := \min_{K \in Q \cap \mathrm{Impl}(f)} U_D(K).$$

Если $Q \cap \mathrm{Impl}(f)$ пусто, то формально полагаем $U_Q(f) = \infty$.

Аналогично определим максимальный потенциал для $f \in P_2(n,m)$:

$$\hat{U}_Q(f) := \min_{K \in Q \cap \mathrm{Impl}(f)} \hat{U}(K).$$

Если $Q \cap \mathrm{Impl}(f)$ пусто, то формально полагаем $\hat{U}_Q(f) = \infty$.

Введём функцию Шеннона для среднего и максимального потенциала:

$$U_Q(n,m) := \max_{f \in P_2(n,m)} U_Q(f).$$

$$\hat{U}_Q(n,m) := \max_{f \in P_2(n,m)} \hat{U}_Q(f).$$

Деревом выходов схемы K назовем минимальное остовное дерево полного графа с вершинами в выходных элементах схемы K, у которого длины рёбер

равны расстоянию между элементами — расстоянию между их центрами в манхэттенской метрике.

Введём величину $T(K)$. Пусть m — количество выходов схемы K, числа $r_1, \ldots, r_{m-1}$ — длины рёбер дерева выходов. Положим

$$T(K) := \sum_{j=1}^{m-1} r_j.$$

То есть $T(K)$ — величина, равная суммарной длине рёбер дерева выходов схемы K, которую для краткости будем называть длиной дерева выходов.

Введём множество $T_h := \{K : T(K) \leqslant h\}$, состоящее из таких объёмных схем, у которых длина дерева выходов не превосходит h.

Через T_{near} обозначим множество объёмных схем K, у которых длина дерева выходов не превосходит числа выходов.

Для удобства для любого $q \in \mathbb{N}$ положим $[q] = \{1, 2, \ldots, q\}$.

Пусть K — объёмная схема, $f : D \mapsto \{0,1\}^m$ — булев оператор, причём $K \in \mathrm{Impl}(f)$. Определим образ $Im(K) := \{y \in \{0,1\}^m \mid f(x) = y, x \in D\}$ схемы K.

В связи с большим числом параметров, от которых будут зависеть оценки (в том числе и неявно), уточним, как будут пониматься в работе такие стандартные обозначения, как $o(\cdot), O(\cdot), \mathcal{O}(\cdot), \Theta(\cdot)$ в случае наличия неявных параметров. Нам часто потребуется писать асимптотические оценки различных величин, явно или неявно зависящих от набора параметров $x = (x_1, \ldots, x_k)$. Пусть есть некоторое множество допустимых наборов параметров X, и нём задана база подмножеств[1] $\mathfrak{B}$. Допустимые значения остальных параметров образуют множество Y и в данном контексте считаются фиксированными. Пусть величины f и g явно или неявно зависят от параметров $x \in X, y \in Y$. Введём обозначения:

1. $f(x, y) = o(g(x, y))$ при базе $\mathfrak{B}$, если

$$\forall y \in Y \ (\exists B \in \mathfrak{B}, \ \forall x \in B, \ g(x, y) \neq 0) : \lim_{\mathfrak{B}} \frac{f(x, y)}{g(x, y)} = 0.$$

2. $f(x, y) = O(g(x, y))$ при базе $\mathfrak{B}$, если

$$\exists C > 0, \ \forall y \in Y, \ \exists B \in \mathfrak{B}, \ \forall x \in B : f(x, y) \leqslant C g(x, y).$$

[1] Непустая система $\mathfrak{B}$ подмножеств множества X называется *базой* множества X, если $\varnothing \notin \mathfrak{B}$ и для любых $B_1, B_2 \in \mathfrak{B}$ существует $B \in \mathfrak{B}$ такое, что $B \subset B_1 \cap B_2$.

3. $f(x,y) \asymp g(x,y)$ или $f(x,y) = \Theta(g(x,y))$ при базе $\mathfrak{B}$, если $f(x,y) = O(g(x,y))$ и $g(x,y) = O(f(x,y))$, то есть

$$\exists C_1, C_2 > 0,\ \forall y \in Y,\ \exists B \in \mathfrak{B},\ \forall x \in B : C_1 g(x,y) \leqslant f(x,y) \leqslant C_2 g(x,y).$$

Для неасимптотических неравенств с точностью до константы будем использовать обозначение $f(x,y) = \mathcal{O}(g(x,y))$, если $f(x,y) \leqslant Cg(x,y)$ для некоторой абсолютной константы C.

Если каждый набор параметров $x \in X$ задаёт некоторое множество объектов $\mathcal{F}(x)$, то будем говорить, что *для почти всех* элементов $f \in \mathcal{F}(x)$ при базе $\mathfrak{B}$ верно утверждение $P(x,f)$, если

$$|\{f \in \mathcal{F}(x) : P(x,f)\}| = |\mathcal{F}(x)|(1 + o(1)) \text{ при базе } \mathfrak{B}.$$

Отметим, что обычно множество $\mathcal{F}(x)$ — это множество булевых операторов, а набор параметров x включает в себя число аргументов n, область определения D, число выходов оператора m, а также ограничения на геометрию схемы. База $\mathfrak{B}$ как правило задается несколькими асимптотическими ограничениями на параметры при $n \to \infty$.

Глава 1 посвящена верхним оценкам. Первая часть состоит из реализации вспомогательных блоков, с помощью которых реализуется схема для любой всюду определённой булевой функции и булева оператора. В частности, особый интерес вызывает дешифратор, который позволяет подводить информацию от одного блока к другому, минимизируя при этом потенциал проводов.

Основная верхняя оценка для булевых функций сформулирована в теореме 1.

Теорема 1. *Пусть дана булева функция $f(x_1, x_2, \ldots, x_n)$. Тогда существует объёмная схема V_f со входами $x_1, x_2, \ldots, x_n$ на одном выходе которой реализуется функция $f(x_1, x_2, \ldots, x_n)$, причём схема V_f обладает следующими характеристиками:*

1. $\ell_1(V_f) = \mathcal{O}(2^{n/3}),\ \ell_2(V_f) = \mathcal{O}(2^{n/3}),\ \ell_3(V_f) = \mathcal{O}(2^{n/3})$.
2. $\boldsymbol{\hat{U}(V_f) = \mathcal{O}(2^{n/3})}$.
3. $V(V_f) = \mathcal{O}(2^n)$.

Следующая теорема является обобщением теоремы 2 на случай, когда нужно реализовать несколько булевых функций (булев оператор).

Теорема 2. *Пусть дан булев оператор* $f : \{0,1\}^n \to \{0,1\}^m$. *Тогда существует объёмная схема* W_f *со входами* $x_1, x_2, \ldots, x_n$ *на* m *выходах которой реализуется оператор* f, *причём схема* W_f *обладает следующими характеристиками: Если* $m \leqslant n$:

1. $\ell_1(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $\ell_2(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $\ell_3(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$.
2. $\boldsymbol{\hat{U}(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).}$
3. $V(W_f) = \mathcal{O}(m \cdot 2^n)$.

Если $m > n$:

1. $\ell_1(W_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $\ell_2(W_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $\ell_3(W_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$.
2. $\boldsymbol{\hat{U}(W_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3}).}$
3. $V(W_f) = \mathcal{O}(m \cdot 2^n)$.

В **главе 2** получена нижняя оценка для частичных булевых операторов. Для доказательства использовалась непрерывная модификация метода расслоения. Идея метода расслоения состоит в том, чтобы считать потенциал схемы по слоям и потом интегрировать оценки. Таким образом была получена теорема 3.

Теорема 3. *Существует такая абсолютная константа* $C > 0$, *что для любого натурального* n, *любого* $D \subseteq \{0,1\}^n$ *верно*

$$\boldsymbol{U(f) \geqslant C \frac{m \sqrt[3]{|D|}}{\min^{2/3}(m, \log_2 |D|)}}$$

для почти всех операторов $f \in P_2(D, m)$ *при* $n \log_2 n = o(|D|), \log_2 m = o(|D|), |D| \to \infty$.

Фраза «для почти всех операторов» означает, что доля операторов стремится к 1 при указанных условиях.

Учитывая результат теоремы 2 и теоремы 3, получаем порядок функции Шеннона для всюду определённых булевых операторов.

Следствие 1. *Для почти всех* $f \in P_2(n, m)$, *при* $n \to \infty$, $\log_2 m = o(2^n)$ *верно асимптотическое равенство:*

$$\boldsymbol{U(f) = \Theta\left(\frac{m \cdot 2^{n/3}}{\min^{2/3}(m, n)}\right).}$$

Следствие 2. *Пусть* $n \to \infty$, $\log_2 m = o(2^n)$. *Тогда верно асимптотическое равенство:*

$$\boldsymbol{U(n,m) \asymp \hat{U}(n,m) = \Theta\left(\frac{m \cdot 2^{n/3}}{\min^{2/3}(m,n)}\right).}$$

Глава 3 посвящена классу T_{near} объёмных схем с близкими выходами и классу T_h. Для класса T_h в теореме 4 получена нижняя оценка потенциала.

Теорема 4. *Существует такая абсолютная константа* C, *что для любого натурального* n, *любого* $D \subseteq \{0,1\}^n, d = |D|$ *неравенство*

$$\boldsymbol{U_{T_h}(f) \geqslant \begin{cases} C\frac{m\sqrt[3]{md}}{\log_2 d}, & \text{если } \sqrt[3]{md} > h, \\ C\frac{m\sqrt{md}}{\sqrt{h}\log_2 d}, & \text{если } \sqrt[3]{md} \leqslant h. \end{cases}}$$

выполнено для почти всех $f \in P_2(D,m)$ *при* $n \to \infty$, $n\log_2(n) = o(d)$, $\log_2(m) = o(d)$.

Также в теореме 5 для класса T_{near} получена верхняя оценка потенциала, совпадающая по порядку с нижней оценкой.

Теорема 5. *Для любого булева оператора* $f : \{0,1\}^n \to \{0,1\}^m$, *существует объёмная схема* $K_f \in T_{\text{near}}$ *со входами* $x_1, x_2, \ldots, x_n$ *на* m *выходах которой реализуется оператор* f, *причём схема* K_f *обладает следующими характеристиками:*

Если $m \leqslant n$:

1. $\ell_1(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right)$, $\ell_2(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right)$, $\ell_3(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right)$.
2. $\boldsymbol{\hat{U}(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right).}$
3. $V(K_f) = \mathcal{O}(m \cdot 2^n)$.

Если $n < m \leqslant 2^{n/2}$:

1. $\ell_1(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right)$, $\ell_2(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right)$, $\ell_3(K_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$.
2. $\boldsymbol{\hat{U}(K_f) = \mathcal{O}\left(\frac{m}{n} \cdot \sqrt[3]{m} \cdot 2^{n/3}\right).}$
3. $V(K_f) = \mathcal{O}(m \cdot 2^n)$.

Если $m > 2^{n/2}$:

1. $\ell_1(K_f) = \mathcal{O}\left(2^{n/2}\right)$, $\ell_2(K_f) = \mathcal{O}\left(2^{n/2}\right)$, $\ell_3(K_f) = \mathcal{O}(m)$.
2. $\boldsymbol{\hat{U}(K_f) = \mathcal{O}\left(\frac{m}{n} \cdot 2^{n/2}\right).}$

3. $V\left(K_f\right) = \mathcal{O}(m \cdot 2^n)$.

Таким образом, в качестве следствия из теорем 4 и 5 получаем порядок функции Шеннона в классе объёмных схем с близкими выходами.

Следствие 3. *Для почти всех* $f \in P_2\left(n, m\right)$, *при* $m \geqslant n, n \to \infty$, $\log_2(m) = o(2^n)$ *верно равенство:*

$$\boldsymbol{U_{T_{\text{near}}}(f) = \Theta\left(\frac{m}{n} \cdot \left(\min(m, 2^{n/2})\right)^{1/3} \cdot 2^{n/3}\right).}$$

Благодарности. Автор выражает особую признательность научному руководителю д.ф.-м.н. профессору Эльяру Эльдаровичу Гасанову за постановку задачи, научное руководство, постоянное внимание к работе и поддержку на всех этапах написания диссертации. Также автор выражает особую благодарность научному руководителю к.ф.-м.н. Глебу Вячеславовичу Калачеву за постоянную помощь, неугасаемый интерес и научные обсуждения, помогающие улучшить читаемость текста и четкость формулировок.

Автор приносит благодарность профессорско-преподавательскому составу механико-математического факультета МГУ имени М.В. Ломоносова. Также, автор благодарит коллектив кафедры Математической теории интеллектуальных систем за опыт, знания и ценные советы, полученные за весь период обучения.

Объем и структура работы. Диссертация состоит из введения, 3 глав и заключения. Полный объём диссертации составляет 102 страницы, включая 29 рисунков. Список литературы содержит 28 наименований.

Глава 1. Верхние оценки

При доказательстве верхних и нижних оценок возникает множество констант, которые мы будем обозначать $C_1, C_2, C_3 \ldots$. Конкретные значения данных констант нам не важны, так как оценки приводятся с точностью до порядка. В доказательстве верхних и нижних оценок нумерация констант будет независимой.

1.1 Параметры основных блоков

Любую плоскую схему можно отождествить с объёмной схемой такой же длины, ширины, и единичной высоты (что следует непосредственно из определения). При этом ясно, что оценки потенциала такой объёмной схемы совпадают с соответствующей ей плоской схемой. Некоторые леммы из работы [17] мы переформулируем указанным образом.

Для реализации булевой функции и булева оператора нам потребуются несколько различных блоков. Опишем их характеристики.

1. Дешифратор D'_n (*Калачёв Г.В., [17, лемма 1]*):

$$\ell_1(D'_n) = 2^n,\ \ell_2(D'_n) \leqslant n(n+3)/2,\ \ell_3(D'_n) = 1,\ \hat{U}(D'_n) = \mathcal{O}(n^2 \cdot 2^n).$$

2. Дешифратор D^1_n:

$$\ell_1(D^1_n) = \mathcal{O}(2^n),\ \ell_2(D^1_n) = \mathcal{O}(2^{n/2}),\ \ell_3(D^1_n) = 1,\ \hat{U}(D^1_n) = \mathcal{O}(2^n).$$

3. Блок дешифраторов $D'_{n,k}$ (*Калачёв Г.В., [17]*):

$$\ell_1(D'_{n,k}) = \mathcal{O}(k \cdot 2^n),\ \ell_2(D'_{n,k}) = \mathcal{O}(n^2) + \mathcal{O}(nk),\ \ell_3(D'_{n,k}) = 1,$$
$$\hat{U}(D'_{n,k}) = \mathcal{O}(kn^2 \cdot 2^n) + \mathcal{O}(k^2 n \cdot 2^n).$$

4. Левый обратный блок $D'^{-1}_{n,k}$ к блоку $D'_{n,k}$, т.е. композиция $D'^{-1}_{n,k} \circ D'_{n,k}$ реализует тождественный оператор (*Калачёв Г.В., [17]*):

$$\ell_1(D'^{-1}_{n,k}) = \mathcal{O}(k \cdot 2^n),\ \ell_2(D'^{-1}_{n,k}) = \mathcal{O}(kn^2),\ \ell_3(D'^{-1}_{n,k}) = 1,$$
$$\hat{U}(D'^{-1}_{n,k}) = \mathcal{O}(k^2 n^2 \cdot 2^n).$$

5. Схема S_f, реализующая функцию f от n переменных (*Калачёв Г.В., [17, лемма 7]*):

$$\ell_1(S_f) = \mathcal{O}(2^{n/2}),\ \ell_2(S_f) = \mathcal{O}(2^{n/2}),\ \ell_3(S_f) = 1,\ \hat{U}(S_f) = \mathcal{O}(2^{n/2}).$$

6. Блок S_f^1:

$$\ell_1(S_f^1) = \mathcal{O}(2^{n/3}),\ \ell_2(S_f^1) = \mathcal{O}(2^{n/3}),\ \ell_3(S_f^1) = 1,\ \hat{U}(S_f^1) = \mathcal{O}(2^{n/3}).$$

7. Схема V_f^1, реализующая функцию f от n переменных:

$$\ell_1(V_f^1) = \mathcal{O}(2^{n/3}),\ \ell_2(V_f^1) = \mathcal{O}(2^{n/3}),\ \ell_3(V_f^1) = \mathcal{O}(2^{n/3}),\ \hat{U}(V_f^1) = \mathcal{O}(2^{n/3}).$$

8. Схема Q_f, реализующая оператор $f : \{0,1\}^n \to \{0,1\}^m, (m \leqslant n)$ (*Калачёв Г.В., [17, лемма 12]*):

$$\ell_1(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^{n/2}),\ \ell_2(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^{n/2}),\ \ell_3(Q_f) = 1,$$
$$\hat{U}(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^{n/2}).$$

9. Схема Q_g^1, такая что схема $D'^{-1}_{m/4,4} \circ Q_g^1 \circ D'_{k-l,4}$ реализует оператор $g : \{0,1\}^{4k-4l} \to \{0,1\}^m, n = 6k, m = 2^{12l}, G := Im(D'_{k-l,4})$:

$$\ell_1(Q_g^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}),\ \ell_2(Q_g^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}),\ \ell_3(Q_g^1) = 1,$$
$$\hat{U}_{\{1\}\times G}(Q_g^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}), \hat{U}_{\{0\}\times G}(Q_g^1) = 4.$$

10. Блок $\vee_n^k$, реализующий k дизъюнкций от n переменных:

$$\ell_1(\vee_n^k) = 1,\ \ell_2(\vee_n^k) = k,\ \ell_3(\vee_n^k) = n,\ \hat{U}(\vee_n^k) = \mathcal{O}(nk).$$

1.2 Реализация вспомогательных блоков

В данном параграфе подробно опишем реализацию всех вспомогательных блоков. Почти все блоки, которые мы будем использовать будут иметь так называемый *управляющий вход* z, а все элементы будут сохранять 0. Таким образом, если $z = 0$ и значения других входов равны 0, то потенциал внутренней части блока равен 0. Отметим, что значения выходов в таком случае также равны 0, то есть реализуемая схемой функция от переменных $z, x_1, \ldots, x_n$ лежит в

классе[1] T_0. Таким образом, вход z играет роль «выключателя» блока. Наличие такого входа позволяет достаточно легко оценивать потенциал схем, состоящих из нескольких блоков.

Для удобства введём еще одно обозначение. Пусть $i \in \mathbb{Z}, 0 \leqslant i \leqslant 2^n - 1$. Тогда $\bar{i}_1, \bar{i}_2, \ldots, \bar{i}_n$ — разложение числа i в двоичном виде, где $\bar{i}_1$ — младший бит разложения, а $\bar{i}_n$ — старший.

Дешифратор D'_n.

Напомним, что дешифратором (а также декодером) называется схема с n входами $x_1, x_2, \ldots, x_n$ и 2^n выходами, на i выходе которой конъюнкция $x_1^{\bar{i}_1} x_2^{\bar{i}_2} \ldots x_n^{\bar{i}_n}$. Таким образом, дешифратор преобразует двоичный код в унарный. D'_n — плоский дешифратор с управляющим входом z.

Лемма 1. *(Калачёв Г.В., [17, лемма 1]) Существует объёмная схема D'_n со входами $z, x_1, \ldots, x_n$ имеющая 2^n выходов, на i-м выходе которой на допустимых наборах $(z \geqslant x_1 \vee \ldots \vee x_n)$ реализуется функция*

$$z x_1^{\bar{i}_1} x_2^{\bar{i}_2} \ldots x_n^{\bar{i}_n},$$

причём схема D'_n обладает следующими характеристиками:

1. $\ell_1(D'_n) = \mathcal{O}(2^n),\ \ell_2(D'_n) = \mathcal{O}(n^2),\ \ell_3(D'_n) = 1.$
2. $\hat{U}(D'_n) = \mathcal{O}(n^2 \cdot 2^n).$

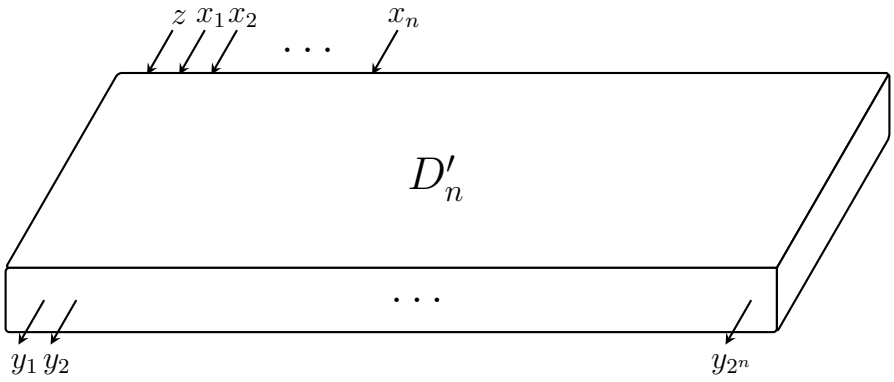


Рисунок 1.1 — Дешифратор D'_n.

Дешифратор D^1_n.

[1] Класс булевых функций, сохраняющих 0

D_n^1 — плоский дешифратор с управляющим входом z, имеющий оптимальный потенциал.

Лемма 2. *Существует объёмная схема D_n^1 со входами $z, x_1, \ldots, x_n$ имеющая 2^n выходов, на i-м выходе которой на допустимых наборах $(z \geqslant x_1 \vee \ldots \vee x_n)$ реализуется функция*

$$z x_1^{\bar{i}_1} x_2^{\bar{i}_2} \ldots x_n^{\bar{i}_n},$$

причём схема D_n^1 обладает следующими характеристиками:

1. $\ell_1(D_n^1) = \mathcal{O}(2^n),\ \ell_2(D_n^1) = \mathcal{O}(2^{n/2}),\ \ell_3(D_n^1) = 1.$
2. $\hat{U}(D_n^1) = \mathcal{O}(2^n).$

Доказательство. Сначала построим схему для случая $n = 2k$. Сделаем дешифратор D_n^1 из двух дешифраторов D'_k и некоторого количества элементов $\&$ и $\&'$ (см. рис. 1.2). Отметим, что похожая схема дешифратора использовалась в работах [15; 16].

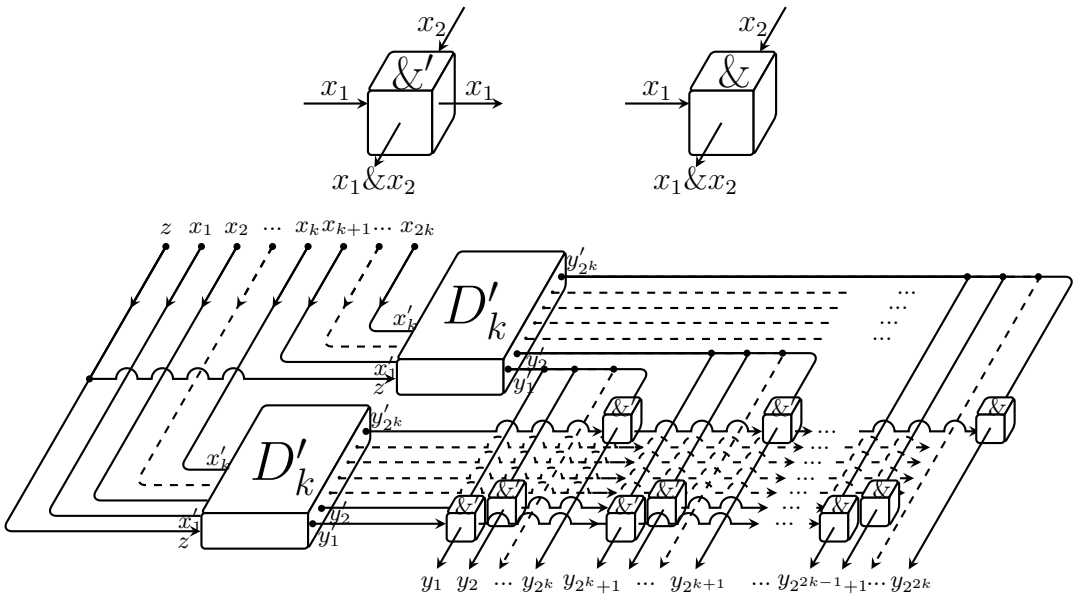


Рисунок 1.2 — Реализация дешифратора D_n^1.

Посчитаем характеристики схемы D_n^1.

$$\ell_1(D_n^1) = (k+1) + 2 \cdot \mathcal{O}(k^2) + 2^k \cdot 2^k = \mathcal{O}(2^{2k}) = \mathcal{O}(2^n).$$
$$\ell_2(D_n^1) = 2 \cdot \ell_1(D'_k) = \mathcal{O}(2^k) = \mathcal{O}(2^{n/2}).$$
$$\ell_3(D_n^1) = 1.$$

Оценим потенциал схемы. Заметим, что так как у каждого элемента схемы максимум 6 входов/выходов, то потенциал не превосходит объёма схемы, умноженного на 6. Таким образом, потенциал всей «левой» части схемы (включая

блоки D'_k) оценим через объём.

$$U_1 \leqslant 6 \cdot \ell_2(D^1_n) \cdot ((k+1) + 2 \cdot \ell_2(D'_k)).$$

Далее воспользуемся тем фактом, что при любом входном наборе из любой из 2-х схем D'_k выходит ровно один активный провод. Оценим длину активного провода нижнего блока D'_k.

$$U_2 = \mathcal{O}(2^{2k}).$$

Оценим длину активного провода верхнего блока D'_k.

$$U_3 = \mathcal{O}(2^{2k}).$$

Также заметим, что сигнал из верхнего блока D'_k в какой-то момент разветвится на 2^k сигналов, которые пойдут вниз и пересекутся с сигналом из нижнего блока D'_k. Оценим потенциал этой части схемы через объём.

$$U_4 \leqslant 6 \cdot 2\ell_1(D'_k) \cdot 2^k.$$

Сложим полученные результаты и получим оценку потенциала:

$$\hat{U}(D^1_n) = U_1 + U_2 + U_3 + U_4 \leqslant 6 \cdot \ell_2(D^1_n) \cdot ((k+1) + 2 \cdot \ell_2(D'_k)) + \mathcal{O}(2^{2k}) + \\ + \mathcal{O}(2^{2k}) + 6 \cdot 2\ell_1(D'_k) \cdot 2^k = \mathcal{O}(2^k) \cdot \mathcal{O}(k^2) + \mathcal{O}(2^{2k}) + \mathcal{O}(2^{2k}) = \mathcal{O}(2^n).$$

В случае, когда $n = 2k + 1$ построим схему для $n' = 2k + 2$, добавив в функцию фиктивную переменную, и подадим на последний вход x_{2k+2} константу 0. Получим схему с нужными характеристиками в силу того, что константы в оценках схемы увеличатся максимум в 2 раза, нам нужны оценки по порядку. □

Замечание: В данной работе мы используем дешифратор D^1_n, так как он имеет оптимальный потенциал. Дешифратор D'_n использовался в работе [17] потому, что у него была оптимальная «глубина», хотя и неоптимальный потенциал.

Блок дешифраторов $D'_{n,k}$.

Плоский блок дешифраторов $D'_{n,k}$. На вход подаются k групп переменных по n штук + отдельная переменная z. Переменные обозначаем x^i_j, где i

— номер группы, а j — номер переменной в этой группе. Каждую группу переменных мы подаем на отдельный дешифратор D'_n, переменную z подаем на все дешифраторы. Объединение выходов всех дешифраторов есть выходы схемы. Основное свойство блока дешифраторов в том, что у него сравнительно небольшой потенциал, а при этом на выходе активны всегда ровно k выходов (по одному с каждого дешифратора).

Лемма 3. *(Калачёв Г.В., [17]) Существует объёмная схема $D'_{n,k}$ со входами $z, x_1^1, \ldots, x_n^1, x_1^2 \ldots, x_n^2, \ldots, x_n^k$ имеющая $k{\cdot}2^n$ выходов, на (i, j)-м выходе которой реализуется функция*

$$(x_1^i)^{\bar{j}_1}(x_2^i)^{\bar{j}_2}\ldots(x_n^i)^{\bar{j}_n},$$

причём схема $D'_{n,k}$ обладает следующими характеристиками:

1. $\ell_1(D'_{n,k}) = \mathcal{O}(k \cdot 2^n),\ \ell_2(D'_{n,k}) = \mathcal{O}(n^2) + \mathcal{O}(nk),\ \ell_3(D'_{n,k}) = 1.$
2. $\hat{U}(D'_{n,k}) = \mathcal{O}(kn^2 \cdot 2^n) + \mathcal{O}(k^2 n \cdot 2^n).$

Обратный блок дешифраторов $D'^{-1}_{n,k}$.

Плоский левый обратный блок дешифраторов $D'^{-1}_{n,k}$ к блоку $D'_{n,k}$, т.е. композиция $D'^{-1}_{n,k} \circ D'_{n,k}$ реализует тождественный оператор.

Лемма 4. *(Калачёв Г.В., [17]) Существует объёмная схема $D'^{-1}_{n,k}$ со входами $x_1^1, \ldots, x_{2^n}^1, x_1^2, \ldots, x_{2^n}^2, \ldots, x_{2^n}^k$ имеющая $k \cdot n + 1$ выход, причём схема $D'^{-1}_{n,k}$ обладает следующими характеристиками:*

1. $\ell_1(D'^{-1}_{n,k}) = \mathcal{O}(k \cdot 2^n),\ \ell_2(D'^{-1}_{n,k}) = \mathcal{O}(kn^2),\ \ell_3(D'^{-1}_{n,k}) = 1.$
2. $\hat{U}(D'^{-1}_{n,k}) = \mathcal{O}(k^2 n^2 \cdot 2^n).$

Иногда выход z нам будет не нужен, и в этих случаях мы будем изображать блок $D'^{-1}_{n,k}$ без выхода z.

Блок S_f.

Плоский блок S_f. Блок, который выдает значения данной булевой функции f и имеет оптимальные по порядку параметры (на плоскости).

Лемма 5. *(Калачёв Г.В., [17, лемма 7]) Пусть дана функция $f(x_1, x_2, \ldots, x_n)$. Тогда существует объёмная схема S_f со входами $z, x_1, x_2, \ldots, x_n$ на одном выходе которой на допустимых наборах $(z \geqslant x_1 \vee \ldots \vee x_n)$ реализуется функция $zf(x_1, x_2, \ldots, x_n)$, причём схема S_f обладает следующими характеристиками:*

1. $\ell_1(S_f) = \mathcal{O}(2^{n/2}),\ \ell_2(S_f) = \mathcal{O}(2^{n/2}),\ \ell_3(S_f) = 1.$
2. $\hat{U}(S_f) = \mathcal{O}(2^n).$

Блок Q_f.

Плоский блок Q_f. Прямоугольный блок, который выдает значения данного булева оператора f и имеет оптимальные по порядку параметры (на плоскости). Лемма, используемая в работе [17], сформулирована для частичных операторов и в общем виде. Мы воспользуемся следствием из неё для случая $m \leqslant n$. Также в самой формулировке леммы не указаны оценки для длины и ширины схемы, но при этом они явно указаны в доказательстве.

Лемма 6. *(Калачёв Г.В., [17, лемма 12]) Пусть дан булев оператор* $f : \{0,1\}^n \to \{0,1\}^m$, *где* $m \leqslant n$. *Тогда существует объёмная схема* Q_f *со входами* $z, x_1, x_2, \ldots, x_n$ *на* m *выходах которой реализуется оператор* $f'(z, \vec{x}) = zf(x)$, *причём схема* Q_f *обладает следующими характеристиками:*

1. $\ell_1(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^{n/2}),\ \ell_2(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^{n/2}),\ \ell_3(Q_f) = 1;$
2. $\hat{U}(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^n).$

Блок $\vee_n^k$.

Объёмный блок $\vee_n^k$ (см. рис. 1.3), реализующий k дизъюнкций от n переменных.

Лемма 7. *Существует объёмная схема* $\vee_n^k$ *с* nk *входами* x_i^j $(i \in [n], j \in [k])$ *на* l *выходе* $(l \in [k])$ *которой реализуется функция* $y_l = x_1^l \vee x_2^l \vee \ldots \vee x_n^l$, *причём схема* $\vee_n^k$ *обладает следующими характеристиками:*

1. $\ell_1(\vee_n^k) = 1,\ \ell_2(\vee_n^k) = k,\ \ell_3(\vee_n^k) = n;$
2. $\hat{U}(\vee_n^k) = \mathcal{O}(nk).$

Доказательство. На рис. 1.3 изображена схема $\vee_n^k$, которая по столбцам собирает дизъюнкцию входов и выдает результат на соответствующий выход; при этом схема имеет требуемые характеристики. □

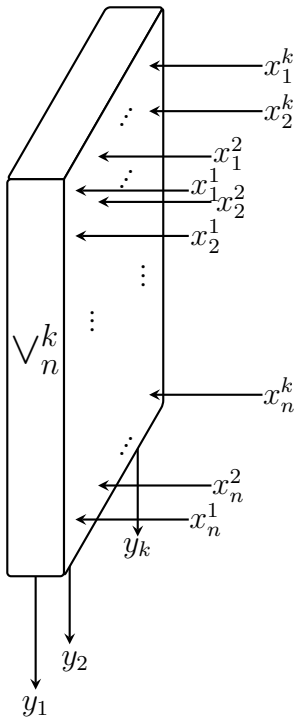


Рисунок 1.3 — Реализация блока $\bigvee_n^k$.

1.3 Реализация булевой функции

Итак, пусть дана булева функция $f(x_1, x_2, \ldots, x_n)$. Рассмотрим случай $n = 6k$. Разложим функцию f по последним $2k$ переменным:

$$f(x_1, x_2, \ldots, x_{6k}) = \bigvee_{i=0}^{2^{2k}-1} x_{4k+1}^{\bar{i}_1} x_{4k+2}^{\bar{i}_2} \ldots x_{6k}^{\bar{i}_{2k}} f_i(x_1, \ldots, x_{4k}), \tag{1.1}$$

где

$$f_i(x_1, \ldots, x_{4k}) = f(x_1, \ldots, x_{4k}, \bar{i}_1, \bar{i}_2, \ldots, \bar{i}_{2k}).$$

Для каждой функции f_i от $4k$ переменных построим вспомогательный блок $S_{f_i}^1$ (см. рис. 1.4), реализующий данную функцию. Особенностью данного блока является тот факт, что на вход ему мы подаем ему выходы из блока дешифраторов $D'_{k,4}$. Таким образом, если вход z неактивен, то потенциал всей схемы равен 4. Подробно посчитаем характеристики схемы.

Лемма 8. *Пусть дана булева функция $g(x_1, x_2, \ldots, x_{4k})$. Тогда существует объёмная схема S_g^1, такая, что схема $S_g^1 \circ D'_{k,4}$ со входами $z, x_1, x_2, \ldots, x_n$ на одном выходе на допустимых наборах $(z \geqslant x_1 \vee \ldots \vee x_n)$ реализует функцию $z \cdot g(x_1, x_2, \ldots, x_{4k})$, причём схема S_g^1 обладает следующими характеристиками:*

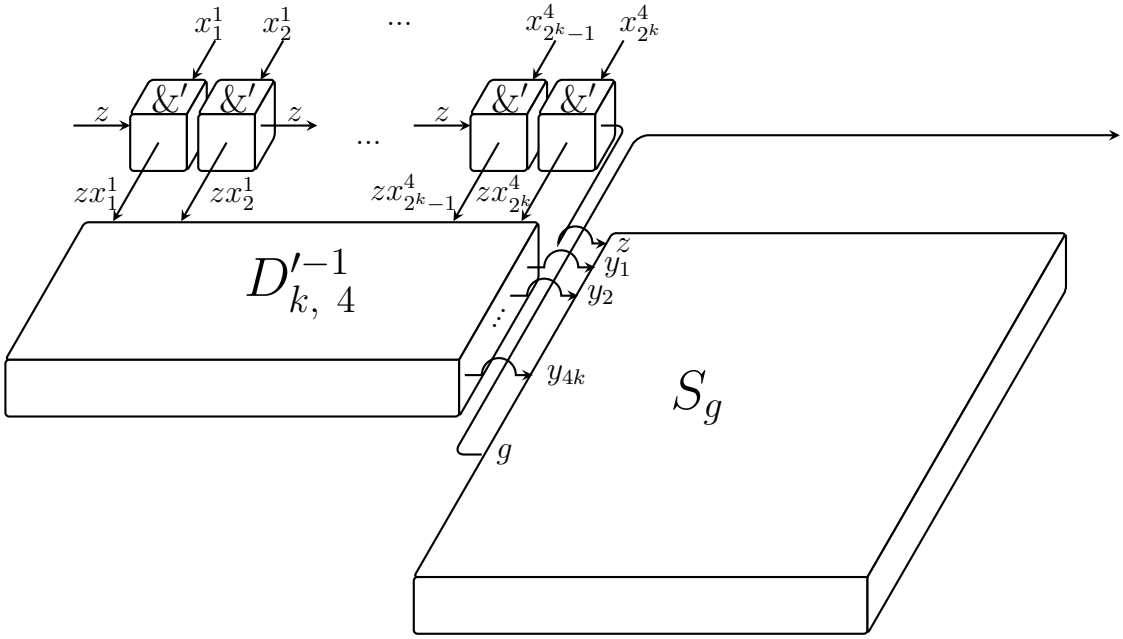


Рисунок 1.4 — Реализация блока S_g^1.

1. $\ell_1(S_g^1) = \mathcal{O}(2^{2k})$, $\ell_2(S_g^1) = \mathcal{O}(2^{2k})$, $\ell_3(S_g^1) = 1$.
2. $\hat{U}_{\{1\}\times Im(D'_{k,4})}(S_g^1) = \mathcal{O}(2^{2k})$ *и* $\hat{U}_{\{0\}\times Im(D'_{k,4})}(S_g^1) = 4$.

Доказательство. Оценим потенциал схемы S_g^1, изображенной на рис. 1.4:

$$\ell_1(S_g^1) = \ell_1(D'^{-1}_{k,4}) + 1 + \ell_2(S_g^1) = \mathcal{O}(4 \cdot 2^k) + \mathcal{O}(2^{2k}) = \mathcal{O}(2^{2k}).$$
$$\ell_2(S_g^1) = \ell_1(S_g^1) + 1 = \mathcal{O}(2^{2k}).$$
$$\ell_3(S_g^1) = 1$$

Оценим потенциал, если $z = 1$.

$$\hat{U}_{\{1\}\times Im(D'_{k,4})}(S_g^1) = \mathcal{O}(4 \cdot 2^k) + \hat{U}(D'^{-1}_{k,4}) + \ell_1(S_g^1) + \ell_2(S_g^1) + \hat{U}(S_g^1) =$$
$$= \mathcal{O}(4 \cdot 2^k) + \mathcal{O}(16k^2 \cdot 2^k) + \mathcal{O}(2^{2k}) + \mathcal{O}(2^{2k}) + \mathcal{O}(2^{2k}) = \mathcal{O}(2^{2k}).$$

□

Лемма 9. *Пусть дана булева функция $f(x_1, x_2, \ldots, x_n)$. Тогда существует объёмная схема V_f^1 со входами $z, x_1, x_2, \ldots, x_n$ на одном выходе которой на допустимых наборах $(z \geqslant x_1 \vee \ldots \vee x_n)$ реализуется функция $zf(x_1, x_2, \ldots, x_n)$, причём схема V_f^1 обладает следующими характеристиками:*

1. $\ell_1(V_f^1) = \mathcal{O}(2^{n/3})$, $\ell_2(V_f^1) = \mathcal{O}(2^{n/3})$, $\ell_3(V_f^1) = \mathcal{O}(2^{n/3})$.
2. $\hat{U}(V_f^1) = \mathcal{O}(2^{n/3})$.

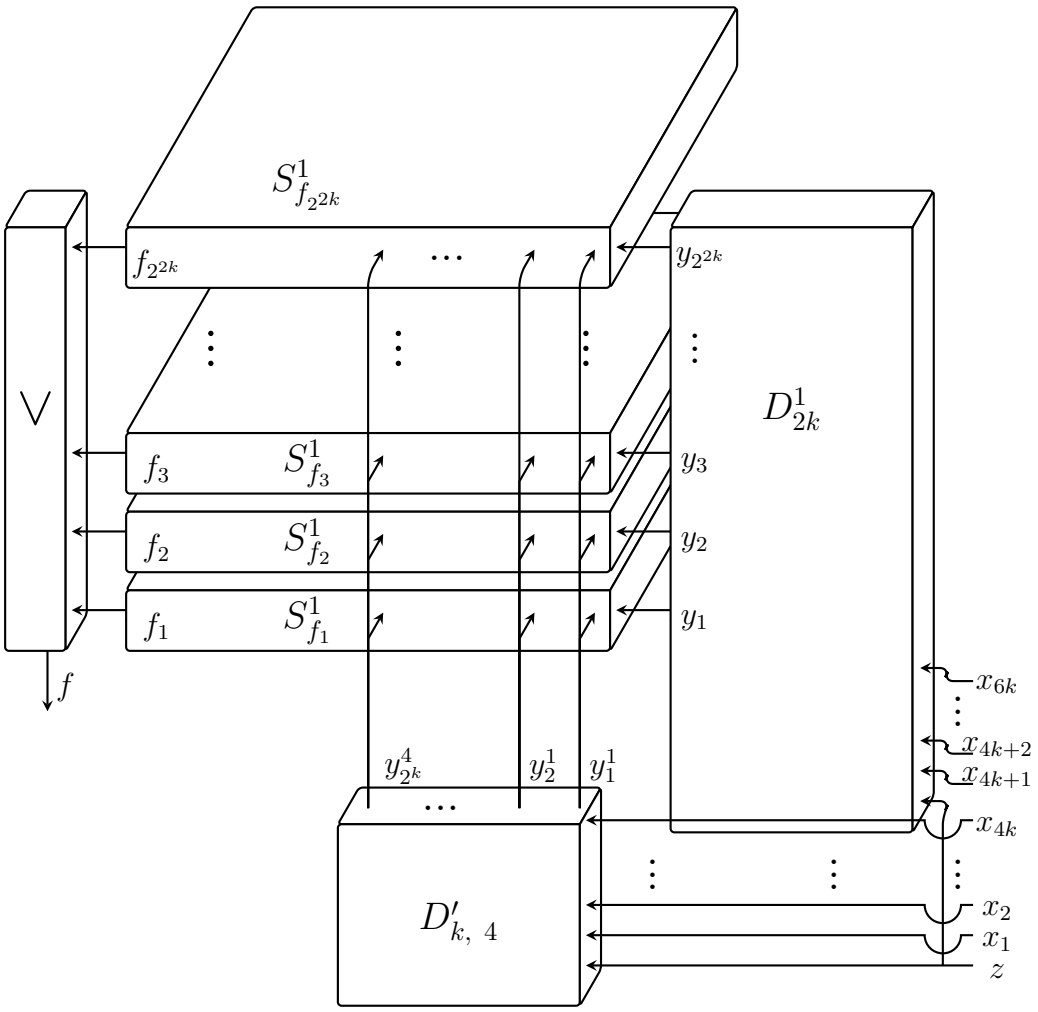


Рисунок 1.5 — Реализация основного блока V^1_f.

Доказательство. Покажем, что схема V^1_f (см. рис. 1.5) реализует функцию f согласно формуле (1.1).

Дешифратор D^1_{2k} реализует все элементарные конъюнкции

$$y_i = x^{\bar{i}_1}_{4k+1} x^{\bar{i}_2}_{4k+2} \dots x^{\bar{i}_{2k}}_{6k},$$

причем при любом значении переменных ровно один выход будет активным, а остальные нет. Это означает, что среди блоков $S^1_{f_i}$ активным будет только один. Оставшиеся переменные $x_1, \dots, x_{4k}$ отправляются на блок дешифраторов $D'_{k,4}$, где в «зашифрованном» виде отправляются на все блоки $S^1_{f_i}$. В каждом блоке $S^1_{f_i}$ они «расшифровываются», то есть преобразуются обратно в переменные $x_1, \dots, x_{4k}$, после чего реализуется функция $f_i(x_1, \dots, x_{4k})$. А так как управляющим входом в блок $S^1_{f_i}$ является $y_i = x^{\bar{i}_1}_{4k+1} x^{\bar{i}_2}_{4k+2} \dots x^{\bar{i}_{2k}}_{6k}$, то фактически на выходе блока $S^1_{f_i}$ реализуется функция

$$x^{\bar{i}_1}_{4k+1} x^{\bar{i}_2}_{4k+2} \dots x^{\bar{i}_{2k}}_{6k} f_i(x_1, \dots, x_{4k}).$$

Далее берется дизъюнкция всех выходов блоков $S^1_{f_i}$, что полностью соответствует формуле (1.1).

Оценим параметры схемы V^1_f в случае $n = 6k$.

$$\ell_1(V^1_f) = 1 + \ell_2(D^1_{2k}) + \ell_1(S^1_{f_i}) + 1 = \mathcal{O}(2^k) + \mathcal{O}(2^{2k}) = \mathcal{O}(2^{2k}).$$
$$\ell_2(V^1_f) = 1 + \ell_2(S^1_{f_i}) = \mathcal{O}(2^{2k}).$$
$$\ell_3(V^1_f) = \ell_2(D'_{k,4}) + \ell_1(D^1_{2k}) - 1 = \mathcal{O}(k^2) + \mathcal{O}(4k) + \mathcal{O}(2^{2k}) = \mathcal{O}(2^{2k}).$$

Оценим потенциал схемы. Входы $z, x_1, x_2, \dots x_{4k}$ подводим к блоку $D'_{k,4}$. Эту часть схемы оцениваем через объём.

$$U_1 \leqslant 6 \cdot (4k + 1) \cdot (\ell_2(D^1_{2k}) + 1) = \mathcal{O}(k \cdot 2^k) = \mathcal{O}(2^{2k}).$$

Оценим потенциал блока $D'_{k,4}$ по лемме 3.

$$U_2 \leqslant \hat{U}(D'_{k,4}) = \mathcal{O}(k^2 \cdot 2^k) = \mathcal{O}(2^{2k}).$$

На выходах блока $D'_{k,4}$ будут активны ровно 4 провода, подводим их к блокам $S^1_{f_i}$ и оценим потенциал.

$$U_3 \leqslant 4 \cdot \ell_1(D^1_{2k}) = \mathcal{O}(2^{2k}).$$

Подводим провода $z, x_{4k}, x_{4k+1}, \dots, x_{6k}$ к дешифратору D^1_{2k} и оценим потенциал.

$$U_4 = \mathcal{O}(2k).$$

Оценим потенциал дешифратора D^1_{2k} по лемме 2.

$$U_5 \leqslant \hat{U}(D^1_{2k}) = \mathcal{O}(2^{2k}).$$

Оценим суммарный потенциал блоков $S^1_{f_i}$. Так как среди выходов дешифратора D^1_{2k} будет активным только один, и все его выходы будут подключены к управляющим входам блоков $S^1_{f_i}$, то только 1 из блоков будет активен, а остальные $2^{2k} - 1$ по лемме 8 будут иметь потенциал 4.

Таким образом, с учётом леммы 8 имеем:

$$U_6 \leqslant 4 \cdot (2^{2k} - 1) + \hat{U}(S^1_{f_i}) = \mathcal{O}(2^{2k}).$$

Общую дизъюнкцию всех выходов $S^1_{f_i}$ оценим через объём.

$$U_7 \leqslant 6 \cdot \mathcal{O}(2^{2k}).$$

Таким образом, потенциал каждой части схемы не превосходит $\mathcal{O}(2^{2k})$. В итоге, имеем следующую оценку потенциала схемы V_f^1:

$$\hat{U}(V_f^1) = U_1 + U_2 + U_3 + U_4 + U_5 + U_6 + U_7 = \mathcal{O}(2^{2k}).$$

Таким образом, получаем верное утверждение теоремы в случае $n = 6k$. Если же $n = 6k + r$, где $r \in [5]$, то построим схему для $n = 6k + 6$ и на последние $6 - r$ входов подадим константу 0. Заметим, что в данном случае получим искомую схему и константы в оценках увеличатся не более, чем в 4 раза, а значит оценки по порядку останутся верными. □

В качестве следствия докажем основную теорему.

Теорема 1. *Пусть дана булева функция $f(x_1, x_2, \ldots, x_n)$. Тогда существует объёмная схема V_f со входами $x_1, x_2, \ldots, x_n$ на одном выходе которой реализуется функция $f(x_1, x_2, \ldots, x_n)$, причём схема V_f обладает следующими характеристиками:*

1. $\ell_1(V_f) = \mathcal{O}(2^{n/3}),\ \ell_2(V_f) = \mathcal{O}(2^{n/3}),\ \ell_3(V_f) = \mathcal{O}(2^{n/3})$.
2. $\boldsymbol{\hat{U}(V_f) = \mathcal{O}(2^{n/3}).}$
3. $V(V_f) = \mathcal{O}(2^n)$.

Доказательство. Подадим в схеме V_f^1 на вход z константу 1. Полученная таким образом схема V_f реализует функцию $f(x_1, x_2, \ldots, x_n)$ на всех наборах $x_1, x_2, \ldots, x_n$ и её параметры остаются такими же по порядку, как и у схемы V_f^1. □

1.4 Реализация булева оператора в случае $m \leqslant n$

Пусть дан булев оператор $f : \{0,1\}^n \to \{0,1\}^m$. Рассмотрим случай $n = 6k, m = 2^{12l}, m \leqslant n$. Разложим оператор f по последним $2k + 4l$ переменным:

$$f(x_1, x_2, \ldots, x_{6k}) = \bigvee_{i=0}^{2^{2k+4l}-1} x_{4k-4l+1}^{\bar{i}_1} x_{4k-4l+2}^{\bar{i}_2} \ldots x_{6k}^{\bar{i}_{2k+4l}} f_i(x_1, \ldots, x_{4k-4l}), \qquad (1.2)$$

где

$$f_i(x_1, \ldots, x_{4k-4l}) = f(x_1, \ldots, x_{4k-4l}, \bar{i}_1, \bar{i}_2, \ldots, \bar{i}_{2k+4l}).$$

Для каждого оператора f_i от $4k-4l$ переменных построим вспомогательный блок $Q^1_{f_i}$ (см. рис. 1.6, где $g = f_i$), реализующий данный оператор. Особенностью данного блока является тот факт, что на вход ему мы подаем выходы из блока дешифраторов $D'_{k-l,4}$, а выходы подсхемы Q_{f_i} мы подаем на блок дешифраторов, чтобы уменьшить потенциал проводов. Таким образом, если вход z неактивен, то потенциал всей схемы равен 4. Подробно посчитаем характеристики схемы, воспользовавшись следующей леммой, где $g = f_i$.

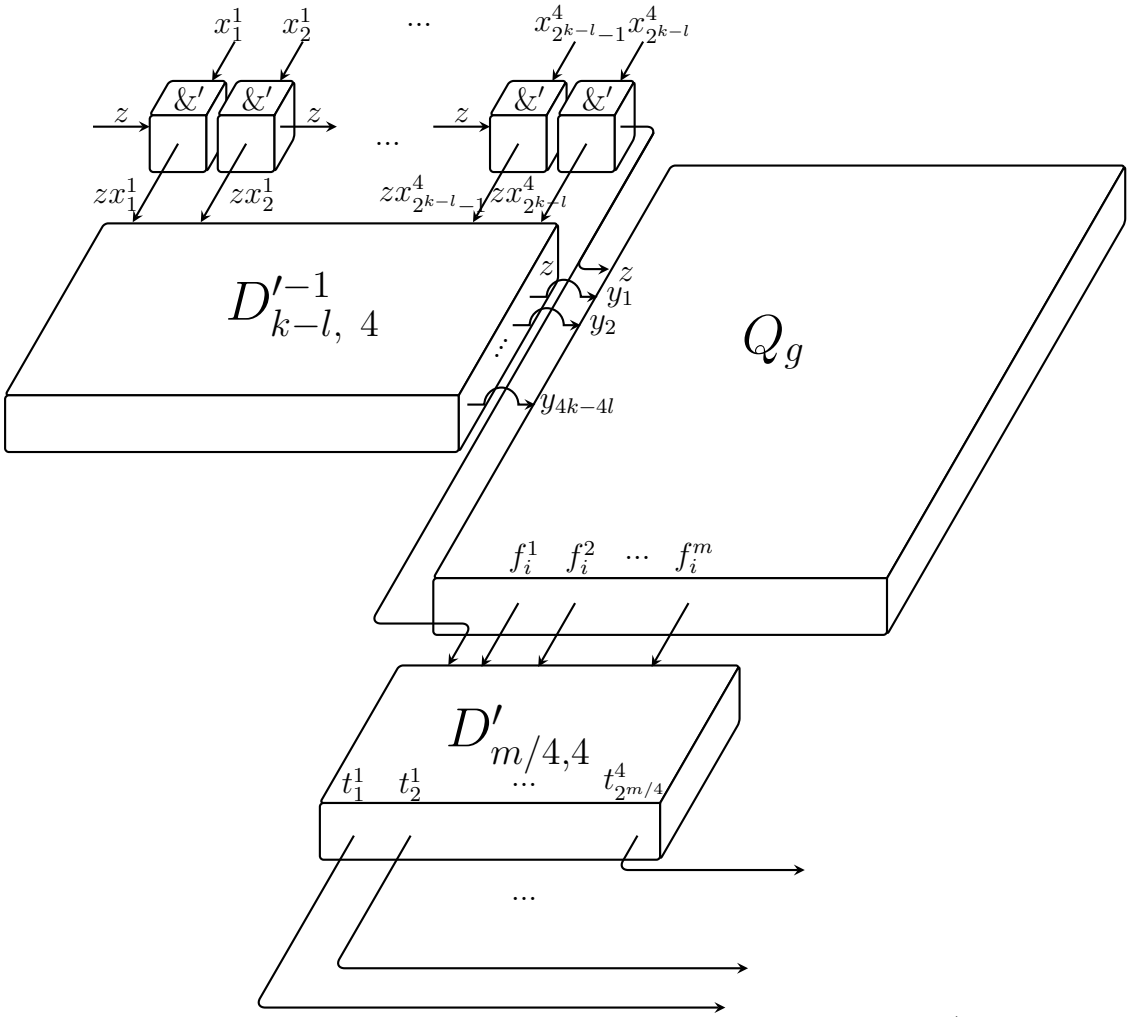


Рисунок 1.6 — Реализация блока Q^1_g.

Лемма 10. *Пусть дан булев оператор* $g : \{0,1\}^{4k-4l} \to \{0,1\}^m, n = 6k, m = 2^{12l}$, $G := Im(D'_{k-l,4})$. *Тогда существует объёмная схема* Q^1_g, *такая, что схема* $D'^{-1}_{m/4,4} \circ Q^1_g \circ D'_{k-l,4}$ *со входами* $z, x_1, x_2, \ldots, x_{4k-4l}$ *на* m *выходах реализует оператор* $g'(z,\vec{x}) = z \cdot g(\vec{x})$, *причём схема* Q^1_g *обладает следующими характеристиками:*

1. $\ell_1(Q^1_g) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $\ell_2(Q^1_g) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $\ell_3(Q^1_g) = 1$;
2. $\hat{U}_{\{1\}\times G}(Q^1_g) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $\hat{U}_{\{0\}\times G}(Q^1_g) = 4$.

Доказательство. Оценим размеры схемы Q_g^1, изображенной на рис. 1.6:

$$\ell_1(Q_g^1) = \ell_1(D_{k-l,4}^{-1}) + 1 + \ell_2(Q_g) = \mathcal{O}(4 \cdot 2^{k-l}) + \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l}) =$$
$$= \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l}) = \mathcal{O}\left(\frac{\sqrt{m} \cdot 2^{2k}}{\sqrt[6]{m}}\right) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{2k}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$
$$\ell_2(Q_g^1) = \ell_1(Q_g) + 1 + \ell_2(D'_{m/4,4}) + \mathcal{O}(4 \cdot 2^{m/4}) =$$
$$= \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l}) + \mathcal{O}(m) + \mathcal{O}(m^2/16) + \mathcal{O}(4 \cdot 2^{m/4}) =$$
$$= \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{2k}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$
$$\ell_3(Q_g^1) = 1.$$

Оценим потенциал схемы Q_g^1, если $z = 1$.

1. Оценим потенциал $4 \cdot 2^{k-l}$ блоков $\&'$:
$$U_1 \leqslant 4 \cdot 2^{k-l} \hat{U}(\&') = \mathcal{O}(2^{k-l}) = \mathcal{O}\left(\frac{2^{n/6}}{m^{1/12}}\right) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$
2. Потенциал блока $D'^{-1}_{k-l,4}$ оценим по лемме 4:
$$U_2 \leqslant \hat{U}(D'^{-1}_{k-l,4}) = \mathcal{O}(16(k-l)^2 \cdot 2^{k-l}) = \mathcal{O}\left(\left(\frac{n}{6} - \frac{\log_2 m}{12}\right)^2 \cdot \frac{2^{n/6}}{m^{1/12}}\right) =$$
$$= \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$
3. Длину управляющего провода z, вышедшего из блоков $\&'$ и подведенного к блоку $D_{k-l,4}^{-1}$ оценим через полупериметр блока Q_g по лемме 6:
$$U_3 \leqslant 6\ell_1(Q_g) + 6\ell_2(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l}) + \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l}) =$$
$$= \mathcal{O}\left(\sqrt{m} \cdot \frac{2^{n/3}}{m^{1/6}}\right) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$
4. Потенциал блока Q_g оценим по лемме 6:
$$U_4 \leqslant \hat{U}(Q_g) = \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l}) = \mathcal{O}\left(\sqrt{m} \cdot \frac{2^{n/3}}{m^{1/6}}\right) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$
5. Потенциал блока $D'_{m/4,4}$ оценим по лемме 3:
$$U_5 \leqslant \hat{U}(D'_{m/4,4}) = \mathcal{O}\left(\frac{m^2}{4} \cdot 2^{m/4}\right) + \mathcal{O}\left(4m^2 \cdot 2^{m/4}\right) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$
6. На выходе блока $D'_{m/4,4}$ будут активны только 4 провода, а значит потенциал этой области можно оценить через 4 полупериметра $4 \cdot (4 \cdot 2^{m/4} + \ell_2(Q_g))$.
$$U_6 = \mathcal{O}(4 \cdot (4 \cdot 2^{m/4} + \ell_2(Q_g))) = \mathcal{O}(2^{m/4} + \sqrt[3]{m} \cdot 2^{n/3}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

Оценим общий потенциал схемы Q_g^1:

$$\hat{U}(Q_g^1) \leqslant U_1 + U_2 + U_3 + U_4 + U_5 + U_6 = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

Если $z = 0$, то активны ровно 4 входа схемы Q_g^1, а значит потенциал $\hat{U}_{\{0\}\times G}(Q_g^1) = 4$. □

Лемма 11. *Пусть дан булев оператор $f : \{0,1\}^n \to \{0,1\}^m$, $(m \leqslant n)$. Тогда существует объёмная схема W_f^1 со входами $z, x_1, x_2, \ldots, x_n$ на m выходах которой на допустимых наборах $(z \geqslant x_1 \vee \ldots \vee x_n)$ реализуется оператор $f'(z, \vec{x}) = zf(\vec{x})$, причём схема W_f^1 обладает следующими характеристиками:*

1. $\ell_1(W_f^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $\ell_2(W_f^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $\ell_3(W_f^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$;
2. $\hat{U}(W_f^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$;
3. $V(W_f^1) = \mathcal{O}(m \cdot 2^n)$.

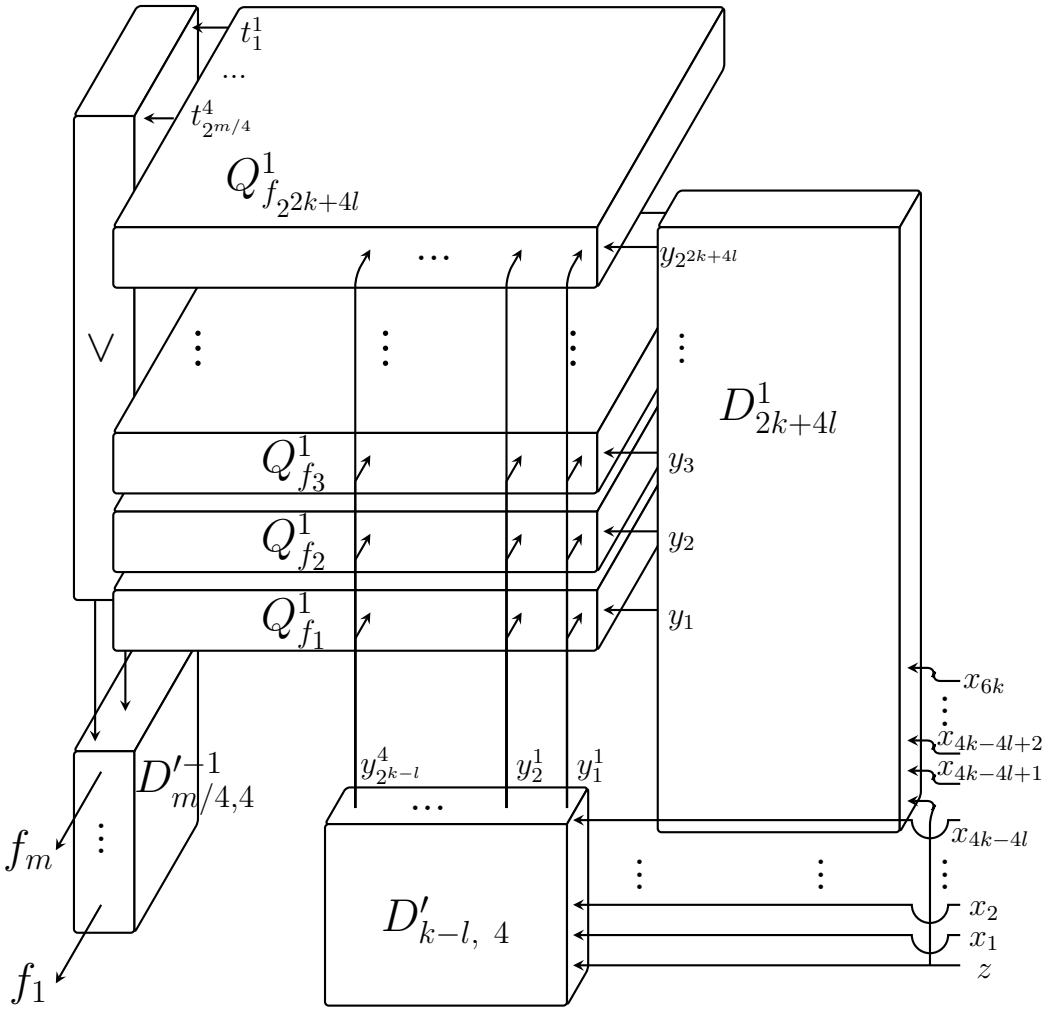


Рисунок 1.7 — Реализация основного блока W_f^1.

Доказательство. Напомним, что мы рассматриваем случай $n = 6k, m = 2^{12l}$. При этом будем строить схему при условии $m \leqslant 2^{12}n$. Покажем, что схема W_f^1 (см. рис. 1.7) реализует оператор f согласно формуле (1.2).

Дешифратор D^1_{2k+4l} реализует все элементарные конъюнкции

$$y_i = x^{\bar{i}_1}_{4k-4l+1} x^{\bar{i}_2}_{4k-4l+2} \dots x^{\bar{i}_{2k+4l}}_{6k},$$

причем при любом значении переменных ровно один выход будет активным, а остальные нет. Это означает, что среди блоков $Q^1_{f_i}$ активным будет только один. Оставшиеся переменные $x_1, \dots, x_{4k-4l}$ отправляются на блок дешифраторов $D'_{k-l,4}$, где в «зашифрованном» виде отправляются на все блоки $Q^1_{f_i}$. В каждом блоке $Q^1_{f_i}$ они «расшифровываются», то есть преобразуются обратно в переменные $x_1, \dots, x_{4k-4l}$, после чего реализуется оператор $f_i(x_1, \dots, x_{4k-4l})$. А так как управляющим входом в блок $Q^1_{f_i}$ является $y_i = x^{\bar{i}_1}_{4k-4l+1} x^{\bar{i}_2}_{4k-4l+2} \dots x^{\bar{i}_{2k+4l}}_{6k}$, то блок $Q^1_{f_i}$ реализует оператор

$$x^{\bar{i}_1}_{4k-4l+1} x^{\bar{i}_2}_{4k-4l+2} \dots x^{\bar{i}_{2k+4l}}_{6k} f_i(x_1, \dots, x_{4k-4l}).$$

Таким образом, если мы возьмем дизъюнкцию всех выходов блоков $Q^1_{f_i}$ (с помощью блока $\vee^m_{2^{2k+4l}}$, на рис. 1.7 он для удобства обозначен просто $\vee$), то получим верное значение согласно формуле (1.2). Но в таком случае мы не получим верной оценки потенциала, поэтому внутри каждого блока $Q^1_{f_i}$ мы сначала «зашифруем» выходы с помощью блока $D'^1_{m/4,4}$, а после взятия дизъюнкции «расшифруем» с помощью блока $D'^{-1}_{m/4,4}$. Поскольку при любом наборе входных переменных активным будет только один блок $Q^1_{f_i}$, то на выходе блока $\vee$ будут «зашифрованные» выходы $Q^1_{f_i}$, а значит на выходе $D^{-1}_{m/4,4}$ будут верные значения согласно формуле (1.2).

Теперь оценим параметры схемы W_f^1 в случае $n = 6k, m = 2^{12l}$.

$$\ell_1(W_f^1) = 1 + \ell_2(D^1_{2k+4l}) + \ell_1(Q^1_{f_i}) + 1 = \mathcal{O}(2^{k+2l}) + \mathcal{O}(\sqrt[3]{m} \cdot 2^{2k}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

$$\ell_2(W_f^1) = 1 + \ell_2(Q^1_{f_i}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{2k}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

$$\begin{aligned}\ell_3(W_f^1) &= \max(\ell_2(D'_{k-l,4}) + \ell_1(D^1_{2k+4l}) - 1, \ell_3(\vee) + \ell_3(D'^{-1}_{m/4,4})) = \\ &= \max(\mathcal{O}((k-l)^2 + 4(k-l)) + \mathcal{O}(2^{2k+4l}), \mathcal{O}(2^{2k+4l}) + \mathcal{O}(4m^2)) = \\ &= \mathcal{O}(2^{2k+4l}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).\end{aligned}$$

Для оценки объёма схемы $V(W_f^1)$ воспользуемся тем фактом, что для любой объёмной схемы K верно неравенство:

$$V(K) \leqslant \ell_1(K) \cdot \ell_2(K) \cdot \ell_3(K).$$

Таким образом, имеем оценку:

$$V(W_f^1) \leqslant \ell_1(W_f^1) \cdot \ell_2(W_f^1) \cdot \ell_3(W_f^1) = \mathcal{O}(m \cdot 2^n).$$

Оценим потенциал схемы.

1. Входы $z, x_1, x_2, \ldots, x_{4k-4l}$ подводим к блоку $D'_{k-l,4}$. Эту часть схемы оцениваем через объём:

$$U_1 \leqslant 6 \cdot (4k - 4l + 1) \cdot (\ell_2(D^1_{2k+4l}) + 1) = \mathcal{O}((4k - 4l + 1) \cdot 2^{k+2l}) = \\ = \mathcal{O}(2^{2k+4l}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

2. Оценим потенциал блока $D'_{k-l,4}$ по лемме 3:

$$U_2 \leqslant \hat{U}(D'_{k-l,4}) = \mathcal{O}(4 \cdot (k-l)^2 \cdot 2^{k-l}) + \mathcal{O}(16 \cdot (k-l) \cdot 2^{k-l}) = \\ = \mathcal{O}(2^{k+2l}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

3. На выходах блока $D'_{k-l,4}$ будут активны ровно 4 провода, подводим их к блокам $Q^1_{f_i}$ и оценим потенциал:

$$U_3 \leqslant 4 \cdot \ell_1(D^1_{2k+4l}) = 4 \cdot \mathcal{O}(2^{2k+4l}) = \mathcal{O}(2^{2k+4l}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

4. Подводим провода $z, x_{4k-4l}, x_{4k+1}, \ldots, x_{6k}$ к дешифратору D^1_{2k+4l} и оценим потенциал:

$$U_4 = \mathcal{O}(2k + 4l) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

5. Оценим потенциал дешифратора D^1_{2k+4l} по лемме 2:

$$U_5 \leqslant \hat{U}(D^1_{2k+4l}) = \mathcal{O}(2^{2k+4l}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

6. Так как среди выходов дешифратора D^1_{2k+4l} будет активным только один, и все его выходы будут подключены к управляющим входам блоков $Q^1_{f_i}$, то только 1 из блоков будет активен, а остальные $2^{2k+4l} - 1$ будут иметь потенциал 4, поэтому с учётом леммы 10 имеем:

$$U_6 \leqslant 4 \cdot (2^{2k+4l} - 1) + \hat{U}(Q^1_{f_i}) = \mathcal{O}(2^{2k+4l}).$$

7. Так как ровно 4 выхода одного блока $Q^1_{f_i}$ будут активны, то потенциал внутри блока $\vee$ можно оценить через объём 4 столбцов схемы $\vee$:

$$U_7 \leqslant 6 \cdot 4 \cdot \ell_3(\vee) = \mathcal{O}(2^{2k+4l}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

8. Осталось оценить потенциал блока $D'^{-1}_{m/4,4}$ по лемме 4:

$$U_8 \leqslant \hat{U}(D'^{-1}_{m/4,4}) = \mathcal{O}(m^2 \cdot 2^{m/4}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

В итоге, имеем следующую оценку потенциала схемы W^1_f:

$$\hat{U}(W^1_f) \leqslant U_1 + U_2 + U_3 + U_4 + U_5 + U_6 + U_7 + U_8 = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

Таким образом, мы доказали теорему в случае $n = 6k$, $m = 2^{12l}, m \leqslant 2^{12}n$. В общем случае, если $n = 6k + r, m = 2^{12l} + t, m \leqslant n$, где $r \in [5], t \in [2^{12(l+1)} - 2^{12l} - 1]$, то построим схему для $n' = 6k + 6, m' = 2^{12(l+1)}$ и на последние $6 - r$ входов подадим константу 0 (выполняется условие $m' \leqslant 2^{12}n'$). Заметим, что в данном случае получим искомую схему и константы в оценках увеличатся не более, чем в $16 \cdot 4 = 64$ раза, а значит оценки по порядку останутся верными. □

1.5 Реализация булева оператора в случае $m > n$

Лемма 12. *Пусть дан булев оператор $f : \{0,1\}^n \to \{0,1\}^m$, $(m > n)$. Тогда существует объёмная схема W^1_f со входами $z, x_1, x_2, \ldots, x_n$ на m выходах которой реализуется на допустимых наборах $(z \geqslant x_1 \vee \ldots \vee x_n)$ реализуется оператор $f'(z, \vec{x}) = zf(\vec{x})$, причём схема W^1_f обладает следующими характеристиками:*

1. $\ell_1(W^1_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $\ell_2(W^1_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $\ell_3(W^1_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$;
2. $\hat{U}(W^1_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$;
3. $V(W^1_f) = \mathcal{O}(m \cdot 2^n)$.

Доказательство. Рассмотрим случай, когда $n = 8t, m = kn$. Тогда определим операторы $f_i(x_1, x_2, \ldots, x_n), i \in [k]$ так, что $i \cdot n + 1, i \cdot n + 2, \ldots, (i+1) \cdot n$ выходы оператора $f(x_1, x_2, \ldots, x_n)$ являются выходами оператора $f_i(x_1, x_2, \ldots, x_n)$, т.е. имеет место равенство:

$$(f_1(\vec{x}), f_2(\vec{x}), \ldots, f_k(\vec{x})) = f(\vec{x}).$$

По лемме 11 существуют блоки $W^1_{f_i}, i \in [k]$, реализующие операторы f_i и имеющие следующие характеристики:

1. $\ell_1(W^1_{f_i}) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $\ell_2(W^1_{f_i}) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $\ell_3(W^1_{f_i}) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$;

2. $\hat{U}(W^1_{f_i}) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$;
3. $V(W^1_{f_i}) = \mathcal{O}(n \cdot 2^n)$.

Покажем, что тогда схема, изображенная на рис. 1.8 реализует оператор f.

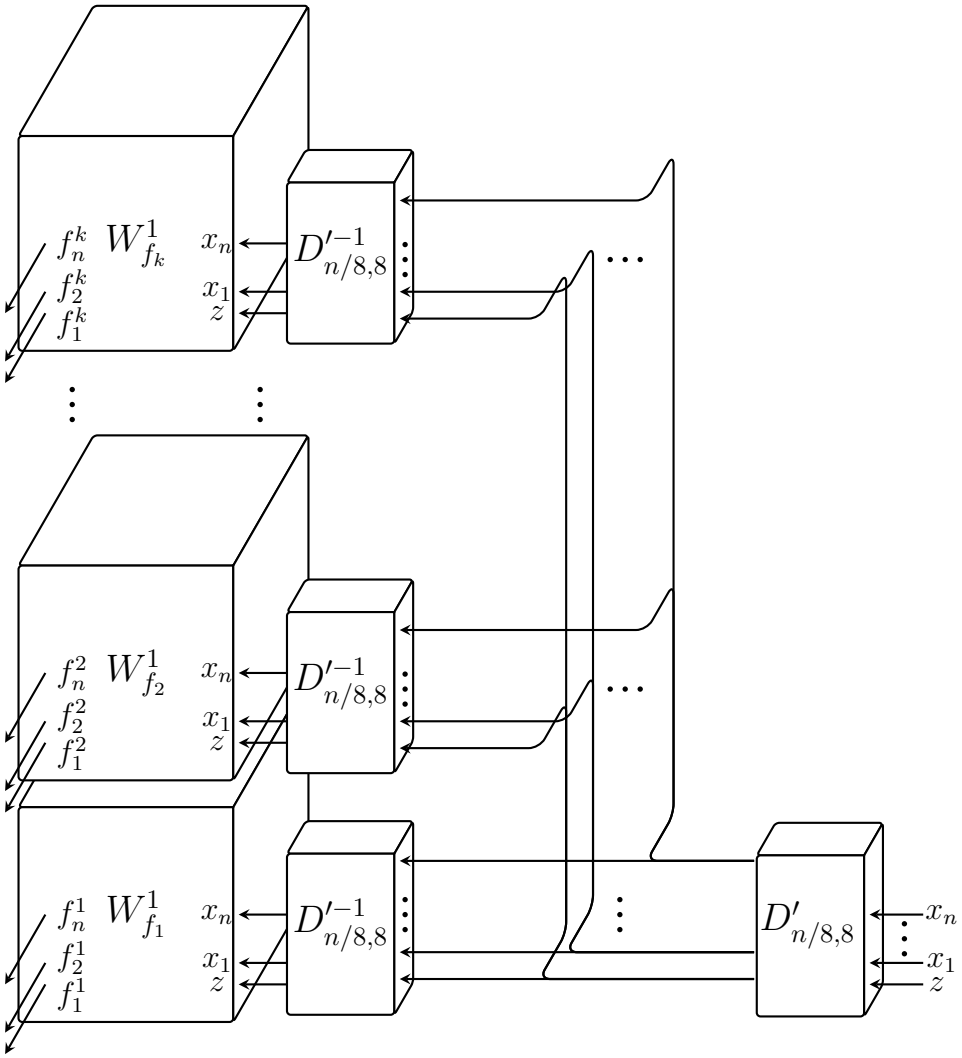


Рисунок 1.8 — Реализация основного блока W^1_f при $m > n$.

Мы подаем входные переменные $z, x_1, \ldots, x_n$ на вход блоку дешифраторов $D'_{n/8,8}$, далее все эти провода подводим к каждому из k блоков обратных дешифраторов $D'^{-1}_{n/8,8}$. «Расшифрованные» переменные $z, x_1, \ldots, x_n$ мы подаем на соответствующий блок $W^1_{f_i}$, который реализует оператор f_i от n переменных. Далее, собирая все выходы блоков $W^1_{f_i}$, получаем выходы оператора f.

Оценим параметры схемы W_f^1.

$$\begin{aligned}\ell_1(W_f^1) &= \ell_1(W_{f_i}^1) + \ell_2(D'^{-1}_{n/8,8}) + \mathcal{O}(8\cdot 2^{n/8}) + \ell_2(D'_{n/8,8}) = \\ &= \mathcal{O}(\sqrt[3]{n}\cdot 2^{n/3}) + \mathcal{O}(n^2/8) + \mathcal{O}(8\cdot 2^{n/8}) + \mathcal{O}(n^2/16+n) \\ &= \mathcal{O}(\sqrt[3]{n}\cdot 2^{n/3}).\end{aligned}$$

$$\ell_2(W_f^1) = \ell_2(W_{f_i}^1) = \mathcal{O}(\sqrt[3]{n}\cdot 2^{n/3}).$$

$$\ell_3(W_f^1) = k\cdot\ell_3(W_{f_i}^1) = \mathcal{O}\left(\frac{m}{n^{2/3}}\cdot 2^{n/3}\right) = \mathcal{O}\left(\frac{m}{n}\cdot\sqrt[3]{n}\cdot 2^{n/3}\right).$$

Аналогично доказательству из леммы 11 оценим объём схемы W_f^1:

$$V(W_f^1) \leqslant \ell_1(W_f^1)\cdot\ell_2(W_f^1)\cdot\ell_3(W_f^1) = \mathcal{O}(m\cdot 2^n).$$

Оценим потенциал схемы W_f^1.

1. Оценим потенциал блока дешифраторов $D'_{n/8,8}$ по лемме 3.

$$\begin{aligned}U_1 \leqslant \hat{U}(D'_{n/8,8}) &= \mathcal{O}(8n\cdot 2^{n/8} + n^2/8\cdot 2^{n/8}) = \mathcal{O}(n^2\cdot 2^{n/8}) = \\ &= \mathcal{O}\left(\frac{m}{n}\cdot\sqrt[3]{n}\cdot 2^{n/3}\right).\end{aligned}$$

2. Далее на выходе из блока дешифраторов $D'_{n/8,8}$ будут активны 8 проводов, которые мы подводим к блокам $D'^{-1}_{n/8,8}$. Таким образом, имеем оценку:

$$U_2 \leqslant 8\cdot(\ell_3(W_f^1) + k\cdot\mathcal{O}(8\cdot 2^{n/8})) = \mathcal{O}\left(\frac{m}{n^{2/3}}\cdot 2^{n/3}\right) = \mathcal{O}\left(\frac{m}{n}\cdot\sqrt[3]{n}\cdot 2^{n/3}\right).$$

3. Оценим потенциал всех k блоков $D'^{-1}_{n/8,8}$ по лемме 4:

$$U_3 \leqslant k\cdot\hat{U}(D'^{-1}_{n/8,8}) = k\cdot\mathcal{O}(n^2\cdot 2^{n/8}) = \mathcal{O}(mn\cdot 2^{n/8}) = \mathcal{O}\left(\frac{m}{n}\cdot\sqrt[3]{n}\cdot 2^{n/3}\right).$$

4. Оценим потенциал всех k блоков $W_{f_i}^1$ по лемме 11:

$$U_4 \leqslant k\cdot\hat{U}(W_{f_i}^1) = k\cdot\mathcal{O}(\sqrt[3]{n}\cdot 2^{n/3}) = \mathcal{O}\left(\frac{m}{n^{2/3}}\cdot 2^{n/3}\right) = \mathcal{O}\left(\frac{m}{n}\cdot\sqrt[3]{n}\cdot 2^{n/3}\right).$$

В итоге, имеем следующую оценку потенциала схемы W_f^1:

$$\hat{U}(W_f^1) \leqslant U_1 + U_2 + U_3 + U_4 = \mathcal{O}\left(\frac{m}{n}\cdot\sqrt[3]{n}\cdot 2^{n/3}\right).$$

Таким образом, получаем верное утверждение теоремы в случае $n = 8t$, $m = kn$. Если же $n = 8t+r, m = kn+l$, где $r \in [7], l \in [n-1]$, то построим схему для $n' = 8t+8, m' = (k+1)n'$ и на последние $8-r$ входов подадим константу 0. Заметим, что в данном случае получим искомую схему и константы в оценках увеличатся не более, чем в константу раз, а значит оценки по порядку останутся верными. □

В качестве следствия из леммы 11 и леммы 12 докажем основную теорему.

Теорема 2. *Пусть дан булев оператор* $f : \{0,1\}^n \to \{0,1\}^m$. *Тогда существует объёмная схема* W_f *со входами* $x_1, x_2, \ldots, x_n$ *на* m *выходах которой реализуется оператор* f, *причём схема* W_f *обладает следующими характеристиками: Если* $m \leqslant n$:

1. $\ell_1(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $\ell_2(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $\ell_3(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$.
2. $\boldsymbol{\hat{U}(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})}$.
3. $V(W_f) = \mathcal{O}(m \cdot 2^n)$.

Если $m > n$:

1. $\ell_1(W_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $\ell_2(W_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $\ell_3(W_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$.
2. $\boldsymbol{\hat{U}(W_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})}$.
3. $V(W_f) = \mathcal{O}(m \cdot 2^n)$.

Доказательство. Построим схему W_f^1, используя лемму 11 при $m \leqslant n$ или лемму 12 при $m > n$. Подадим в схеме W_f^1 на вход z константу 1. Полученная таким образом схема W_f реализует оператор $f(x_1, x_2, \ldots, x_n)$ на всех наборах $x_1, x_2, \ldots, x_n$ и его параметры остаются такими же по порядку, как и у схемы W_f^1. □

Глава 2. Нижние оценки

2.1 Метод расслоения

Для доказательства основной теоремы воспользуемся некоторыми определениями, введёнными ранее в работах Г.В. Калачёва [16], [18].

Пусть M — подсхема схемы K. Входы и выходы схемы M, не являющиеся входами и выходами схемы K, назовём *граничными контактами* подсхемы M относительно схемы K. Множество граничных контактов обозначим $(M|K)$ и будем называть *разрезом*.

Через $\mathrm{In}(M|K)$ обозначим множество входов M, которые лежат в разрезе $(M|K)$ (такие входы будем называть *граничными*), то есть

$$\mathrm{In}(M|K) = \mathrm{In}(M) \cap (M|K) = \mathrm{In}(M) \setminus \mathrm{In}(K).$$

Через $\mathrm{Out}(MK)$ обозначим множество выходов M, которые являются выходами K, то есть

$$\mathrm{Out}(MK) = \mathrm{Out}(M) \cap \mathrm{Out}(K).$$

Идея метода расслоения состоит в том, чтобы считать потенциал схемы по слоям. В работах [16], [18] выделяется множество подсхем такое, чтобы их контакты, не являющиеся контактами всей схемы, не пересекались, и оценивается снизу сумма потенциалов на контактах каждой подсхемы. В доказательстве нижней оценки для частичных операторов такой подход приводит к существенным техническим трудностям, связанным с тем, что при построении расслоения характеристики подсхем изменяются дискретно, что сильно осложняет точные оценки и ведёт к необходимости некоторых огрублений. В частности, в работе [16] из-за этого возникает дополнительный случай $\log m \succeq \sqrt{|D|}$, рассмотрение которого занимает несколько страниц и требует дополнительного ограничения на множество операторов, для которых верна оценка.

В данной работе предлагается модифицированный подход, позволяющий строить «непрерывное» расслоение. Он основан на геометрическом представлении схемы в пространстве таким образом, что элементы расположены в узлах

целочисленной решётки, а провода — отрезки, соединяющие соседние вершины. При этом если провод активен, то энергия выделяется равномерно по всей его длине. Вместо того чтобы рассматривать расслоение, в котором границей является множество проводов (контактов подсхемы), мы будем рассматривать пересечение бесконечного семейства слоёв с проводами схемы. Вместо суммирования мы будем интегрировать по элементам расслоения таким образом, чтобы потенциал каждого провода получался как интеграл по множеству слоёв, пересекающих этот провод.

Такой подход требует некоторого количества дополнительных подготовительных определений, но зато доказательство основного результата будет более прозрачным и не потребует рассмотрения дополнительных ограничений на параметры m, n и $|D|$. Перейдём к формальным определениям.

Расслоением назовём такое произвольное множество Ω подмножеств $\mathbb{R}^3$, что границы[1] различных элементов Ω не пересекаются. Границы элементов расслоения назовём *слоями*.

Если зафиксируем некоторое ребро w целочисленной решётки в $\mathbb{R}^3$, то для любого элемента расслоения $R \in \Omega$ можно определить функцию

$$I_w(R) = \begin{cases} 1, & \text{если } \partial R \cap w \neq \varnothing, \\ 0, & \text{если } \partial R \cap w = \varnothing. \end{cases} \tag{2.1}$$

Проводом схемы K будем называть отрезок, соединяющий центры соседних элементов схемы, если его середина — узел схемы K. Множество проводов схемы K обозначим через $W(K)$. Все провода являются рёбрами целочисленной решётки $\mathbb{Z}^3$. Далее нам будет удобно отождествлять узлы и соответствующие провода. В частности, разрез $(M|K)$ мы также будем понимать как множество проводов в разрезе.

Для объёмной схемы K и множества $R \subseteq \mathbb{R}^3$ через $K(R)$ обозначим подсхему, состоящую из тех элементов схемы K, центры которых попали в R. Пусть $D \subset \{0,1\}^n$. Через $U_D(\alpha)$ обозначим средний потенциал в узле α схемы K:

$$U_D(\alpha) = \frac{1}{|D|} \sum_{x \in D} g_\alpha(x),$$

где $g_\alpha(x)$ — булева функция, которая реализуется в узле α схемы K.

[1] граница ∂R множества R здесь понимается в обычном топологическом смысле

Если X — подмножество узлов схемы K, то определим $U_D(X)$:

$$U_D(X) = \sum_{\alpha \in X} U_D(\alpha).$$

В частности, если M — подсхема схемы K, то $U_D(M|K)$ — средний потенциал на граничных контактах подсхемы M, а $U_D(\mathrm{In}(M|K))$ — средний потенциал на граничных входах подсхемы M.

Лемма 13. *Рассмотрим на расслоении Ω такую σ-алгебру $\mathcal{A}$, что функции $R \mapsto I_w(R)$ измеримы для каждого w. Пусть на измеримом пространстве $(\Omega, \mathcal{A})$ введена такая мера μ, что для любого ребра w целочисленной решётки $\mathbb{Z}^3$ верно условие:*

$$\int\limits_{\Omega} I_w(R)\, d\mu(R) \leqslant C, \tag{2.2}$$

где $C > 0$ — некоторая константа. Тогда функция $U_D(K(R)|K)$ также измерима и верно следующее неравенство:

$$U_D(K) \geqslant \frac{1}{C} \int\limits_{\Omega} U_D(K(R)|K)\, d\mu(R). \tag{2.3}$$

Доказательство. Заметим, что разрез $(K(R)|K)$ состоит в точности из тех проводов схемы K, которые пересекаются со слоем ∂R. Поэтому

$$U_D(K(R)|K) = \sum_{\alpha \in W(K)} I_\alpha(R) U_D(\alpha).$$

Интегрируя по множеству слоёв и используя (2.2), получим

$$\begin{aligned} \frac{1}{C} \int\limits_{\Omega} U_D(K(R)|K)\, d\mu(R) &= \sum_{\alpha \in W(K)} U_D(\alpha) \frac{1}{C} \int\limits_{\Omega} I_\alpha(R)\, d\mu(R) \leqslant \\ &\leqslant \sum_{\alpha \in W(K)} U_D(\alpha) = U_D(K). \end{aligned}$$

□

2.2 Идея и схема доказательства

Нижнюю оценку будем доказывать следующим образом. Пусть есть класс B частичных булевых операторов, причём для каждого оператора $f \in B$ и любой схемы K, реализующей оператор f есть нижние оценки для потенциала

на границе любой подсхемы, удовлетворяющей определённым ограничениям. Тогда будем строить непрерывное расслоение $\mathfrak{R} = \mathfrak{R}(K)$ такое, что подсхемы $K(R)$ для всех $R \in \mathfrak{R}$ удовлетворяют этим ограничениям, и затем интегрировать оценку потенциала на разрезе $(K(R)|K)$ по слоям, чтобы получить оценку для всей схемы K по формуле (2.3).

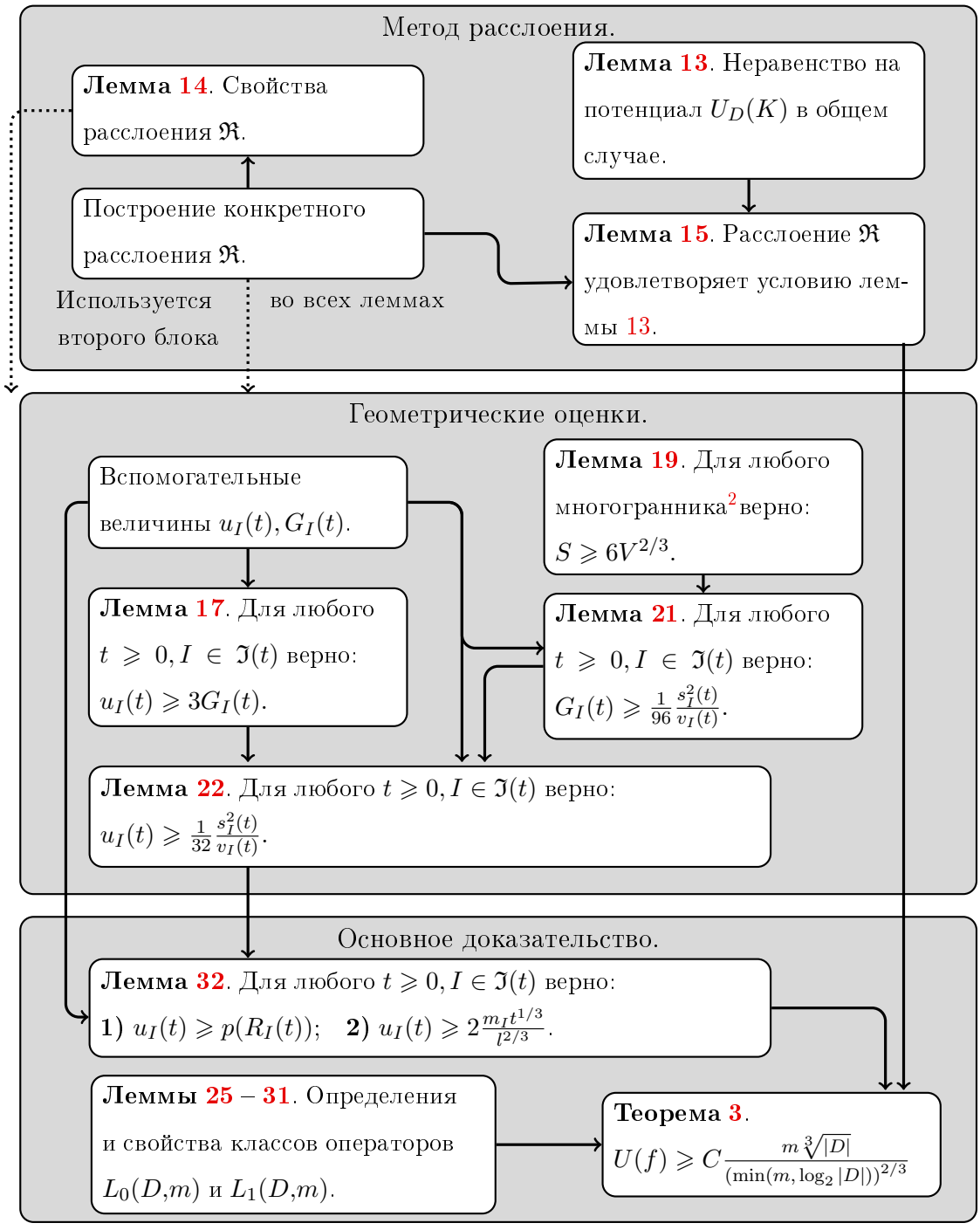


Рисунок 2.1 — Схема доказательства нижней оценки.

На рис. 2.1 изображена схема доказательства. Леммы 13–15 посвящены методу расслоения. В лемме 13 получено общее неравенство на потенциал с

[2]Многогранника с гранями, параллельными координатным плоскостям

использованием расслоения с мерой, удовлетворяющей некоторым условиям. В лемме 14 получено свойство конкретного расслоения $\mathfrak{R}$, а в лемме 15 проверено, что расслоение $\mathfrak{R}$ удовлетворяет условию леммы 13.

Геометрическим оценкам посвящены леммы 16–24. Вводим вспомогательную величину $u_I(t)$, через которую будем оценивать снизу потенциал схемы K. Для этого нам потребуется оценка из леммы 22: $u_I(t) \geqslant \frac{1}{32}\frac{s_I^2(t)}{v_I(t)}$. Но напрямую получить искомую оценку не получается, поэтому вводим величину $G_I(t)$, зависящую от длины остовного дерева некоторого взвешенного графа. Оценив $G_I(t)$ в леммах 17 и 21, получаем результат леммы 22.

Основная часть доказательства теоремы 3 состоит из лемм 25–32. В леммах 25–31 рассматриваются классы операторов $L_0(D,m)$ и $L_1(D,m)$, такие, что для любого оператора B из $L_0(D,m)$ или $L_1(D,m)$ существует реализующая их объёмная схема K и её подсхема K_0 со свойством, что на границе подсхемы K_0 имеется верхняя оценка потенциала. Показывается, что $|L_0(D,m)| = o(2^{m|D|})$ и $|L_1(D,m)| = o(2^{m|D|})$. Нижнюю оценку мы получаем для операторов из класса $P_2(D,m) \setminus L_0(D,m) \setminus L_1(D,m)$. Таким образом, для почти всех операторов на любом разрезе имеются нижние оценки на потенциал, которые определенным образом суммируются (интегрируются). В лемме 32 и теореме 3 собираются все предыдущие оценки и получается итоговый результат.

2.3 Построение непрерывного расслоения $\mathfrak{R}$

Рассмотрим произвольную объёмную схему K, имеющую n входов и m выходов. Далее в разделах 2.3 и 2.4 будем считать схему K фиксированной. Пусть в схеме имеется s элементов, к которым подключены выходы схемы, занумеруем их от 1 до s. Центры этих элементов обозначим через $c_1, \ldots, c_s$. Через m_i обозначим число выходов элемента с центром c_i, $i \in [s]$. Для произвольного $I \subseteq 2^{[s]}$ положим $m_I = \sum\limits_{i \in I} m_i$.

Формальное построение расслоения немного громоздкое, но оно имеет достаточно естественную физическую интерпретацию. Опишем неформально эту интерпретацию. Допустим, что точка c_i является источником жидкости с интенсивностью m_i. В момент $t = 0$ в пространстве нет жидкости. Начиная с момента $t = 0$ в каждую точку c_i, $i \in [s]$, начинает подаваться жидкость со скоростью

m_i, при этом каждая точка изначально окружена абсолютно эластичной плёнкой, ограничивающей жидкость. При подаче жидкости плёнка расширяется равномерно по всей поверхности, то есть скорость её расширения перпендикулярно поверхности одинаковая во всех точках поверхности. В момент, когда две плёнки касаются друг друга, они сливаются и начинают образовывать единую компоненту связности, которая дальше расширяется равномерно по всей поверхности объединения. Важным свойством этого процесса является то, что по построению в момент времени t объём компоненты связности $R_I(t)$, содержащей внутри источники c_i, $i \in I$, равен в точности $m_I \cdot t$. Это свойство является ключевым для доказательства основной теоремы.

Поскольку компоненты, расширяясь, иногда объединяются, в конечном итоге они сливаются в одну компоненту, поэтому множество элементов расслоения можно представлять в виде дерева, изображённого ниже на рисунке 2.2. С целью выполнить условие (2.2) леммы 13, меру на расслоении вводим таким образом, чтобы её плотность в каждой точке была пропорциональна скорости расширения компоненты связности расслоения, соответствующей этой точке, перпендикулярно поверхности.

На протяжении всего доказательства будем использовать метрику Чебышева ℓ_∞, где расстояние определяется как $\|\vec{x}-\vec{y}\|_\infty = \max\limits_{i=1,2,3} |x_i - y_i|$ в $\mathbb{R}^3$. Через $B(x,r)$ будем обозначать шар с центром $x \in \mathbb{R}^3$ и радиусом $r \geqslant 0$, то есть $B(x,r) = \{y \in \mathbb{R}^3 \mid \|x-y\|_\infty \leqslant r\}$.

Пусть множества $A_1, A_2 \subseteq \mathbb{R}^3$. Определим для них сумму множеств

$$A_1 + A_2 = \{x + y \mid x \in A_1, y \in A_2\}.$$

Введём $A + r := A + B(\mathbf{0}, r), A \in \mathbb{R}^3, r \in \mathbb{R}^+$.

По индукции будем строить множества $\mathfrak{I}(t) \subseteq 2^{[s]}$, $R_I(t) \subseteq \mathbb{R}^3$, $t \geqslant 0$, $I \in \mathfrak{I}(t)$, при этом последовательно определяя возрастающую последовательность $0 = t_0 < t_1 < \ldots < t_{q-1} < t_q = \infty$, на i-м шаге индукции определяя число $t_{i+1} > t_i$ и упомянутые множества при $t \in [t_i, t_{i+1})$.

База индукции. Положим

$$t_0 = 0; \qquad \mathfrak{I}(0) = \{\{1\}, \{2\}, \ldots, \{s\}\}; \qquad R_{\{i\}}(0) = \{c_i\} \text{ при } i \in [s].$$

Переход индукции. Пусть $t_0 = 0, t_1, \ldots, t_i$ образуют строго возрастающую последовательность, и для всех $t \in [0, t_i]$ определены множества $\mathfrak{I}(t) \subseteq 2^{[s]}$. Пусть также для всех $j < i$, $t \geqslant t_j$, $I \in \mathfrak{I}(t_j)$ определено множество $R_I(t) \subseteq \mathbb{R}^3$.

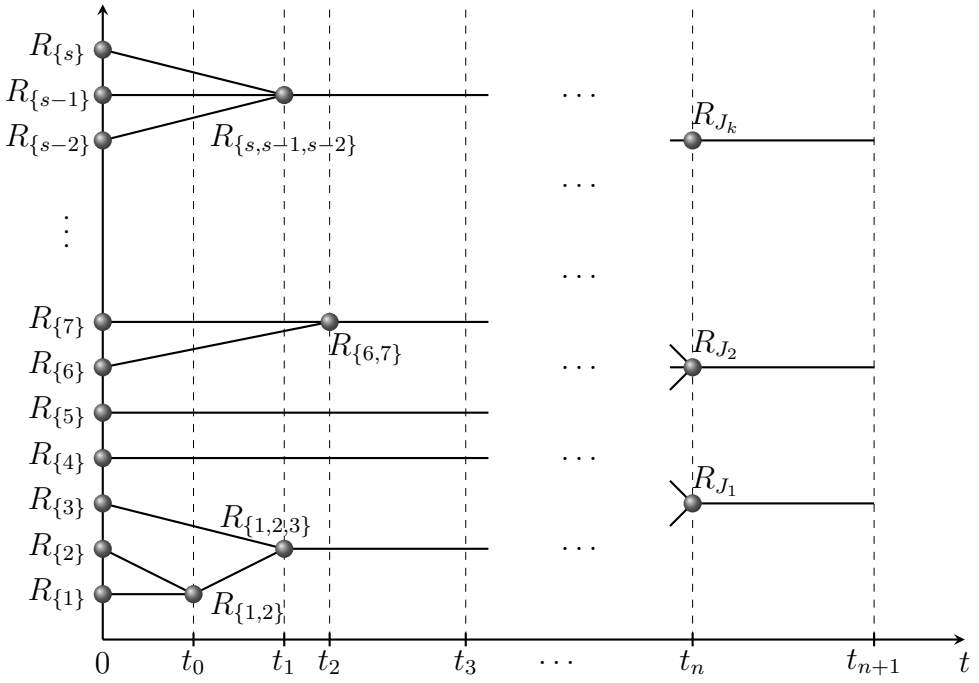


Рисунок 2.2 — Построение множеств $R_I(t)$.

На шаге индукции нам необходимо определить момент $t_{i+1} > t_i$, множества $\mathfrak{I}(t)$ при $t \in (t_i, t_{i+1})$, а также множества $R_I(t)$ для всех $I \in \mathfrak{I}(t_i) \setminus \mathfrak{I}(t_{i-1})$, $t \geqslant t_i$. В случае, если $t_{i+1} < \infty$, требуется также определить $\mathfrak{I}(t_{i+1})$.

– Рассмотрим $I \in \mathfrak{I}(t_i)$. Если $i > 0$ и $I \in \mathfrak{I}(t_{i-1})$, то $R_I(t)$ при $t \geqslant t_i > t_{i-1}$ определено по предположению индукции и выполнено $V(R_I(t_i)) = m_I t_i$. Иначе $R_I(t_i)$ было получено операцией объединения в момент t_i, либо $t_i = 0$. Поскольку функция $V(R_I(t_i) + r)$ непрерывна и строго и неограниченно возрастает по r, то для $t \geqslant t_i$, существует единственное r такое, что $V(R_I(t_i) + r) = m_I t$; обозначим его через $r_I(t)$. Определим множество $R_I(t) = R_I(t_i) + r_I(t)$ при $t \geqslant t_i$. Отметим, что равенство $V(R_I(t)) = m_I t$ выполнено по определению $r_I(t)$.

  Если $|\mathfrak{I}(t_i)| = 1$, то положим $t_{i+1} = \infty$. Иначе определим

$$t_{i+1} = \min\bigl\{t \geqslant t_i \mid \exists I,J \in \mathfrak{I}(t_i) : I \neq J \text{ и } R_I(t) \cap R_J(t) \neq \varnothing\bigr\}.$$

  Для $t \in (t_i,t_{i+1})$ положим $\mathfrak{I}(t) = \mathfrak{I}(t_i)$.

– Если $t_{i+1} = \infty$, то завершим построение. Иначе, пусть $t = t_{i+1}$.

  Заметим, что существуют такие $l \geqslant 1$ групп индексов $I^j_1, I^j_2, \ldots, I^j_{k_j} \in \mathfrak{I}(t_i)$, $j \in [l]$, что множества $R_{I^j_1}(t), R_{I^j_2}(t), \ldots, R_{I^j_{k_j}}(t)$ попарно не имеют общих точек при $t < t_{i+1}$, а при $t = t_{i+1}$ образуют одну компоненту связности. Положим

$$J^j = I^j_1 \cup I^j_2 \cup \ldots \cup I^j_{k_j}, \quad R_{J^j}(t) = R_{I_1}(t) \cup \ldots \cup R_{I^j_{k_j}}(t), \quad j \in [l]$$

В таком случае будем говорить, что множество $R_{J^j}(t)$ получено из множеств $R_{I_1^j}(t), \ldots, R_{I_{k_j}^j}(t)$ *операцией объединения*. Также определим

$$\mathfrak{I}(t_{i+1}) := (\mathfrak{I}(t_i) \setminus \bigcup_{j=1}^{l} \{I_1^j, I_2^j, \ldots, I_{k_j}^j\}) \cup \{J^1, \ldots, J^l\}.$$

В качестве расслоения будем рассматривать $\mathfrak{R} = \{R_I(t) \mid t \geqslant 0, I \in \mathfrak{I}(t)\}$.

В доказательстве будем также использовать несколько дополнительных обозначений. Нетрудно видеть, что множество $R_I(t)$ является многогранником, поэтому его объём и площадь поверхности определены. Через $v_I(t)$ будем обозначать объём множества $R_I(t)$, а через $s_I(t)$ — площадь поверхности $R_I(t)$.

Обозначим $\mathfrak{I} = \bigcup\limits_{t \geqslant 0} \mathfrak{I}(t)$. Для фиксированного $I \in \mathfrak{I}$ введём числа

$$a_I = \min\{t \geqslant 0 \mid I \in \mathfrak{I}(t)\}, \qquad b_I = \sup\{t \geqslant 0 \mid I \in \mathfrak{I}(t)\}$$

(если $I = [s]$, то $b_I = \infty$, иначе b_I конечно). Заметим, что $I \in \mathfrak{I}(t)$ тогда и только тогда, когда $t \in [a_I, b_I)$.

Нам также понадобится объединение множеств $R(t) = \bigcup\limits_{I \in \mathfrak{I}(t)} R_I(t)$. Введём подсхемы $M_I(t) = K(R_I(t))$, и $M(t) = K(R(t))$.

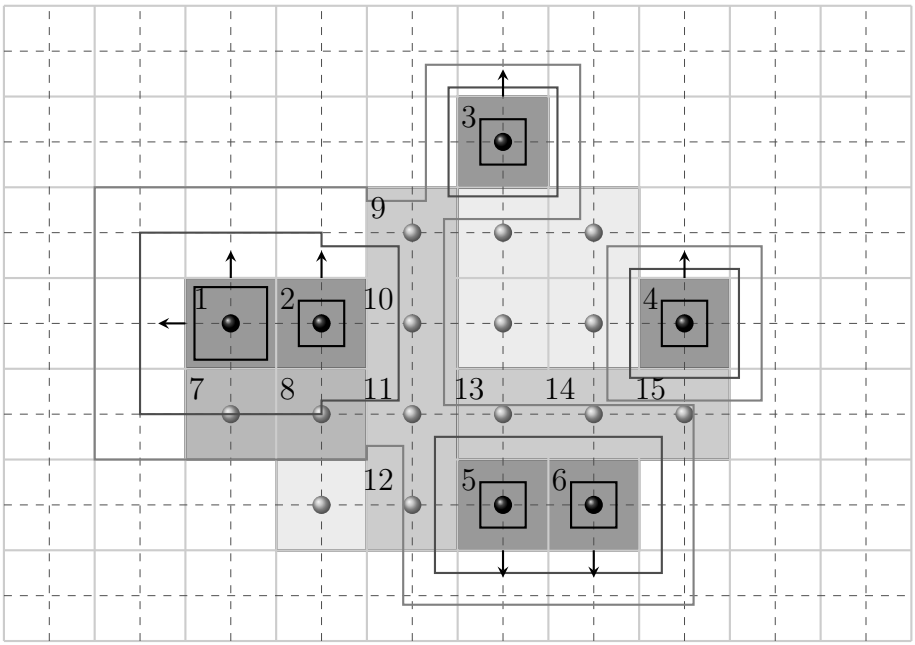


Рисунок 2.3 — Построение $M(t)$.

Опишем процесс построения подсхемы $M(t)$ на примере плоской схемы (на рис. 2.3 центры обозначены точками, выходы — стрелками). Сплошные серые линии — это границы элементов, пересечения пунктирных линий — это

центры элементов. Отрезки пунктирных линий, соединяющие центры соседних элементов, — это провода схемы. Сплошными линиями обозначены границы некоторых множеств 1–6 из $R(t')$ при некотором $t' > 0$; элементы 1–6 принадлежат подсхеме $M(t')$. Более светлыми сплошными линиями обозначены границы некоторых множеств 7–8 из $R(t'')$ при некотором $t'' > t'$; элементы 7–8 принадлежат подсхеме $M(t'')$, но не входят в подсхему $M(t')$, то есть те элементы, которые добавляются в $M(t)$ при $t = t''$ по сравнению с $t = t'$. Аналогично, самыми светлыми сплошными линиями обозначены границы некоторых множеств 9–15 из $R(t''')$ при некотором $t''' > t''$; элементы 9–15 принадлежат подсхеме $M(t''')$, но не входят в подсхему $M(t'')$.

Пусть $A \in \mathbb{R}^3$. Через $\ell_1(A), \ell_2(A), \ell_3(A)$ обозначим соответственно длину, ширину и высоту стягивающего прямоугольного параллелепипеда[3] для множества A и положим

$$p(A) := \sum_{i=1}^{3} \ell_i(A).$$

Построим меру ρ для расслоения $\mathfrak{R}$, которое можно параметризовать точками дерева (см. рис. 2.2). Естественная σ-алгебра на дереве индуцирует σ-алгебру на $\mathfrak{R}$. Рёбра дерева индексируются элементами множества $\mathfrak{I}$. Положим $\mathfrak{R}_I = \{R_I(t) \mid t \in [a_I, b_I)\}$; это множество соответствует ребру с индексом I в дереве $\mathfrak{R}$. Тогда $\mathfrak{R} = \bigsqcup\limits_{I \in \mathfrak{I}} \mathfrak{R}_I$. Поскольку множество $\mathfrak{R}_I$ является образом промежутка $[a_I,b_I)$, на нём определена мера Лебега-Стилтьеса ρ_I с функцией распределения $p_I(t) = p(R_I(t))$, $t \in [a_I, b_I)$. В частности,

$$\rho_I(\{R_I(t) \mid t \in [x,y)\}) = p(R_I(y)) - p(R_I(x)),\ a_I \leqslant x < y \leqslant b_I.$$

Поскольку функция p_I строго возрастает, то мера ρ_I положительная. Кроме того, поскольку p_I непрерывна, то мера любого конечного подмножества $\mathfrak{R}_I$ равна нулю. Меру ρ на множестве $\mathfrak{R}$ введём так, чтобы она совпадала с ρ_I на подмножестве $\mathfrak{R}_I$ для всех $I \in \mathfrak{I}$. А именно, если $X \subseteq \mathfrak{R}$ измеримо, то

$$\rho(X) = \sum_{I \in \mathfrak{I}} \rho_I(X \cap \mathfrak{R}_I).$$

Сформулируем в виде леммы некоторые дополнительные свойства построенного расслоения $\mathfrak{R}$. Пусть $B(x,r) = \{y \in \mathbb{R}^3 \mid \|x - y\|_\infty \leqslant r\}$.

[3]Наименьший прямоугольный параллелепипед с рёбрами, параллельными осями координат и содержащий множество A

Лемма 14. *Для любого $t > 0$ выполнено:*

1. $\bigsqcup\limits_{I\in\mathfrak{I}(t)} I = [s]$, *т.е.* $\mathfrak{I}(t)$ *задаёт некоторое разбиение множества* $[s]$.
2. *Существуют числа* $r_i(t)$, $i \in [s]$ *такие, что для всех* $I \in \mathfrak{I}(t)$ *множество* $R_I(t)$ *является объединением шаров*

$$R_I(t) = \bigcup_{i\in I} B(c_i,r_i(t)).$$

3. *Шары* $B(c_i,r_i(t))$ *для различных* i *не вложены друг в друга, т.е.*

$$\|c_i - c_j\|_\infty + r_i(t) - r_j(t) > 0 \quad при \quad i,j \in [s], i \neq j.$$

Кроме того, если $a_I \leqslant x \leqslant y \leqslant b_I$, *то для всех* $i \in I$ *выполнено*

$$p(R_I(y)) - p(R_I(x)) = 6(r_i(y) - r_i(x)).$$

Доказательство. Упорядочим элементы множества $\{a_I \mid I \in \mathfrak{I}\}$ по возрастанию и обозначим их $t_0 = 0, t_1, t_2, \ldots, t_q$. Докажем свойства 1)–3) индукцией по i, $t \in [t_i, t_{i+1})$.

База индукции. Пусть $t \in [0, t_1)$.

1. Так как $\mathfrak{I}(t) = \{\{1\}, \{2\}, \ldots, \{s\}\}$, то элементы $\mathfrak{I}(t)$ не пересекаются, и

$$\bigsqcup_{I\in\mathfrak{I}(t)} I = \bigsqcup_{i=1}^{s}\{i\} = [s].$$

2. Каждое множество $R_{\{i\}}(t) = B(c_i, r_{\{i\}}(t)), i \in [s]$, положим в этом случае $r_i(t) = r_{\{i\}}(t)$.
3. Заметим, что условие $\|c_i - c_j\|_\infty + r_i(t) - r_j(t) > 0$ означает, что расстояние между центрами шаров больше разности радиусов $r_j(t) - r_i(t)$, что эквивалентно тому, что $B(c_i, r_i(t)) \not\subseteq B(c_j, r_j(t))$.

   В данном случае, так как все шары $B(c_i, r_i(t))$ не пересекаются, то они не вложены друг в друга.

Переход индукции. Пусть $t \in [t_i, t_{i+1})$. Заметим, что по построению тогда существует $l \geqslant 1$ таких групп индексов $I_1^j, I_2^j, \ldots, I_{k_j}^j \in \mathfrak{I}(t_i)$, $j \in [l]$, что множество $R_{I_1^j \cup I_2^j \cup \ldots \cup I_{k_j}^j}(t_i)$ получено из множеств $R_{I_1^j}(t_i)$, $R_{I_2^j}(t_i)$, …, $R_{I_{k_j}^j}(t_i)$ операцией объединения. Обозначим $J^j = I_1^j \cup I_2^j \cup \ldots \cup I_{k_j}^j$, $j \in [l]$.

1. Тогда $\mathfrak{I}(t) = \mathfrak{I}(t_{i-1}) \setminus \bigcup_{j=1}^{l}\{I_1^j, I_2^j, \ldots, I_{k_j}^j\} \cup \{J^1, \ldots, J^l\}$. По предположению индукции верно

$$\bigsqcup_{I\in\mathfrak{I}(t_{i-1})} I = [s].$$

Учитывая определение J^j, получаем

$$\bigcup_{I\in\mathfrak{I}(t)} I = \bigcup_{I\in\mathfrak{I}(t_{i-1})} I \setminus \Big(\bigcup_{j=1}^{l}\bigcup_{l=1}^{k_j} I_l^j\Big) \cup \Big(\bigcup_{j=1}^{l} J^j\Big) = [s].$$

Покажем, что $\forall A, B \in \mathfrak{I}(t_i)$ верно $A \cap B = \varnothing$. Если $A \neq J^j, B \neq J^j$, то $A, B \in \mathfrak{I}(t_{i-1})$, значит по предположению индукции верно $A \cap B = \varnothing$. Пусть без ограничения общности $B = J^j$. Тогда по предположению индукции $A \cap I_z^j = \varnothing, z \in [k_j]$, а значит $A \cap J^j = \varnothing$.

2. Для всех $j \in [l]$ верно

$$R_{J^j}(t_i) = \bigcup_{z=1}^{k_j} R_{I_z^j}(t_i) = \bigcup_{z=1}^{k_j}\bigcup_{v\in I_z^j} B(c_v, r_v(t_i)) = \bigcup_{z\in J^j} B(c_z, r_z(t_i)).$$

При $t \in (t_i, t_{i+1})$ получаем

$$R_{J^j}(t) = R_{J^j}(t_i) + r_{J^j}(t) = \bigcup_{z\in J^j} B(c_z, r_z(t_i) + r_{J^j}(t)), \quad j \in [q].$$

Если $I \in \mathfrak{I}(t), a_I \neq t_i$, то выполняется равенство

$$R_I(t) = R_I(a_I) + r_I(t) = \bigcup_{j\in I} B(c_j, r_j(a_I) + r_I(t)) \quad \text{при} \quad t \in [a_I, b_I].$$

3. Если $i \in I, j \in J, I \neq J$, то шары $B(c_i, r_i(t))$ и $B(c_j, r_j(t))$ не пересекаются, а значит и не вложены друг в друга.
Рассмотрим случай $i, j \in I$. Так как $R_I(t) = \bigcup\limits_{v\in I} B(c_v, r_v(a_I) + r_I(t))$ при $t \in [a_I, b_I]$, то

$$r_i(t) = r_i(a_I) + r_I(t), \quad r_j(t) = r_j(a_I) + r_I(t), \quad t \in [a_I, b_I].$$

Так как по предположению индукции верно

$$\|c_i - c_j\|_\infty + r_i(a_I) - r_j(a_I) > 0,$$

То имеем при $t \in [a_I, b_I]$

$$\|c_i - c_j\|_\infty + r_i(t) - r_j(t) = \|c_i - c_j\|_\infty + r_i(a_I) + r_I(t) - r_j(a_I) - r_I(t) > 0.$$

Докажем последний пункт леммы 14. По определению R_I и r_i выполнено

$$R_I(x) = R_I(a_I) + r_I(x), \qquad R_I(y) = R_I(a_I) + r_I(y),$$
$$r_i(x) = r_i(a_I) + r_I(x), \qquad r_i(y) = r_j(a_I) + r_I(y).$$

Поскольку при расширении множества A на r, его проекция на каждое направление увеличивается на $2r$, то

$$\ell_v(A + r) = \ell_v(A) + 2r, \quad v = 1, 2, 3.$$

Таким образом, имеем

$$p(R_I(y)) - p(R_I(x)) = \sum_{v=1}^{3} (\ell_v(R_I(a_I) + r_I(y)) - \ell_v(R_I(a_I) + r_I(x))) = \\ = 6(r_I(y) - r_I(x)) = 6(r_i(y) - r_i(x)).$$

□

С учётом последнего пункта леммы 14, для $x,y \in [a_I,b_I]$ можно определить величину $\Delta r_I(x,y)$ такую, что

$$r_i(y) - r_i(x) = \Delta r_I(x,y) \text{ для всех } i \in I. \tag{2.4}$$

Покажем, что мера ρ удовлетворяет неравенству (2.2).

Лемма 15. *Пусть $\mathfrak{R}$ — построенное выше расслоение. Тогда для любого ребра w целочисленной решетки $\mathbb{Z}^3$ верно неравенство:*

$$\int_{\mathfrak{R}} I_w(R)\, d\rho(R) \leqslant 6. \tag{2.5}$$

Доказательство. Зафиксируем ребро w. Пусть $A \in \mathfrak{R}$. Обозначим $\lambda(A)$ длину $w \cap A$. Тогда на множестве $\mathfrak{R}_I$ определена мера λ_I с функцией распределения $\lambda(R_I(t))$ при $t \in [a_I, b_I)$.

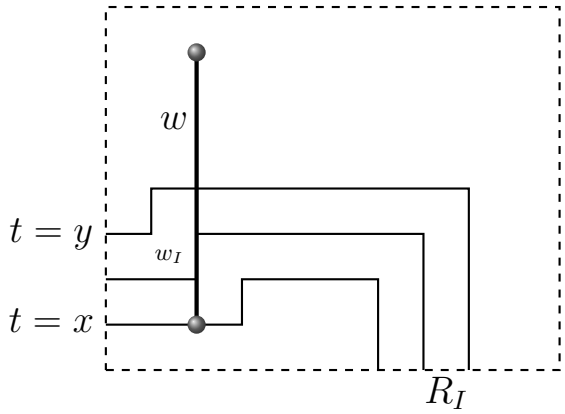


Рисунок 2.4 — К доказательству леммы 15.

Докажем, что если $a_I \leqslant x < y < b_I, I_w(R_I(x)) = I_w(R_I(y)) = 1$ (см. рис. 2.4), то верно

$$p(R_I(y)) - p(R_I(x)) \leqslant 6\left(\lambda(R_I(y)) - \lambda(R_I(x))\right). \tag{2.6}$$

Заметим, что

$$p(R_I(y)) - p(R_I(x)) = \sum_{i=1}^{3} \left(\ell_i(R_I(y)) - \ell_i(R_I(x))\right) = 6(r_I(y) - r_I(x)) \leqslant$$
$$\leqslant 6\left(\lambda(R_I(y)) - \lambda(R_I(x))\right).$$

Обозначим w_I ту часть отрезка w, которая пересекается со слоем $\partial R_I(t), t \in [a_I, b_I)$. Отметим, что при $I \neq J \in \mathfrak{I}$ верно $w_I \cap w_J = \varnothing$, так как слои в расслоении $\mathfrak{R}$ не пересекаются. В таком случае в силу неравенства (2.6) имеем

$$\int\limits_{\mathfrak{R}_I} I_w(R)\, d\rho(R) = \int\limits_{a_I}^{b_I} I_w(R_I(t))\, dp(R_I(t)) \leqslant$$
$$\leqslant 6 \int\limits_{a_I}^{b_I} I_w(R_I(t))\, d\lambda(R_I(t)) = 6|w_I|.$$

Таким образом, имеем

$$\int\limits_{\mathfrak{R}} I_w(R)\, d\rho(R) = \sum_{I\in\mathfrak{I}} \int\limits_{\mathfrak{R}_I} I_w(R)\, d\rho(R) \leqslant \sum_{I\in\mathfrak{I}} 6|w_I| \leqslant 6|w| = 6.$$

□

Таким образом, по лемме 13 для меры ρ и расслоения $\mathfrak{R}$ имеет место неравенство, полученное из неравенства (2.3):

$$U_D(K) \geqslant \frac{1}{6} \int\limits_{\mathfrak{R}} U_D(M|K)\, d\rho(R). \tag{2.7}$$

2.4 Геометрические оценки

Для множества $I \subseteq [s]$ рассмотрим полный взвешенный граф с вершинами в точках c_i, $i \in I$, где вес ребра $\{c_i, c_j\}$ равен $w(\{c_i, c_j\}) = \|c_i - c_j\|_\infty$,

то есть расстоянию между точками c_i и c_j (напомним, что c_i — центр i-го выходного элемента схемы). Пусть T — некоторое остовное дерево этого графа с множеством рёбер $E(T)$. Через $w(T)$ обозначим сумму весов его рёбер. Введём также величину $G_I^T(t)$:

$$G_I^T(t) = w(T) + \sum_{i \in I} (2 - \deg_T(c_i)) r_i(t),$$

где $\deg_T(c)$ — степень вершины c в дереве T. В основном нас будет интересовать величина $G_I(t) = \min\limits_T G_I^T(t)$, где минимум берётся по всем остовным деревьям T. Из (2.4) для всех $I \in \mathfrak{I}(t)$ следует, что

$$G_I^T(t) = G_I^T(a_I) + \Delta r_I(a_I, t) \sum_{i \in I} (2 - \deg_T(c_i)) = G_I^T(a_I) + 2\Delta r_I(a_I, t),$$

поскольку сумма степеней вершин в дереве с $|I|$ вершинами равна $2|I| - 2$. Значит для фиксированного $I \in \mathfrak{I}$ можно выбрать дерево T_I, на котором будет достигаться минимум при всех $t \in [a_I, b_I)$, причём

$$G_I(t) = G_I(a_I) + 2\Delta r_I(a_I, t) \quad \text{при} \quad t \in [a_I, b_I). \tag{2.8}$$

Для каждого $I \in \mathfrak{I}$ и $t \in [a_I, b_I]$ определим величину $u_I(t)$:

$$u_I(t) = \sum_{J \in \mathfrak{I} : J \subseteq I} \int_{a_J}^{\min(b_J, t)} \max\left(\frac{m_J}{l}, 1\right) dp(R_J(t)). \tag{2.9}$$

Нам понадобятся следующие свойства величины $u_I(t)$, следующие непосредственно из определений.

Лемма 16. *Для любого $t \geqslant 0$ и $I \in \mathfrak{I}(t)$ верно:*

1. *$u_I(0) = 0$ для всех $I \in \mathfrak{I}(0)$.*
2. *Если $t = a_I > 0$, то множество $R_I(t)$ получено операцией объединения из некоторых множеств $R_{J_1}(t), R_{J_2}(t), \ldots, R_{J_k}(t)$ в момент времени t, в этом случае $u_I(t) = u_{J_1}(t) + u_{J_2}(t) + \ldots + u_{J_k}(t)$.*
3. *Если $t \in [a_I, b_I]$, то*

$$u_I(t) = u_I(a_I) + \int_{a_I}^{t} \max\left(\frac{m_I}{l}, 1\right) dp(R_I(t)).$$

Доказательство. Обозначим $\alpha_J = \max(\frac{m_J}{l}, 1)$, $p_J = p(R_J(t))$ для краткости. По определению u_I имеем:

1. $u_I(0) = \sum\limits_{J\in\mathfrak{I}:J\subseteq I} \int\limits_0^{\min(b_J,0)} \alpha_J\, dp_J(t) = 0.$
2. Так как $I = J_1 \cup J_2 \cup \ldots \cup J_k$, то при $t = a_I$

$$u_I(t) = \sum_{J\in\mathfrak{I}:J\subseteq I} \int_{a_J}^{\min(b_J,t)} \alpha_J\, dp_J(t) =$$

$$= \underbrace{\int_{a_I}^{\min(b_I,t)} \alpha_I\, dp_I(t)}_{=0} + \sum_{i=1}^{k} \underbrace{\sum_{J\in\mathfrak{I}:J\subseteq J_i} \int_{a_J}^{\min(b_J,t)} \alpha_J\, dp_J(t)}_{=u_{J_i}(t)} = \sum_{i=1}^{k} u_{J_i}(t).$$

3. Пусть $t \in [a_I, b_I]$. По пункту 1 леммы 14 элементы $\mathfrak{I}(t')$ не пересекаются при $t' \geqslant 0$, значит $b_J \leqslant a_I \leqslant t$ для всех $J \subsetneq I$, поэтому

$$u_I(t) = \sum_{J\in\mathfrak{I}:J\subseteq I} \int_{a_J}^{\min(b_J,t)} \alpha_J\, dp_J(t) =$$

$$= \sum_{J\in\mathfrak{I}:J\subsetneq I} \int_{a_J}^{\min(b_J,a_I)} \alpha_J\, dp_J(t) + \int_{a_I}^{\min(b_I,t)} \alpha_I\, dp_I(t) =$$

$$= u_I(a_I) + \int_{a_I}^{t} \alpha_I\, dp_I(t).$$

□

Заметим, что поскольку интегрируется константа, то

$$u_I(t) = u_I(a_I) + \max\left(\frac{m_I}{l}, 1\right)(p(R_I(t)) - p(R_I(a_I))). \tag{2.10}$$

С учётом леммы 14, для всех $i \in I$ выполнено

$$u_I(t) = u_I(a_I) + 6\max\left(\frac{m_I}{l}, 1\right)(r_i(t) - r_i(a_I)). \tag{2.11}$$

Используя (2.4), это можно переписать также в виде

$$u_I(t) = u_I(a_I) + 6\max\left(\frac{m_I}{l}, 1\right)\Delta r_I(a_I, t). \tag{2.12}$$

Лемма 17. *Для любого $t \geqslant 0$ и $I \in \mathfrak{I}(t)$ верна оценка:*

$$u_I(t) \geqslant 3G_I(t).$$

Доказательство. Будем строить рассуждения индукцией по мощности множества I.

База индукции: $|I| = 1$ (множество $R_I(t)$ состоит из одного шара). Тогда $I = \{i\}$ для некоторого $i \in [s]$ и $I \in \mathfrak{I}(0)$, значит $a_I = 0$. Тогда из (2.11) получим:

$$u_I(t) = u_I(0) + 6\max\left(\frac{m_I}{l},1\right)(r_i(t) - r_i(0)) \geqslant 6r_i(t).$$

Поскольку в дереве T_I всего одна вершина c_i, поэтому $w(T_I) = 0$, $\deg c_i = 0$, значит

$$G_I(t) = T_I + (2 - \deg_{T_I}(c_i))r_i(t) = 2r_i(t) \leqslant \frac{1}{3}u_I(t).$$

Шаг индукции: $|I| > 1$. Предположим, что условие леммы выполнено для всех $J \in \mathfrak{I}$ мощности $|J| < |I|$. Поскольку I фиксировано, для краткости обозначим $a = a_I$.

Сначала покажем, что $u_I(a) \geqslant G_I(a)$. Поскольку $|I| > 1$, то $I \notin \mathfrak{I}(0)$, значит $a = a_I > 0$, то есть a — момент объединения. Без ограничения общности считаем, что $R_I(a) = R_{I_1}(a) \cup R_{I_2}(a)$ (см. рис. 2.5), иначе проделаем операцию несколько раз, последовательно добавляя элементы.

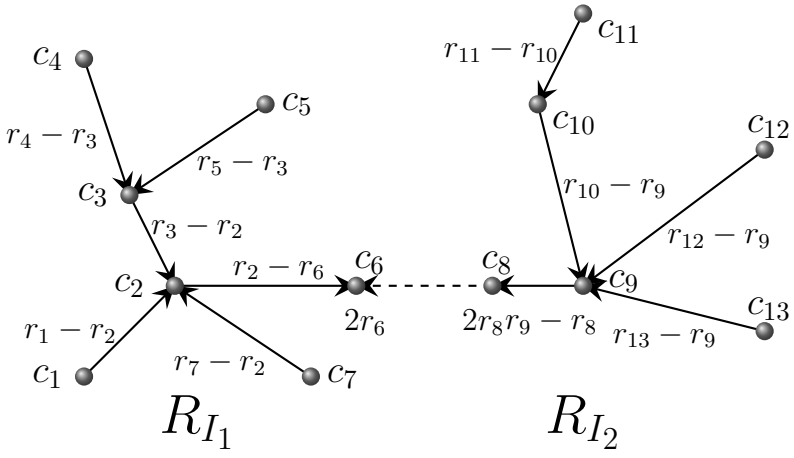


Рисунок 2.5 — Операция объединения.

По лемме 14 множества $R_{I_1}(a)$, $R_{I_2}(a)$ представляются в виде объединения шаров:

$$R_{I_1}(a) = \bigcup_{i\in I_1} B(c_i, r_i(a)), \qquad R_{I_2}(t) = \bigcup_{i\in I_2} B(c_i, r_i(a)).$$

Отметим, что если множества $R_{I_1}(a)$ и $R_{I_2}(a)$ коснулись в точке, которая принадлежит шарам $B(c_{j_1}, r_{j_1}(a))$ и $B(c_{j_2}, r_{j_2}(a))$, то длина ребра равна $w(\{c_{j_1}, c_{j_2}\}) = \|c_{j_1} - c_{j_2}\|_\infty = r_{j_1}(a) + r_{j_2}(a)$. Рассмотрим дерево T, полученное соединением деревьев T_{I_1} и T_{I_2} ребром $\{c_{j_1}, c_{j_2}\}$. Формально, дерево

T является графом с множеством вершин $\{c_i \mid i \in I\}$ и множеством рёбер $E(T) = E(T_{I_1}) \cup E(T_{I_2}) \cup \{\{c_{j_1}, c_{j_2}\}\}$.

Покажем, что $G_I^T(a) = G_{I_1}(a) + G_{I_2}(a)$. Заметим, что степени всех в дереве T, кроме c_{j_1} и c_{j_2}, совпадают со степенями соответствующих вершин в деревьях T_{I_1} и T_{I_2}, а $\deg_T(c_{j_k}) = \deg_{T_{I_k}}(c_{j_k}) + 1$ при $k = 1{,}2$.

$$G_I^T(t) - G_{I_1}(t) - G_{I_2}(t) = w(T) - w(T_{I_1}) - w(T_{I_2}) + \\ + \sum_{k=1}^{2} \sum_{i \in I_k} (\deg_{T_{I_k}}(c_i) - \deg_T(c_i)) r_i(t) = w(\{c_{j_1}, c_{j_2}\}) - \sum_{k=1}^{2} r_{j_k}(t) = 0.$$

Поскольку $|I_1| \leqslant |I| - 1$, $|I_2| \leqslant |I| - 1$ и $a = b_{I_1} = b_{I_2}$, то по предположению индукции имеем:

$$u_{I_1}(a) \geqslant 3G_{I_1}(a), \qquad u_{I_2}(a) \geqslant 3G_{I_2}(a).$$

Таким образом, получаем оценку:

$$u_I(a) = u_{I_1}(a) + u_{I_2}(a) \geqslant 3G_{I_1}(a) + 3G_{I_2}(a) = 3G_I^T(a) \geqslant 3G_I(a). \tag{2.13}$$

Пусть $t \in [a_I, b_I]$, тогда, применяя (2.12), затем (2.13) и (2.8), получим:

$$u_I(t) = u_I(a_I) + 6 \max\left(\frac{m_I}{l}, 1\right) \Delta r_I(a_I, t) \geqslant \\ \geqslant u_I(a_I) + 6\Delta r_I(a_I, t) \geqslant 3(G_I(a_I) + 2\Delta r_I(a_I, t)) = 3G_I(t),$$

что и требовалось. □

Лемма 18. *Для любого измеримого ограниченного множества A выполнено*

$$p(A) \geqslant 3(V(A))^{1/3}.$$

Доказательство. Пусть P — стягивающий параллелепипед для множества A. Тогда по определению p и по неравенству средних выполнено

$$p(A) = \sum_{i=1}^{3} \ell_i(P) \geqslant 3\sqrt[3]{\ell_1(P) \cdot \ell_2(P) \cdot \ell_3(P)} = 3\sqrt[3]{V(P)}.$$

Поскольку $A \subseteq P$, то $V(A) \leqslant V(P)$, отсюда следует утверждение леммы. □

Лемма 19 (Изопериметрическое неравенство)**.** *Пусть $A \subseteq \mathbb{R}^3$ — произвольный многогранник с гранями, параллельными координатным плоскостям. Тогда верна следующая оценка:*

$$S \geqslant 6 \cdot V^{2/3},$$

где S — площадь поверхности множества A, V — объём A.

Доказательство.

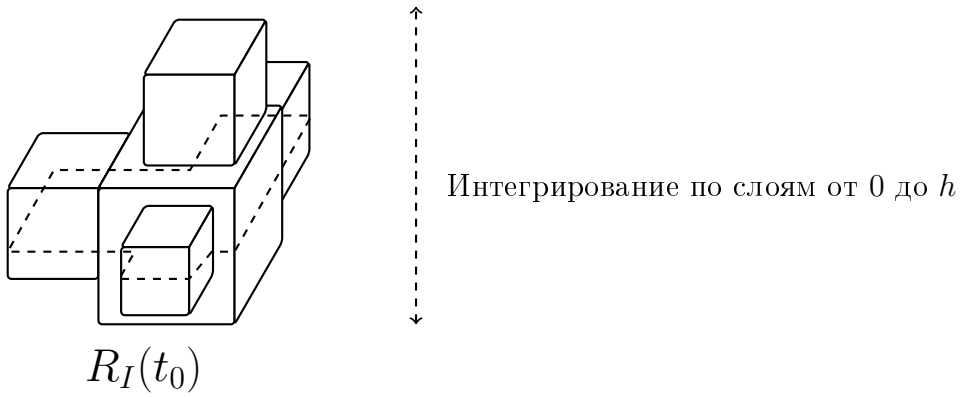


Рисунок 2.6 — Оценка площади боковой поверхности через объём.

Искомую оценку получим, используя аналогичный результат в плоскости и интегрируя его по слоям (см. рис. 2.6). Обозначим $w(x), x \in [0; h]$ длину границы слоя (x — параметр, указывающий высоту слоя), $s(x)$ — площадь слоя. Также обозначим $s_{max} = \max\limits_{x \in [0;h]} s(x)$. Тогда площадь горизонтальных граней множества A не меньше $2s_{\max}$. Выражая площадь вертикальных граней и объём множества A через интеграл, получим:

$$S \geqslant \int\limits_0^h w(x)dx + 2s_{\max},\ V = \int\limits_0^h s(x)dx.$$

Существует аналог искомого утверждения для плоского случая, который был показан в работе [18, стр.20, лемма 11]:

$$w(x) \geqslant 4\sqrt{s(x)}.$$

Используя данное неравенство и неравенство средних, получаем:

$$S \geqslant \int\limits_0^h w(x)dx + 2s_{max} \geqslant \int\limits_0^h 4\sqrt{s(x)}dx + 2s_{max} =$$
$$= 2\left(\int\limits_0^h \sqrt{s(x)}dx + \int\limits_0^h \sqrt{s(x)}dx + s_{max}\right) \geqslant$$
$$\geqslant 6\sqrt[3]{\left(\int\limits_0^h \sqrt{s(x)}dx\right)^2 \cdot s_{max}} = 6\sqrt[3]{\left(\int\limits_0^h \sqrt{s(x) \cdot s_{max}}dx\right)^2} \geqslant$$
$$\geqslant 6\sqrt[3]{\left(\int\limits_0^h s(x)dx\right)^2} = 6V^{2/3}.$$

□

По лемме 14 множество $R_I(t)$ является объединением шаров в метрике l_∞. Шар в метрике l_∞ является кубом с гранями, параллельными координатным плоскостям, а значит $R_I(t)$ является многогранником с гранями, параллельными координатным плоскостям. Таким образом, по лемме 19 имеем

$$s_I(t) \geqslant 6 \cdot (v_I(t))^{2/3}.$$

Нам понадобится следующая простая лемма

Лемма 20. *Для любых* $a,b \in \mathbb{R}$ *выполнено неравенство:*

$$(a-b)(a^3-b^3) \geqslant \frac{3}{4}(a^2-b^2)^2.$$

Доказательство. Вычтем из левой части неравенства правую часть, домножим на 4 и преобразуем:

$$4(a-b)(a^3-b^3) - 3(a^2-b^2)^2 =$$
$$= 4(a-b)^2(a^2+ab+b^2) - 3(a-b)^2(a+b)^2 =$$
$$= (a-b)^2(4a^2+4ab+4b^2-3(a+b)^2) =$$
$$= (a-b)^4 \geqslant 0.$$

□

Лемма 21. *Для любого $t \geqslant 0$ и $I \in \mathfrak{I}(t)$ верна следующая оценка:*

$$G_I(t) \geqslant \frac{1}{96} \cdot \frac{s_I^2(t)}{v_I(t)},$$

где $s_I(t)$ — площадь поверхности $R_I(t)$, $v_I(t)$ — объём $R_I(t)$.

Доказательство. Поскольку параметр t в данной лемме фиксирован, то далее будем его опускать для упрощения обозначений.

По лемме 14 множество R_I является объединением шаров, а значит верно равенство $R_I(t) = \bigcup\limits_{i \in I} B(c_i, r_i)$.

Для доказательства нам понадобится по индукции собирать множество $R_I(t)$ из шаров, поэтому введём такие вспомогательные вложенные множества $J_1 \subseteq J_2 \subseteq \cdots \subseteq J_{|I|} = I$, а также для $k \in [|I|]$ определим множество

$$A_k = \bigcup_{i \in J_k} B(c_i, r_i)$$

и граф T_k — подграф T_I с множеством вершин $\{c_i \mid i \in J_k\}$. Множества J_k построим так, чтобы T_k было деревом с k вершинами, причём $T_{|I|} = T_I$ и T_{k-1} получалось из T_k удалением одного листа для $k \in [|I|] \setminus \{1\}$.

По индукции покажем, что

$$G_{J_k}^{T_k} \geqslant \frac{1}{96} \cdot \frac{S^2(A_k)}{V(A_k)}.$$

База индукции: $k = 1$, тогда $J_1 = \{j\}$ для некоторого $j \in I$ и A_1 является шаром с радиусом r_j, поэтому

$$G_j = 2r_j, \quad S(A_1) = 24r_j^2, \quad V(A_1) = 8r_j^3.$$

Подставим в правую часть:

$$\frac{1}{96} \cdot \frac{S(A_1)^2}{V(A_1)} = \frac{1}{96} \cdot \frac{24^2 r_j^4}{8r_j^3} = \frac{3}{4} r_j.$$

Таким образом, неравенство верно при $k = 1$.

Переход индукции. Пусть $k < |I|$ и $J_{k+1} = J_k \cup \{j\}$, причём c_j является листом в дереве T_{k+1}. Пусть c_i — та вершина T_k, к которой присоединён лист c_j, $d = w(\{c_i, c_j\})$ — вес ребра, присоединяющего лист c_j к поддереву T_k. Для краткости обозначим

$$\begin{aligned} S &= S(A_k), & V &= V(A_k), & G &= G_{J_k}^{T_k}, \\ S' &= S(A_{k+1}), & V &= V(A_{k+1}), & G &= G_{J_{k+1}}^{T_{k+1}}. \end{aligned}$$

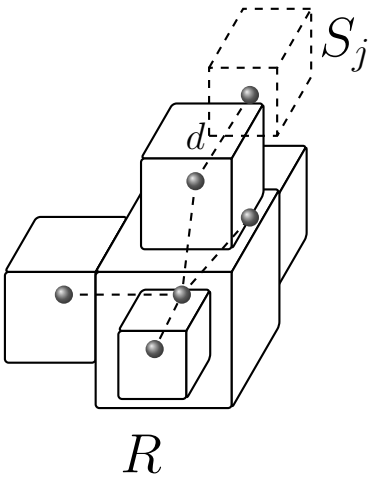


Рисунок 2.7 — Переход индукции.

По предположению индукции имеем:

$$G \geqslant \frac{1}{96} \cdot \frac{S^2}{V}. \tag{2.14}$$

Докажем, что:

$$G' \geqslant \frac{1}{96} \cdot \frac{S'^2}{V'}. \tag{2.15}$$

Также обозначим $\Delta G = G' - G$, $\Delta S = S' - S$, $\Delta V = V' - V$. Напомним, что по определению $A_{k+1} = A_k \cup B(c_j, r_j)$. Нетрудно убедиться, что выполнены равенства:

$$\Delta G = d + r_j - r_i, \quad \Delta S = 24r_j^2 - s, \quad \Delta V = 8r_j^3 - v, \tag{2.16}$$

где s и v — соответственно площадь поверхности и объём $A_k \cap B(c_j,r_j)$.

Заметим, что неравенство (2.15) равносильно:

$$(G + \Delta G)(V + \Delta V) \geqslant \frac{1}{96} \cdot (S + \Delta S)^2. \tag{2.17}$$

Докажем вспомогательное неравенство:

$$\Delta G \cdot \Delta V \geqslant \frac{1}{96}(\Delta S)^2. \tag{2.18}$$

Сначала оценим ΔG снизу, а именно, покажем, что

$$\Delta G \geqslant r_j - \frac{1}{2}v^{1/3}, \tag{2.19}$$

1. Если $r_i \leqslant d$, то $\Delta G = d - r_i + r_j \geqslant r_j$, и (2.19) выполнено.

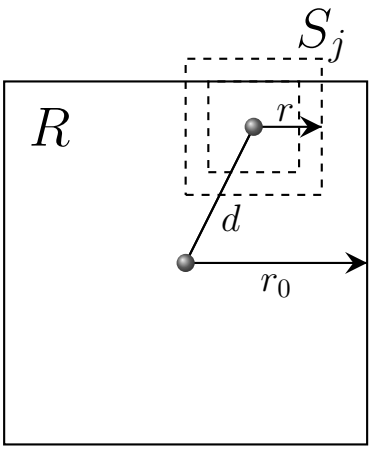


Рисунок 2.8 — Переход индукции при $d \leqslant r_i$.

2. Рассмотрим случай $r_i > d$. По лемме 14 шар $B(c_j, r_j)$ не вложен в шар $B(c_i, r_i)$. Тогда заметим, что множество $A_k \cap B(c_j, r_j)$ содержит пересечение $B(c_i, r_i) \cap B(c_j, r_j)$, внутри которого помещается шар радиуса $r_i - d$ (см. рис. 2.8).

   Таким образом, имеет место неравенство $v \geqslant (2(r_i - d))^3$, а значит $r_i - d \leqslant \frac{1}{2}v^{1/3}$, значит (2.19) выполнено.

Используя (2.19), (2.16), затем лемму 20 при $a = 2r_j$, $b = v^{1/3}$, получим

$$\Delta G \cdot \Delta V \geqslant \left(r_j - \frac{1}{2}v^{1/3}\right)(8r_j^3 - v) \geqslant \frac{3}{8}(4r_j^2 - v^{2/3})^2. \tag{2.20}$$

Применяя лемму 19 для множества $A_k \cap B(c_j, r_j)$, имеем $s \geqslant 6v^{2/3}$, значит с учётом (2.20) получим

$$\frac{1}{96}\Delta S^2 = \frac{1}{96}(24r_j^2 - s)^2 \leqslant \frac{1}{96}(24r_j^2 - 6v^{2/3})^2 = \frac{3}{8}(4r_j - v^{2/3})^2 \leqslant \Delta G \cdot \Delta V.$$

Таким образом, вспомогательное неравенство (2.18) доказано. Используя его, докажем основное неравенство (2.17):

$$(G + \Delta G)(V + \Delta V) \geqslant \frac{1}{96} \cdot (S + \Delta S)^2$$

$$G \cdot V + \Delta G \cdot V + \Delta V \cdot G + \Delta G \cdot \Delta V \geqslant \frac{1}{96}(S^2 + 2S \cdot \Delta S + (\Delta S)^2)$$

По неравенству (2.14) имеем:

$$G \cdot V \geqslant \frac{1}{96}S^2. \tag{2.21}$$

Далее по неравенству средних и из неравенств (2.21),(2.18) следует:

$$\Delta G \cdot V + \Delta V \cdot G \geqslant 2\sqrt{G \cdot V \cdot \Delta V \cdot \Delta G} \geqslant \frac{1}{96}(2S \cdot \Delta S). \tag{2.22}$$

Таким образом, сложив неравенства (2.21), (2.18) и (2.22), получим требуемое неравенство (2.17). □

В качестве прямого следствия из лемм 17 и 21 получаем утверждение:

Лемма 22. *Для любого $t \geqslant 0$, $I \in \mathfrak{I}(t)$ верна следующая оценка:*

$$u_I(t) \geqslant \frac{1}{32} \cdot \frac{s_I^2(t)}{v_I(t)},$$

где $s_I(t)$ — площадь поверхности $R_I(t)$, $v_I(t)$ — объём $R_I(t)$.

Также имеет место следующее соотношение:

Лемма 23. *Для любого множества $I \in \mathfrak{I}$, $t \in (a_I,b_I)$ верно равенство:*

$$v_I'(t) = \frac{1}{6} s_I(t) p_I'(t),$$

где $s_I(t)$ — площадь поверхности $R_I(t)$, $v_I(t)$ — объём $R_I(t)$.

Доказательство. По определению производной с учётом леммы 14 имеем:

$$\begin{aligned} v_I'(t_0) &= \lim_{t \to t_0} \frac{v_I(t) - v_I(t_0)}{t - t_0} = \lim_{t \to t_0} \frac{v_I(t) - v_I(t_0)}{\Delta r_I(t_0, t)} \cdot \frac{\Delta r_I(t_0, t)}{t - t_0} = \\ &= \frac{1}{6} \lim_{t \to t_0} \frac{v_I(t) - v_I(t_0)}{\Delta r_I(t_0, t)} \cdot \frac{p_I(t) - p_I(t_0)}{t - t_0} = \frac{1}{6} s_I(t_0) p_I'(t_0). \end{aligned}$$

□

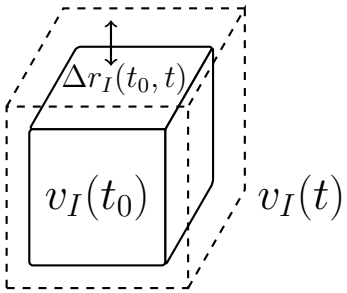


Рисунок 2.9 — Расширение множества $R_I(t)$.

Лемма 24. *Для любого $t \geqslant 0$, $I \in \mathfrak{I}(t)$ верно следующее утверждение:*

$$V(M_I(t)) \leqslant 8V(R_I(t)) + m_I.$$

Доказательство. Заметим, что множество $M_I(t)$ состоит из $|I|$ кубических элементов, в которых находятся выходы схемы K (на рис. 2.10 центры этих элементов обозначены черными точками) и оставшихся элементов (их центры обозначены серыми точками). Объём кубических элементов с выходами схемы K равен $|I| \leqslant m_I$. Объём оставшихся элементов не больше $8V(R_I(t))$, так как если кубический элемент $s \in M_I(t)$, то центр s находится в $R_I(t)$, а значит пересечение с множеством $R_I(t)$ занимает не менее $1/8$ части s. Таким образом, получаем требуемую оценку. □

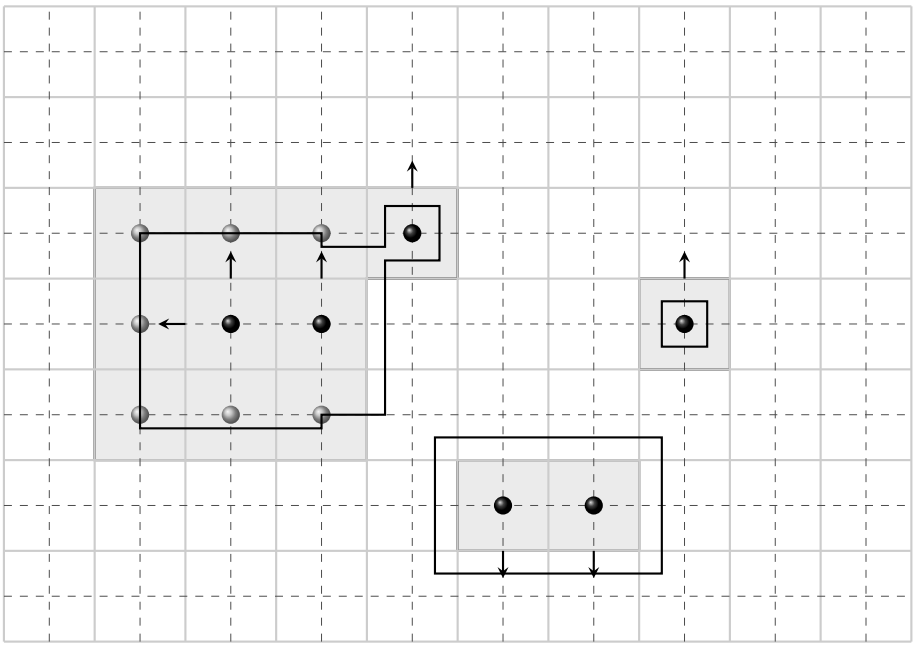


Рисунок 2.10 — Оценка $V(M_I(t))$.

2.5 Общие оценки

В данном параграфе обобщим некоторые результаты для плоских схем, полученные в работе [18], на объёмные схемы. Доказательство всех лемм аналогично и отличается лишь заменой некоторых констант, которые будут явно указаны ниже и никак не влияют на идею рассуждений.

Определение: Здесь и всюду далее будем полагать, что $D \subseteq \{0,1\}^n$. Пусть $d = |D|, h \geqslant 1$. Обозначим за $P_u(D,h)$ множество таких операторов

$G : D \to \{0,1\}^h$, что

$$\frac{1}{d}\sum_{x\in D}|G(x)| \leqslant u.$$

Лемма 25. *(Калачёв Г.В., [18, лемма 1]) Если $u \leqslant h$, то*

$$\log_2 |P_u(D,h)| \leqslant du \log_2 \frac{eh}{u}.$$

Лемма 26. *Количество различных кубических элементов равно* $C_1 = 90\ 537\ 043\ 409$.

Доказательство. У кубического элемента может быть от 0 до 5-ти входов. Рассмотрим каждый из случаев.

1. В этом случае каждая из 6-ти граней либо изолятор, либо реализует константу (то есть 3 варианта для каждой грани). Всего $3^6 = 729$ кубических элементов.
2. Есть 6 расположений входа. Каждая из оставшихся граней либо изолятор, либо реализует функцию от одной переменной (всего 5 вариантов для каждой стороны), причем все 5 оставшихся граней не могут одновременно быть изоляторами. Поэтому элементов $6 \cdot (5^5 - 1) = 18\ 744$.
3. Есть $\binom{2}{6} = 15$ вариантов расположений входов. Каждая из оставшихся граней либо изолятор, либо реализует функцию от двух переменных (всего $2^{2^2} + 1 = 17$ вариантов для каждой стороны), причем все 4 оставшиеся грани не могут быть одновременно изоляторами. Поэтому элементов $15 \cdot (17^4 - 1) = 1\ 252\ 800$.
4. Есть $\binom{3}{6} = 20$ вариантов расположений входов. Каждая из оставшихся граней либо изолятор, либо реализует функцию от трёх переменных (всего $2^{2^3} + 1 = 257$ вариантов для каждой стороны), причем все 3 оставшиеся грани не могут быть одновременно изоляторами. Поэтому элементов $20 \cdot (257^3 - 1) = 339\ 491\ 840$.
5. Есть $\binom{4}{6} = 15$ вариантов расположений входов. Каждая из оставшихся граней либо изолятор, либо реализует функцию от четырёх переменных (всего $2^{2^4} + 1 = 65\ 537$ вариантов для каждой стороны), причем обе оставшиеся грани не могут быть одновременно изоляторами. Поэтому элементов $15 \cdot (65\ 537^2 - 1) = 64\ 426\ 475\ 520$.
6. В этом случае есть единственный выход, который не может быть изолятором. Есть 6 расположений выхода, причем на нём реализуется любая

из $2^{2^5} = 4\,294\,967\,296$ функций от 5-ти переменных. Поэтому элементов $6 \cdot 4\,294\,967\,296 = 25\,769\,803\,776$.

Суммируя, получаем 90 537 043 409. Обозначим это число через C_1.

□

Лемма 27. *Количество объёмных схем объёмом v не больше, чем $2^{C_2 v}$, где C_2 – некоторая константа.*

Доказательство. Сначала рассмотрим объёмные схемы со связным носителем. Имеется не более $(5e)^v$ связных областей с объёмом v (поликубы) [17]. Далее, для каждой связной области M объёмом v в каждый кубик можно поставить один из C_1 видов кубиков (лемма 26). Поэтому область M можно заполнить кубиками $(C_1)^v$ способами. Таким образом, существует не более $(5e \cdot C_1)^v$ схем объёмом v со связным носителем. Обозначим $C' = \log_2(5e \cdot C_1)$.

Теперь рассмотрим случай, когда носитель несвязен. Если он разбивается на части с объёмами $v_1, v_2, \ldots, v_k, v_1 + v_2 + \ldots + v_k = v$, то количество таких схем не больше, чем $2^{C' v_1} \cdot 2^{C' v_2} \cdot \ldots \cdot 2^{C' v_k} = 2^{C' v}$.

Пусть $v \in \mathbb{N}$. Оценим сверху количество всевозможных разбиений $\sigma_v = (v_1, v_2, \ldots, v_k)$ числа $v = \sum\limits_{i=1}^{k} v_i$, где $v_i > 0, i \in [k]$, причём разбиения, отличающиеся порядком слагаемых будем считать одинаковыми. Каждое разбиение σ_v можно закодировать при помощи последовательности ρ_v длины $v - 1$ из нулей и единиц следующим образом. Если разбиение σ_v состоит из k элементов, то в соответствующей последовательности ρ_v будет $k - 1$ единица. Пусть $\{j_1, j_2, \ldots, j_{k-1}\}$ — места, где стоят единицы в ρ_v. Положим $j_i = \sum\limits_{s=1}^{i} v_s$. Отметим, что разным разбиениям σ_v будут соответствовать разные последовательности ρ_v. Поэтому количество разбиений не больше, чем 2^{v-1}.

Для каждого разбиения имеется не более $2^{C' v}$ схем, поэтому схем меньше, чем $2^{C' v} 2^{C' v - 1} < 2^{(C'+1)s}$. Далее взяв $C_2 = C' + 1$, получим утверждение леммы.

□

Определение: Пусть у нас есть алгоритм определения *последнего слоя* схемы относительно некоторых ее выходов, который зависит только от геометрии схемы. Введём множество $L(u, v, h, D, m)$ операторов $f : D \to \{0,1\}^m$ вида $f = F(x, G(x))$, где существует такая схема K, что выполнены условия:

1. K имеет m выходов, h входов на последнем слое и не более n входов, не лежащих на последнем слое.

2. объём K не превосходит v.
3. K реализует оператор $F : D \times \{0,1\}^h \to \{0,1\}^m$, причем последние h аргументов подаются на входы K, расположенные на последнем слое.
4. $G \in P_u(D,h)$.

Лемма 28. *Если* $d = |D|, h \geqslant 1$ *и* $v \leqslant \frac{3}{5C_3} md$, *то*

$$L(u,v,h,D,m) < m!n!2^{m(1-\varepsilon_1)d}$$

при $u \leqslant \frac{m}{5\log_2 d}$, *где* C_2 *взято из условия леммы 27,* $C_3 = \max\{C_2, 30\}, \varepsilon_1 = \frac{1}{5} - \frac{3}{C_3 \ln 2}$.

Доказательство. Отметим заранее, что идея доказательства аналогична доказательству из работы [18, лемма 4]. В частности было доказано, что

$$\log_2 x \leqslant \frac{x}{e \ln 2}. \tag{2.23}$$

Заметим, что поскольку у каждого элемента схемы может быть не более 5-ти входов, то если $h > 5v$, то схем объёма v с h входами нет, и утверждение верно. Поэтому далее полагаем, что $h \leqslant 5v \leqslant \frac{3}{C_3} md$.

Оценим число $|L(u,v,h,D,m)|$. По лемме 25 количество различных операторов G из $P_u(D,h)$ не больше, чем $2^{du\log_2 \frac{eh}{u}}$. Количество операторов F с точностью до перестановок входов не больше, чем количество схем объёма v, то есть $2^{C_2 v}$. Для каждой схемы можно осуществить произвольную перестановку выходов, а также входов, на которые подается x. С учетом перестановок выходов и входов, на которые подается x, получается не более $m!n!2^{C_2 v}$ операторов.

Таким образом,

$$|L(u,v,h,D,m)| \leqslant m!n!2^{C_2 v} 2^{du\log_2 \frac{eh}{u}} = m!n!2^{C_2 v + du\log_2 \frac{eh}{u}}. \tag{2.24}$$

Оценим показатель степени при $u \leqslant \frac{m}{5\log_2 d}$, учитывая, что $v \leqslant \frac{3}{5C_3} md$, $h \leqslant \frac{3}{C_3} md$:

$$C_2 v + du \log_2 \frac{eh}{u} \leqslant C_2 v + du \log_2 d + du \log_2 \frac{eh}{du} \leqslant$$
$$\leqslant \frac{3}{5} md + d \frac{m}{5 \log_2 d} \log_2 d + du \frac{eh}{du \cdot e \ln 2} \leqslant$$
$$\leqslant \frac{4}{5} md + \frac{3}{C_3 \ln 2} md =$$
$$= md(1 - \varepsilon_1).$$

Отметим, что C_3 выбрано таким образом, чтобы $\varepsilon_1 > 0$. Отсюда

$$2^{C_2 v + du \log_2 \frac{eh}{u}} \leqslant 2^{m(1-\varepsilon_1)d},$$

и домножая на $m!n!$ и подставляя в (2.24), получаем утверждение леммы.

□

Определение: Пусть $D \subseteq \{0,1\}^n, d := |D|$. Рассмотрим множество $L_0(D, m)$ операторов $f : D \to \{0,1\}^m$, реализуемых некоторой схемой K так, что существует её подсхема K_0, содержащая хотя бы один выход схемы K такая, что

$$V(K_0) \leqslant \frac{1}{C_0} |\mathrm{Out}(K_0 K)| d, \qquad U_D(\mathrm{In}(K_0|K)) \leqslant \frac{|\mathrm{Out}(K_0 K)|}{5 \log_2 d}, \tag{2.25}$$

где $C_0 = \frac{5C_3}{3}$ — некоторая константа.

Лемма 29. *(Калачёв Г.В., [16, лемма 10]) Для любой плоской схемы K и любого подмножества её выходов U существует схема K_U, носитель которой лежит в носителе схемы K, множество её выходов совпадает с U и на каждом из этих выходов K_U реализует ту же функцию, что и схема K.*

Отметим, что конструктивное доказательство этого факта содержит алгоритм, который можно дословно повторить для объёмных схем (то есть он никак существенно не использует геометрию схемы).

Доказательство следующей леммы идейно аналогично доказательству из работы [18, лемма 5], но использует другие константы и ограничения.

Лемма 30. *(Аналог [18, лемма 5] для объёмных схем). Пусть $\log_2 m \leqslant \frac{\varepsilon_1}{6} d$, где значение ε_1 взято из условия леммы 28. Тогда $|L_0(D, m)| = o(2^{md})$ при $d \to \infty, n \log_2 n = o(d)$.*

Доказательство. Рассмотрим классы $l(v,h,D,m_0) \subset L_0(D,m)$, для которых выполнено (2.25), причём $V(K_0) = v, |In(K_0|K)| = h, |Out(K_0K)| = m_0$ при фиксированных $1 \leqslant m_0 \leqslant m, 0 \leqslant v \leqslant \frac{3}{5C_3}md$ и $h > 0$. Подсчитаем число элементов в $l(v,h,D,m_0)$. Как уже отмечалось в лемме 28, имеет смысл рассматривать лишь $h \leqslant 5v \leqslant \frac{3}{C_3}md$ (иначе $l(v,h,D,m_0) = \varnothing$).

Аналогично доказательству из [18, лемма 5], получим оценку:

$$|l(v,h,D,m_0)| \leqslant \frac{2^{md}}{2^{d\left(\varepsilon_1 - \frac{2\log_2 m + n\log_2 n}{d}\right)}}.$$

Оценим количество элементов в $L_0(D,m)$:

$$|L_0(D,m)| = \left| \bigsqcup_{m_0=1}^{m} \bigsqcup_{v=0}^{\frac{3}{5C_3}m_0 d} \bigsqcup_{h=0}^{\frac{3}{C_3}m_0 d} l(v,h,D,m_0) \right| \leqslant$$
$$\leqslant \sum_{m_0=1}^{m} \frac{9}{5C_3^2} m_0^2 d^2 \frac{2^{md}}{2^{d\left(\varepsilon_1 - \frac{2\log_2 m + n\log_2 n}{d}\right)}} \leqslant$$
$$\leqslant m^3 d^2 \frac{2^{md}}{2^{d\left(\varepsilon_1 - \frac{2\log_2 m + n\log_2 n}{d}\right)}}.$$

Значит доля операторов из $L_0(D,m)$ равна:

$$\frac{|L_0(D,m)|}{2^{md}} \leqslant \frac{m^3 d^2}{2^{d\left(\varepsilon_1 - \frac{2\log_2 m + n\log_2 n}{d}\right)}} \leqslant \frac{1}{2^{d\left(\varepsilon_1 - \frac{5\log_2 m + 2\log_2 d + n\log_2 n}{d}\right)}}.$$

Оценим выражение в показателе. $\log_2 m \leqslant \frac{\varepsilon_1}{6}d, \log_2 d + n\log_2 n = o(d)$ при $d \to \infty, n\log_2 n = o(d)$, поэтому

$$d\left(\varepsilon_1 - \frac{5\log_2 m + 2\log_2 d + n\log_2 n}{d}\right) \geqslant d\left(\frac{\varepsilon_1}{6} + o(1)\right) \to \infty$$

при $d \to \infty, n\log_2 n = o(d)$.

Поэтому $\frac{|L_0(D,m)|}{2^{md}} \to 0$ при $d \to \infty, n\log_2 n = o(d)$.

□

Пусть у нас есть алгоритм определения *последнего слоя* схемы относительно некоторых её выходов, который зависит только от геометрии схемы.

Определение: Рассмотрим множество $L_1(D,m)$ операторов $f : D \to \{0,1\}^m$, реализуемых некоторой схемой K так, что существует подсхема K_0

такая, что все входы $\mathrm{In}(K_0|K)$ лежат на последнем слое схемы K_0 относительно выходов $\mathrm{Out}(K_0K)$ и

$$V(K_0) \leqslant \frac{1}{C_4}|\mathrm{Out}(K_0K)|\,d, \quad U_D(K_0|K) \leqslant \frac{1}{9}, \tag{2.26}$$

где $C_4 = \frac{32}{15}C_2$.

Лемма 31. *(Аналог [18, лемма 10] для объёмных схем). Пусть $m, n \in \mathbb{N}$, $D \subseteq \{0,1\}^n$, $d = |D|$. Тогда*

$$|L_1(D,m)| = o(2^{md}) \text{ при } d \to \infty, \log_2 m \leqslant \frac{d}{50},\ n\log_2 n = o(d).$$

Доказательство. Отметим, что подобный выбор константы C_4 в определении класса L_1 позволил оставить все технические выкладки из доказательства леммы 10 в [18] в неизменном виде. Единственный геометрический факт, который следует учесть: имеется не более $2^{C_2\frac{1}{C_4}m_0d} = 2^{\frac{15}{32}m_0d}$ схем объёма не более $\frac{1}{C_4}m_0d$ (лемма 27). □

Отметим, что определение и свойства классов $L_0(D,m)$ и $L_1(D,m)$ не зависит от геометрии схемы и аналогично обобщается на объёмные схемы, чем мы будем пользоваться в дальнейшем. Также формально положим:

$$\alpha = \frac{1}{16}\min\left(\frac{1}{C_0}, \frac{1}{C_4}\right).$$

2.6 Основное доказательство

Лемма 32. *Для любого $t \geqslant 0$ и множества $I \in \mathfrak{I}(t)$ верны следующие оценки:*

1. $u_I(t) \geqslant p(R_I(t))$;
2. $u_I(t) \geqslant 2^{\frac{m_I t^{1/3}}{l^{2/3}}}$.

Доказательство. Проведём доказательство индукцией по мощности множества I. **База индукции:** $|I| = 0$. Поскольку $\varnothing \notin \mathfrak{I}$, то здесь доказывать нечего. **Шаг индукции:** $|I| \geqslant 1$.

I. Сначала покажем, что условие леммы выполнено при $t = a_I$.

Ia. Если $|I| = 1$, то $I \in \mathfrak{I}(0)$, значит $t = a_I = 0$. Легко видеть, что $u_I(0) = p(R_I(0)) = 2^{\frac{m_I t^{1/3}}{l^{2/3}}} = 0$, и условия леммы выполнены.

Ib. Рассмотрим основной случай, когда $|I| \geqslant 2$. В этом случае множество $R_I(a_I)$ получено из множеств $R_{I_1}(a_I), \ldots, R_{I_k}(a_I)$ с помощью операции **объединения**.

Покажем, что неравенства 1), 2) сохраняются при операции объединения в момент $t = a_I$. Поскольку в данном случае t фиксировано, опустим его для упрощения обозначений.

1. $u_I = \sum\limits_{j=1}^{k} u_{I_j}$ по определению. Верна оценка

$$\ell_q(R_I) = \ell_q\Big(\bigcup_{j=1}^{k} R_{I_j}\Big) \leqslant \sum_{j=1}^{k} \ell_q(R_{I_j}), \quad q \in [3].$$

Складывая неравенства, получаем

$$p(R_I) = \sum_{q=1}^{3} \ell_q(R_I) \leqslant \sum_{j=1}^{k}\sum_{q=1}^{3} \ell_q(R_{I_j}) = \sum_{j=1}^{k} p(R_{I_j}).$$

Поскольку $|I_j| \leqslant |I|$, $j \in [k]$, то по предположению индукции верно

$$u_{I_j} \geqslant p(R_{I_j}), \qquad j \in [k].$$

Отсюда получаем оценку

$$u_I = \sum_{j=1}^{k} u_{I_j} \geqslant \sum_{j=1}^{k} p(R_{I_j}) \geqslant p(R_I).$$

2. По определению и свойствам u_I, верно $u_I = \sum\limits_{j=1}^{k} u_{I_j}, m_I = \sum\limits_{j=1}^{k} m_{I_j}$. По предположению индукции имеем:

$$u_J \geqslant 2\frac{m_J t^{1/3}}{l^{2/3}}, \qquad J = I_1, \ldots, I_k.$$

Складывая неравенства, получаем требуемую оценку:

$$u_I = \sum_{j=1}^{k} u_{I_j} \geqslant \sum_{j=1}^{k} 2\frac{m_{I_j} t^{1/3}}{l^{2/3}} = 2\frac{m_I^{2/3} v_I^{1/3}}{l^{2/3}}.$$

II. Покажем, что утверждение леммы верно для всех $t \in (a_I, b_I]$.

1. Покажем, что

$$u_I(t) \geqslant p(R_I(t)) \quad \text{при} \quad t \in [a_I, b_I]. \tag{2.27}$$

Случай $t = a_I$ рассмотрен в пункте I. Из (2.10) имеем:

$$u_I(t) = u_I(a_I) + \max\left(\frac{m_I}{l}, 1\right)(p(R_I(t)) - p(R_I(a_I))) \geqslant$$
$$\geqslant u_I(t_i) + (p(R_I(t)) - p(R_I(t_i))) \geqslant p(R_I(t)).$$

2. Напомним, что по построению выполнено равенство $v_I(t) = m_I t$. Поэтому условие пункта 2) эквивалентно следующему:

$$u_I(t) \geqslant 2\frac{m_I^{2/3} v_I^{1/3}(t)}{l^{2/3}}.$$

Преобразуем:

$$u_I^{3/2}(t) \geqslant 2^{3/2} \cdot \frac{m_I}{l} v_I^{1/2}(t). \tag{2.28}$$

Заметим, что так как неравенство верно при $t = a_I$ по пункту I, то достаточно показать, что:

$$\left(u_I^{3/2}(t)\right)' \geqslant 2^{3/2}\left(\frac{m_I}{l} v_I^{1/2}(t)\right)' \quad \text{при} \quad a_I < t < b_I.$$

Преобразуем неравенство:

$$\frac{3}{2}(u_I(t))^{1/2} u_I'(t) \geqslant \sqrt{2} \cdot \frac{m_I}{l} \frac{v_I'(t)}{(v_I(t))^{1/2}}. \tag{2.29}$$

По определению $u_I(t)$ имеем неравенство:

$$u_I'(t) \geqslant \frac{m_I}{l} p_I'(t). \tag{2.30}$$

Также из лемм 22 и 23 имеем:

$$(u_I(t))^{1/2} \geqslant \sqrt{\frac{1}{32}} \frac{s_I(t)}{(v_I(t))^{1/2}} = \frac{3}{\sqrt{8}} \frac{v_I'(t)}{(v_I(t))^{1/2} \cdot p_I'(t)}. \tag{2.31}$$

Перемножив неравенства (2.30) и (2.31) и огрубив константу, получим неравенство (2.29).

Таким образом, основная лемма доказана. □

Теорема 3. *Существует такая абсолютная константа $C > 0$, что для любого натурального n, любого $D \subseteq \{0,1\}^n$ верно*

$$\boldsymbol{U(f) \geqslant C \frac{m\sqrt[3]{|D|}}{\min^{2/3}(m, \log_2 |D|)}}$$

для почти всех операторов $f \in P_2(D, m)$ при $n \log_2 n = o(|D|), \log_2 m = o(|D|), |D| \to \infty$.

Доказательство. Обозначим $d := |D|, l := \log_2 d$. Можно считать, что d достаточно велико, и $d \geqslant \frac{1}{8\alpha}$. Зафиксируем произвольный оператор $f \in P_2(D,m) \setminus L_0(D,m) \setminus L_1(D,m)$ и оценим его средний потенциал. Заметим, что по леммам 30 и 31 при $n\log_2 n = o(d), \log_2 m = o(d), d \to \infty$ верно $|L_0(D,m) \cup L_1(D,m)| = o(2^{md})$. Таким образом, полученная далее оценка верна для почти всех операторов из $P_2(D,m)$. Зафиксируем схему K, реализующую f с минимальным потенциалом (то есть, такую, что $U_D(K) = U(f)$), и построим для неё расслоение $\mathfrak{R}$.

Обозначим $t_0 = \alpha d$. По лемме 24 и определению α для $t \in [0, t_0]$ имеем:

$$\begin{aligned} V(M_I(t)) &\leqslant 8V(R_I(t)) + m_I = 8m_I t + m_I \leqslant \\ &\leqslant 8\alpha d m_I + m_I = (8\alpha d + 1)|\mathrm{Out}(M_I(t)K)| \leqslant \\ &\leqslant 16\alpha d \cdot |\mathrm{Out}(M_I(t)K)| = \min\left(\frac{1}{C_0}, \frac{1}{C_4}\right) d \cdot |\mathrm{Out}(M_I(t)K)|. \end{aligned}$$

Поэтому раз $f \notin L_0(D,m) \cup L_1(D,m)$, то при $t \in [0, t_0]$ выполнено

$$U_D(M_I(t)|K) \geqslant \max\left(\frac{1}{9}, \frac{\mathrm{Out}(M_I(t)K)}{5l}\right) \geqslant \frac{1}{9}\max\left(1, \frac{m_I}{l}\right). \tag{2.32}$$

Обозначим $\mathfrak{I}_0 = \bigcup\limits_{t\in[0,t_0]} \mathfrak{I}(t)$. Заметим, что

$$\mathfrak{I}_0 = \bigsqcup_{I\in\mathfrak{I}(t_0)} \{J \in \mathfrak{I} \mid J \subseteq I\}.$$

Из неравенств (2.7), (2.32) и определения $u_I(t)$ получаем:

$$\begin{aligned} U_D(K) &\geqslant \frac{1}{6}\int\limits_{\mathfrak{R}} U_D(K(R)|K)\, d\rho(R) \geqslant \\ &\geqslant \frac{1}{6}\sum_{I\in\mathfrak{I}_0} \int\limits_{a_I}^{\min(b_I,t_0)} U_D(M_I(t)|K)\, dp(R_I(t)) \geqslant \\ &\geqslant \frac{1}{54}\sum_{I\in\mathfrak{I}_0} \int\limits_{a_I}^{\min(b_I,t_0)} \max\left(1, \frac{m_I}{l}\right) dp(R_I(t)) \geqslant \\ &= \frac{1}{54}\sum_{I\in\mathfrak{I}(t_0)} \sum_{J\in\mathfrak{I}:J\subseteq I} \int\limits_{a_I}^{\min(b_I,t_0)} \max\left(1, \frac{m_J}{l}\right) dp(R_J(t)) = \\ &= \frac{1}{54}\sum_{I\in\mathfrak{I}(t_0)} u_I(t_0). \end{aligned}$$

Из леммы 18 и пункта 1) леммы 32 следует:

$$u_I(t) \geqslant p(R_I(t)) \geqslant 3v_I(t)^{1/3}.$$

Так как по построению множества $R_I(t)$ верно равенство $v_I(t) = m_I \cdot t$, то имеем неравенство:

$$U_D(K) \geqslant \frac{1}{54} \sum_{I \in \mathfrak{I}(t_0)} u_I(t_0) \geqslant \frac{1}{18} \sum_{I \in \mathfrak{I}(t_0)} v_I(t_0)^{1/3} = \frac{t_0^{1/3}}{18} \sum_{I \in \mathfrak{I}(t_0)} m_I^{1/3}. \tag{2.33}$$

Также заметим, что если дан вектор $x = (x_1, x_2, \ldots, x_s), x_i \geqslant 0, i \in [s]$, то по неравенству Минковского в пространстве l_3 имеем:

$$(x_1^3)^{1/3} + (x_2^3)^{1/3} + \ldots + (x_s^3)^{1/3} \geqslant (x_1^3 + x_2^3 + \ldots + x_s^3)^{1/3},$$

$$x_1 + x_2 + \ldots + x_s \geqslant (x_1^3 + x_2^3 + \ldots + x_s^3)^{1/3}.$$

Заменив $m_i = x_i^3, i \in [s]$, получим неравенство:

$$m_1^{1/3} + m_2^{1/3} + \ldots + m_s^{1/3} \geqslant (m_1 + m_2 + \ldots + m_s)^{1/3}.$$

Воспользуемся полученным результатом и продолжим неравенство (2.33):

$$U_D(K) \geqslant \frac{1}{18} \left(\sum_{I \in \mathfrak{I}(t_0)} m_I^{1/3} \right) \cdot t_0^{1/3} \geqslant \frac{1}{18} m^{1/3} \cdot t_0^{1/3} = \frac{\alpha^{1/3}}{18} \sqrt[3]{m \cdot d}. \tag{2.34}$$

При $m > l$ по пункту 2) леммы 24 получаем:

$$\begin{aligned} U_D(K) &\geqslant \frac{1}{54} \sum_{I \in \mathfrak{I}(t_0)} u_I(t_0) \geqslant \\ &\geqslant \frac{1}{27} \sum_{I \in \mathfrak{I}(t_0)} \frac{m_I \cdot t_0^{1/3}}{l^{2/3}} = \frac{1}{27} \frac{m \cdot t_0^{1/3}}{l^{2/3}} = \frac{\alpha^{1/3}}{27} \frac{m \sqrt[3]{d}}{l^{2/3}}. \end{aligned} \tag{2.35}$$

Соединив результаты неравенств (2.34) и (2.35) и приняв $C = \alpha^{1/3}/27$, получаем требуемое условие теоремы. □

С учётом Теоремы 2 и Теоремы 3, получаем следующие следствия.

Следствие 1. *Для почти всех $f \in P_2(n, m)$, при $n \to \infty$, $\log_2 m = o(2^n)$ верно асимптотическое равенство:*

$$\boldsymbol{U(f) = \Theta\left(\frac{m \cdot 2^{n/3}}{\min^{2/3}(m, n)} \right).}$$

Следствие 2. *Пусть* $n \to \infty$, $\log_2 m = o(2^n)$. *Тогда верно асимптотическое равенство:*

$$\boldsymbol{U(n,m) \asymp \hat{U}(n,m) = \Theta\left(\frac{m \cdot 2^{n/3}}{\min^{2/3}(m,n)}\right).}$$

Глава 3. Объёмные схемы с близкими выходами

3.1 Нижние оценки

3.1.1 Оценки для площади и объема

Кубиком будем называть единичный куб с центрами в точках с целочисленными координатами и сторонами, параллельными осям координат.

Расстоянием между кубиками будем называть расстояние между их центрами по манхэттенской метрике (l^1 метрике). Отметим, что в главе 2 использовалась l^∞ метрика, а в данной главе мы будем использовать манхэттенскую метрику.

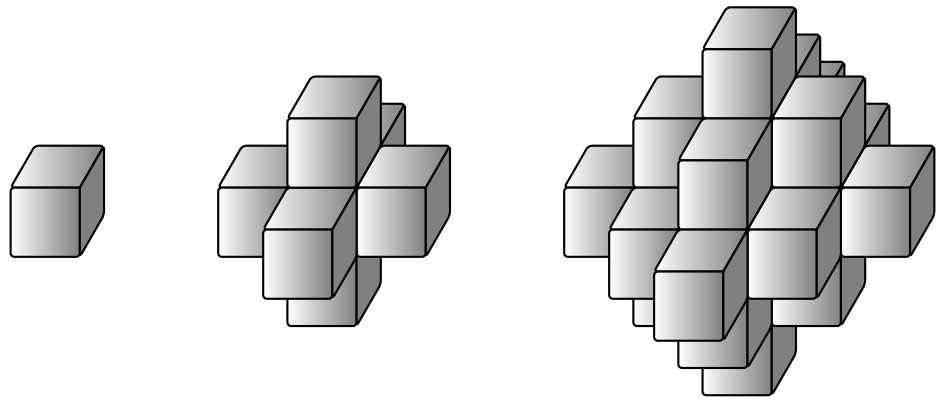
Шаром радиуса r с данным центральным кубиком C^0 будем называть множество кубиков, лежащих на расстоянии не более $r-1$ от C^0 (при $r=0$ это множество пусто, см. рис. 3.1). Площадь поверхности шара радиуса r будем обозначать S_r.

Пусть $M \subseteq \mathbb{Z}^3$. Будем называть элементы из M *соседними*, если их координаты отличаются на 1 в одной компоненте, а две другие компоненты одинаковы. Рассмотрим граф Q_M, вершинами которого являются элементы множества M, а рёбра соединяют соседние элементы. Будем говорить что множество M *связно*, если граф Q_M связен.

Пусть W — некоторое множество кубиков. Через $S(W)$ обозначим площадь поверхности объединения кубиков из W. Будем говорить, что множество W *связно*, если связно его множество центров кубиков.

Введём некоторые обозначения. Пусть $M \subseteq \mathbb{Z}^3, r \geqslant 1$.

- $B_M(r)$ — множество кубиков в пространстве, отстоящих от точек из M не более чем на $r-1$ по манхэттенской метрике.
- $V_M(r) = |B_M(r)|$ — объём множества $B_M(r)$; $V_M(0) := 0$.
- $S_M(r)$ — площадь поверхности объединения кубиков из множества $B_M(r)$.
- $k_M(r)$ — количество компонент связности множества $B_M(r)$ при $r \geqslant 1$; $k_M(0) := |M|$.



$r = 1$ $r = 2$ $r = 3$

Рисунок 3.1 — Шары различного радиуса.

– $\varphi_M(r) := \sum\limits_{j=0}^{r} k_M(j)$ — вспомогательная функция, через которую выражаются оценки для $S_M(r), V_M(r)$.

Лемма 33. *Площадь поверхности S_r шара радиуса r равна*

$$6(r^2 + (r-1)^2).$$

Доказательство. Рассмотрим любую из 6 проекций шара (см. рис. 3.2).

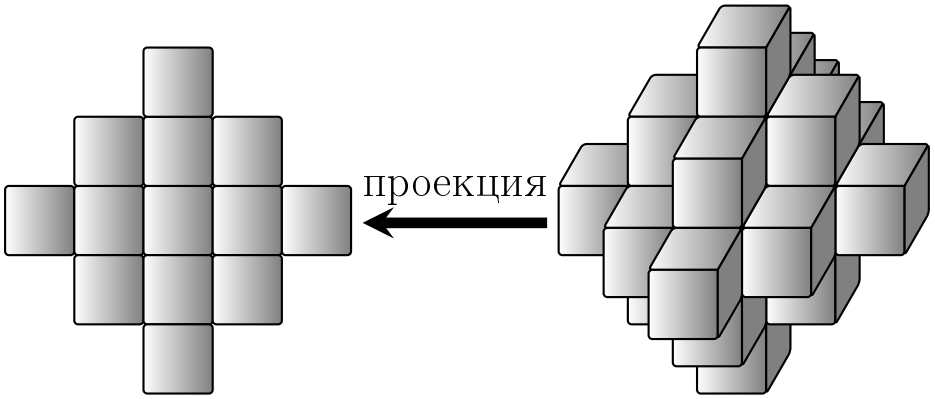


Рисунок 3.2 — Проекция шара.

Заметим, что площадь поверхности данного шара будет равна площади поверхности проекции, увеличенной в 6 раз. Также заметим, что площадь поверхности поверхности равна (считаем по слоям, сверху вниз)

$$\sum_{i=1}^{r}(2i-1) + \sum_{i=1}^{r-1}(2i-1) = r^2 + (r-1)^2.$$

А значит, площадь поверхности всего шара равняется $6(r^2 + (r-1)^2)$, что и требовалось.

□

Следствие 4. *Площадь поверхности* $S_r \leqslant 12r^2$.

Лемма 34. *Пусть* $C^1, C^2 \in \mathbb{Z}^3$. *Через* $W_i(r)$ *обозначим шар радиуса* r *с центром в* $C^i, i \in [2]$. *Пусть* r_0 *такое, что* $W_1(r_0) \cap W_2(r_0) = \varnothing$ *(не имеет общих граней), а* $W_1(r_0+1) \cap W_2(r_0+1) \neq \varnothing$. *Обозначим* $\Delta = r - r_0$. *Тогда для любого* $r \geqslant r_0$ *имеет место оценка*

$$S(W_1(r) \cup W_2(r)) \leqslant 24r^2 - 6((\Delta-1)^2 + (\Delta-2)^2).$$

Доказательство. Оценим площадь поверхности двух шаров как сумму площадей поверхностей шаров и разность той части поверхности шара, которая окажется внутри пересечения (см. рис. 3.3). Такие грани кубиков, которые оказываются внутри пересечения, будем называть «испорченными». Если все грани кубика «испорчены», то такой кубик назовём «испорченным».

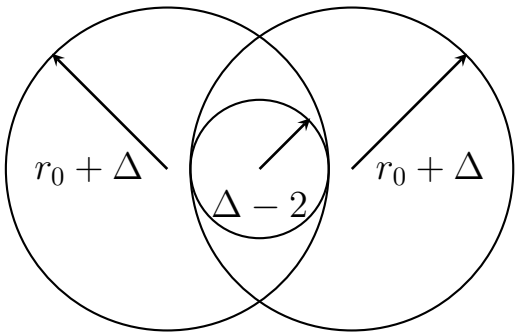


Рисунок 3.3

Случай $\Delta = 1$. Заметим, что тогда в каждом шаре «испорчена» хотя бы одна грань. Тогда площадь поверхности объединения двух шаров можно оценить сверху как разность суммы площадей поверхности и удвоенной площади «испорченной» грани. Получаем

$$\begin{aligned} S(W_1(r) \cup W_2(r)) &\leqslant 6 \cdot ((r_0+1)^2 + r_0^2) + 6 \cdot ((r_0+1)^2 + r_0^2) - 2 \leqslant \\ &\leqslant 12 \cdot (2r_0^2 + 2r_0 + 1) - 2 \leqslant 24r_0^2 + 24r_0 + 10 \leqslant \\ &\leqslant 24r_0^2 + 48r_0 + 18 \leqslant \\ &\leqslant 24(r_0+1)^2 - 6((1-1)^2 + (1-2)^2), \end{aligned}$$

что и требовалось доказать.

Случай $\Delta \geqslant 2$. Отметим, что при $\Delta = 2$ будет полностью испорчен хотя бы один кубик, назовём его базовым. Введём $U(r) = W_1(r) \cap W_2(r)$. Заметим также, что если внутри $U(r)$ находится какая-нибудь фигура, то внутри $U(r+x)$

будет находиться фигура, составленная из всех кубиков, расположенных на расстоянии не более x от $U(r)$.

Т.к. при $r = r_0 + 2$ внутри пересечения шаров $U(r_0 + 2)$ находится один базовый кубик (то есть шар радиуса 1), то при $r = r_0 + \Delta$ внутри поместится шар радиуса $\Delta - 1$. Далее заметим, что площадь поверхности пересечения $U(r_0 + \Delta)$ не меньше площади указанного шара радиуса $\Delta - 1$, так как для каждой грани шара можно указать грань $U(r_0 + \Delta)$, которую можно на неё спроецировать. По лемме 33 площадь поверхности шара радиуса $\Delta - 1$ равна $6((\Delta-1)^2 + (\Delta-2)^2)$. Таким образом, получаем

$$\begin{aligned} S(W_1(r) \cup W_2(r)) &= S(W_1(r)) + S(W_1(r)) - S(U(r)) \leqslant \\ &\leqslant 24(r_0 + \Delta)^2 - 6((\Delta - 1)^2 + (\Delta - 2)^2). \end{aligned}$$

□

Лемма 35. *Пусть* $M = \{C^1, C^2, \ldots, C^n\} \subseteq \mathbb{Z}^3$. *Тогда*

$$S_M(r) \leqslant 60r \cdot \varphi_M(r - 1).$$

Доказательство. Обозначим $W_i(r)$ — шар радиуса r с центром C^i. Проведем доказательство индукцией по числу шаров.

Базис индукции: $n = 1$. Согласно следствию 4 площадь поверхности шара

$$S_M(r) = S(W_1(r)) \leqslant 12r^2 \leqslant 60r^2 \leqslant 60r \cdot \varphi_M(r - 1).$$

Шаг индукции: пусть для всех множеств, состоящих не более, чем из $n - 1$ элементов утверждение верно, докажем для n.

1) Рассмотрим случай, когда $W(r)$ разбивается на две несвязные друг с другом компоненты $A(r)$ и $B(r)$, т.е. $W(r) = A(r) \bigsqcup B(r)$. Через M_1 обозначим множество центров шаров $A(r)$, а через M_2 обозначим множество центров шаров $B(r)$. Тогда $M = M_1 \bigsqcup M_2$. Заметим, что

$$S_M(r) = S_{M_1}(r) + S_{M_2}(r). \tag{3.1}$$

По предположению индукции верны оценки

$$\begin{aligned} S_{M_1}(r) &\leqslant 60r \cdot \varphi_{M_1}(r - 1), \\ S_{M_2}(r) &\leqslant 60r \cdot \varphi_{M_2}(r - 1). \end{aligned} \tag{3.2}$$

Заметим, что так как для всех $i \leqslant r-1$ верно

$$k_M(i) = k_{M_1}(i) + k_{M_2}(i),$$

то имеет место равенство

$$\begin{aligned} \varphi_M(r-1) = \sum_{j=0}^{r-1} k_M(j) = \sum_{j=0}^{r-1} k_{M_1}(j) + \sum_{j=0}^{r-1} k_{M_2}(j) = \\ = \varphi_{M_1}(r-1) + \varphi_{M_2}(r-1). \end{aligned} \tag{3.3}$$

Совместив результаты утверждений (3.1), (3.2) и (3.3), получаем:

$$\begin{aligned} S_M(r) = S_{M_1}(r) + S_{M_2}(r) \leqslant 60r \cdot \varphi_{M_1}(r-1) + 60r \cdot \varphi_{M_2}(r-1) = \\ = 60r \cdot \varphi_M(r-1). \end{aligned}$$

2) Теперь рассмотрим основной случай, когда множество $W(r)$ является связным. Введём полный граф G, где вершинами являются точки C^i, а длины ребер — расстояния между ними. Рассмотрим минимальное остовное дерево T в графе G, и без ограничения общности будем считать, что C^n является листом в T.

Обозначим $W'(r) = W_1(r) \cup W_2(r) \cup \ldots \cup W_{n-1}(r)$, $W(r) = W'(r) \cup W_n(r)$; $M = M' \cup \{C^n\}$. Через r_0 обозначим такое максимальное r, что шар $W_n(r)$ не пересекается с множеством $W'(r)$, т.е.

$$r_0 = \max\{x : W'(x) \cap W_n(x) = \varnothing\}.$$

Так как $W(r) = W'(r) \bigsqcup W_n(r)$ при $r \leqslant r_0$ (по определению r_0), то

$$k_M(r) = k_{M'}(r) + 1, \text{ при } r \leqslant r_0. \tag{3.4}$$

Докажем, что

$$k_M(r) = k_{M'}(r), \text{ при } r > r_0. \tag{3.5}$$

Заметим, что $k_M(r) \leqslant k_{M'}(r)$ при $r > r_0$, так как шар $W_n(r)$ при $r > r_0$ пересекается с множеством $W'(r)$, а значит число компонент связности в множестве $W(r)$ будет не больше, чем в множестве $W'(r)$.

Предположим, что при некотором $r > r_0$ выполняется неравенство $k_M(r) < k_{M'}(r)$. Это может произойти только в случае, если шар $W_n(r)$ будет пересекаться с двумя шарами $W_{j_1}(r)$ и $W_{j_2}(r)$, которые лежат в разных компонентах связности множества $W'(r)$ (см. рис. 3.4). Рассмотрим ребра $C^{j_1}C^n$ и

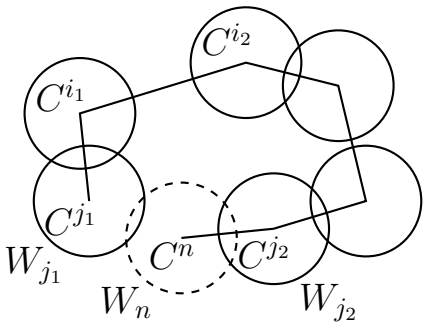


Рисунок 3.4

$C^{j_2}C^n$ графа G. Эти ребра одновременно не могут лежать в МОД T, так как C^n является листом графа T. Без ограничения общности считаем, что $C^nC^{j_2} \in T$. Заметим тогда, что вершины C^{j_1} и C^{j_2} будут соединены путем в графе T, причем одно из рёбер этого пути будет больше (на рисунке это ребро $C^{i_1}C^{i_2}$), чем ребро $C^{j_1}C^n$. Тогда можно удалить ребро $C^{i_1}C^{i_2}$ и вместо него добавить ребро $C^{j_1}C^n$ в граф T. Отметим, что полученный граф будет остовным деревом для графа G, но с меньшей суммарной длиной рёбер, чем T, что противоречит тому, что T является МОД. Значит, $k_M(r) \geqslant k_{M'}(r)$ при $r > r_0$. Таким образом, утверждение (3.5) доказано.

В качестве следствия из оценок (3.4) и (3.5) получаем

$$\begin{aligned}\varphi_M(r-1) = \sum_{j=0}^{r-1} k_M(j) = \sum_{j=0}^{r_0} k_M(j) + \sum_{j=r_0+1}^{r-1} k_M(j) = \\ = \sum_{j=0}^{r-1} k_{M'}(j) + r_0 + 1 = \varphi_{M'}(r-1) + r_0 + 1.\end{aligned} \tag{3.6}$$

Обозначим $\Delta = r - r_0$. Рассмотрим случай, когда шар $W_n(r)$ пересекается только с одним шаром $W_j(r)$ из множества $W(r)$. Тогда согласно лемме 34 имеем оценку

$$S_M(r) - S_{M'}(r) \leqslant 12(r_0 + \Delta)^2 - 6((\Delta - 1)^2 + (\Delta - 2)^2). \tag{3.7}$$

Покажем, что если шар $W_n(r)$ пересекается с несколькими шарами, то оценка (3.7) также верна. Обозначим шары, с которыми пересекается шар $W_n(r)$ следующим образом: $W_j(r), W_{i_1}(r), W_{i_2}(r), \ldots$. Разрежем всю картинку по слоям и зафиксируем слой (см. рис. 3.5). Обозначим прямоугольник $R = W_j \cap W_n$, а множество $R' = W' \cap W_n$. Так как прямоугольник $R \subseteq R'$, то его периметр не превосходит периметра R'. Таким образом, так как площадь поверхности

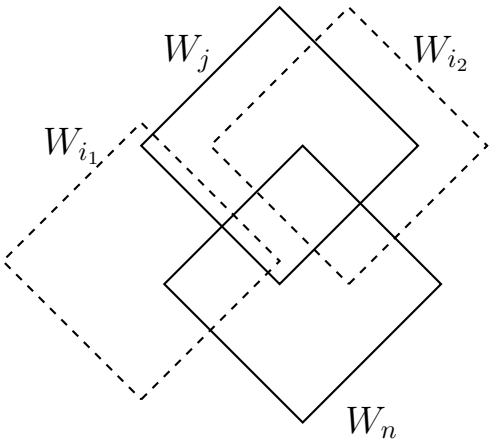


Рисунок 3.5

пересечения — это сумма периметров пересечения по слоям, то оценка (3.7) верна и в данном случае.

Из оценок (3.6), (3.7), предположения индукции и определения Δ получаем:

$$\begin{aligned}
S_M(r) &\leqslant S_{M'}(r) + 12(r_0+\Delta)^2 - 6((\Delta-1)^2+(\Delta-2)^2) \leqslant \\
&\leqslant 60r\cdot\varphi_{M'}(r-1) + 12(r_0+\Delta)^2 - 6((\Delta-1)^2+(\Delta-2)^2) = \\
&= 60r\cdot(\varphi_M(r-1) - r_0 - 1) + 12(r_0+\Delta)^2 - 6(2\Delta^2 - 6\Delta + 5) = \\
&= 60r\cdot\varphi_M(r-1) - 60r(r_0+1) + 12r_0^2 + 24r_0\Delta + 36\Delta - 30 = \\
&= 60r\cdot\varphi_M(r-1) - 60(r_0+\Delta)(r_0+1) + 12r_0^2 + 24r_0\Delta + 36\Delta - \\
&- 30 = 60r\cdot\varphi_M(r-1) - 48r_0^2 - 36r_0\Delta - 24\Delta - 90 \leqslant \\
&\leqslant 60r\cdot\varphi_M(r-1).
\end{aligned}$$

Утверждение доказано.

□

Лемма 36. *Пусть* $M = \{C^1, C^2, \ldots, C^n\} \subseteq \mathbb{Z}^3$. *Тогда*

$$V_M(r) \leqslant 60r^2\cdot\varphi_M(r-1).$$

Доказательство. Проведем доказательство индукцией по величине радиуса r.

Базис индукции: $r = 1$.

$$V_M(1) = n \leqslant 60\cdot 1\cdot n.$$

Шаг индукции: так как каждая грань относится только к одному кубику, то имеет место следующее неравенство

$$\begin{aligned} V_M(r+1) &\leqslant V_M(r) + S_M(r+1) \leqslant 60r^2\varphi_M(r-1) + 60(r+1)\varphi_M(r) \leqslant \\ &\leqslant 60r^2\varphi_M(r) + 60(r+1)\varphi_M(r) \leqslant 60\varphi_M(r)(r^2+r+1) \leqslant \\ &\leqslant 60(r+1)^2\varphi_M(r). \end{aligned}$$

□

3.1.2 Доказательство основной теоремы

Нижнюю оценку будем доказывать следующим образом. Ранее в параграфе 2.1 был введён непрерывный метод расслоения. Мы воспользуемся его дискретным аналогом, т.е. мы по-прежнему будем считать потенциал схемы по слоям. Но в данном случае границей расслоения является множество проводов (контактов подсхемы), а не пересечение бесконечного семейства слоёв схемы. Также вместо интегрирования мы будем суммировать по элементам расслоения.

Пусть есть класс B операторов, причем для каждого оператора $f \in B$ и любой схемы K, реализующей оператор f есть нижние оценки для потенциала на границе любой подсхемы, удовлетворяющей определенным ограничениям. *Расслоением* схемы K назовём произвольное множество $(M_i)_{i=1}^t$ её подсхем такое, что $In(M_i|K) \cap In(M_j|K) = \varnothing$, если $i \neq j$. Тогда будем строить расслоение $(M_i)_{i=1}^t$ такое, что подсхемы M_i удовлетворяют этому ограничению, и для каждого $M_i, i \in [t]$ использовать оценку потенциала на границе $(M_i|K)$, а потом суммировать, чтобы получить оценку для всей схемы K, то есть $U_D(K) \geqslant \sum\limits_{i=1}^{t} U_D(\mathrm{In}(M_i|K))$.

Введём величину $\bar{T}(K)$. Пусть m — количество выходов схемы K, числа $r_1,..,r_{m-1}$ — длины рёбер дерева выходов в порядке возрастания. Положим

$$\bar{T}(K) := \sum_{j=1}^{m-2} \left\lceil \frac{r_j}{2} \right\rceil + 2 \left\lceil \frac{r_{m-1}}{2} \right\rceil.$$

То есть $\bar{T}(K)$ — величина, равная по порядку суммарной длине рёбер дерева выходов.

Введём множество $\bar{T}_h := \{K : \bar{T}(K) \leqslant h\}$, состоящее из таких объёмных схем, у которых длина дерева выходов не превосходит h по порядку.

Заметим, что справедлива оценка

$$\bar{T}(K) = \sum_{j=1}^{m-2} \left\lceil \frac{r_j}{2} \right\rceil + 2 \left\lceil \frac{r_{m-1}}{2} \right\rceil \leqslant \sum_{j=1}^{m-2} r_j + r_{m-1} + 1 = T(K) + 1. \tag{3.8}$$

Если схема $K \in T_h$, то по определению верно $T(K) \leqslant h$, что в силу неравенства (3.8) означает $\bar{T}(K) \leqslant h + 1$. Таким образом $T_h \subseteq \bar{T}_{h+1}$.

Далее воспользуемся следующей леммой для плоского случая, доказательство которой аналогично переносится на объёмный случай.

Лемма 37. *(Калачёв Г.В., [18, лемма 8]). Для любой схемы K с более, чем одним выходом, выполнено*

1) $\varphi(r' - 1) = \bar{T}(K)$, *где* $r' := \min\{r : k_r = 1\}$,
2) $\varphi(r) \leqslant \bar{T}(K) + r$ *при* $r \geqslant 1$.

Введём некоторые обозначения. Пусть K — объёмная схема, $M \subseteq \mathbb{Z}^3$ — носитель схемы K.

- K_r — множество элементов схемы K, лежащих в множестве $B_M(r)$.
- $v_r := V(K_r)$ — объём схемы K_r; $v_0 := 0$.
- $\varphi(r) := \varphi_M(r)$.
- $u_r := U_D(K_r \mid K)$.

Лемма 38. *Если $m \geqslant 2, f \in P_2(D, m) \backslash L_0(D, m), d = |D|$, то*

$$U_{T_h}(f) \geqslant C_6 \frac{m\sqrt{md}}{\sqrt{(h + \sqrt[3]{md}) \log_2 d}},$$

где C_6 — некоторая константа.

Доказательство. Заметим, что $T_h \subseteq \bar{T}_{h+1}$. Возьмём произвольную схему $K \in \bar{T}_{h+1}$, реализующую оператор f и её расслоение $\{K_r\}_{r=1}^{r_0}$, приняв

$$r_0 := \max\left\{ r \in \mathbb{N} : r^2 \varphi(r-1) \leqslant \frac{md}{C_4} \right\},$$

где $C_4 = \frac{5 \cdot 60}{3} C_3$, а константа C_3 взята из условия леммы 28.

Тогда $(r_0+1)^2\varphi(r_0) \geqslant \frac{md}{C_4}$, значит $r_0+1 \geqslant \sqrt{\frac{md}{C_4\varphi(r_0)}}$. По лемме 37 и определению $\bar{T}_{h+1}$ получаем

$$r_0+1 \geqslant \sqrt{\frac{md}{C_4\varphi(r_0)}} \geqslant \frac{\sqrt{md}}{\sqrt{C_4(\bar{T}(K)+r_0)}} \geqslant \frac{\sqrt{md}}{\sqrt{C_4\,(h+1+r_0)}}. \tag{3.9}$$

Поскольку $r_0^3 \leqslant r_0^2\varphi(r_0-1) \leqslant \frac{md}{C_4}$, то $r_0 \leqslant \frac{\sqrt[3]{md}}{\sqrt[3]{C_4}}$. Обозначим $C_5 := \frac{1}{\sqrt[3]{C_4}}$, и получим из (3.9)

$$r_0+1 \geqslant \frac{\sqrt{md}}{\sqrt{C_4\left(h+1+C_5\sqrt[3]{md}\right)}}$$

Далее по лемме 36 при всех $r \leqslant r_0$ получаем $v_r \leqslant 60r^2\varphi(r-1) \leqslant \frac{3}{5C_3}md$. Тогда поскольку $f \notin L_0(D,m)$, то для любого $r \leqslant r_0$ выполнено $u_r \geqslant \frac{m}{5\log_2 d}$, значит

$$\begin{aligned} U_D(K) &\geqslant \sum_{r=0}^{r_0} u_r \geqslant \sum_{r=0}^{r_0} \frac{m}{5\log_2 d} = \frac{m(r_0+1)}{5\log_2 d} \geqslant \\ &\geqslant \frac{m\sqrt{md}}{5\sqrt{C_4\left(h+1+C_5\sqrt[3]{md}\right)\log_2 d}} \geqslant C_6\frac{m\sqrt{md}}{\sqrt{(h+\sqrt[3]{md})\log_2 d}}, \end{aligned} \tag{3.10}$$

где $C_6 := \frac{1}{5\sqrt{C_4\max\{2,C_5\}}}$.

□

Рассматривая отдельно случаи $\sqrt[3]{md} > h$ и $\sqrt[3]{md} \leqslant h$, и взяв $C = \frac{C_6}{\sqrt{2}}$, получаем утверждение основной теоремы.

Теорема 4. *Существует такая абсолютная константа C, что для любого натурального n, любого $D \subseteq \{0,1\}^n, d = |D|$ неравенство*

$$\boldsymbol{U_{T_h}(f) \geqslant \begin{cases} C\frac{m\sqrt[3]{md}}{\log_2 d}, & \text{если } \sqrt[3]{md} > h, \\ C\frac{m\sqrt{md}}{\sqrt{h}\log_2 d}, & \text{если } \sqrt[3]{md} \leqslant h. \end{cases}}$$

выполнено для почти всех $f \in P_2(D,m)$ при $n \to \infty$, $n\log_2(n) = o(d)$, $\log_2(m) = o(d)$.

3.2 Верхние оценки

3.2.1 Параметры основных блоков

Для реализации булева оператора нам потребуются несколько различных блоков из главы 1. Напомним их характеристики.

1. Дешифратор D_n^1 (лемма 2):

$$\ell_1\left(D_n^1\right) = \mathcal{O}\left(2^n\right),\ \ell_2\left(D_n^1\right) = \mathcal{O}\left(2^{n/2}\right),\ \ell_3\left(D_n^1\right) = 1,\ \hat{U}\left(D_n^1\right) = \mathcal{O}\left(2^n\right).$$

2. Блок дешифраторов $D'_{n,k}$ (лемма 3):

$$\ell_1\left(D'_{n,k}\right) = \mathcal{O}\left(k \cdot 2^n\right),\ \ell_2\left(D'_{n,k}\right) = \mathcal{O}\left(n^2\right) + \mathcal{O}\left(nk\right),\ \ell_3\left(D'_{n,k}\right) = 1,$$
$$\hat{U}\left(D'_{n,k}\right) = \mathcal{O}\left(kn^2 \cdot 2^n\right) + \mathcal{O}\left(k^2 n \cdot 2^n\right).$$

3. Левый обратный блок $D'^{-1}_{n,k}$ (лемма 4):

$$\ell_1\left(D'^{-1}_{n,k}\right) = \mathcal{O}\left(k \cdot 2^n\right),\ \ell_2\left(D'^{-1}_{n,k}\right) = \mathcal{O}\left(kn^2\right),\ \ell_3\left(D'^{-1}_{n,k}\right) = 1,$$
$$\hat{U}\left(D'^{-1}_{n,k}\right) = \mathcal{O}\left(k^2 n^2 \cdot 2^n\right).$$

4. Блок $\vee_n^k$, реализующий k дизъюнкций от n переменных (лемма 7):

$$\ell_1\left(\vee_n^k\right) = 1,\ \ell_2\left(\vee_n^k\right) = k,\ \ell_3\left(\vee_n^k\right) = n,\ \hat{U}\left(\vee_n^k\right) = \mathcal{O}\left(nk\right).$$

5. Схема Q_g^1, такая что схема $D'^{-1}_{m/4,4} \circ Q_g^1 \circ D'_{k-l,4}$ реализует оператор $g : \{0,1\}^{4k-4l} \to \{0,1\}^m, n = 6k, m = 2^{12l}, G := Im(D'_{k-l,4})$ (лемма 10):

$$\ell_1(Q_g^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}),\ \ell_2(Q_g^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}),\ \ell_3(Q_g^1) = 1,$$
$$\hat{U}_{\{1\}\times G}(Q_g^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}), \hat{U}_{\{0\}\times G}(Q_g^1) = 4.$$

6. Схема W_f^1, реализующая оператор $f'(z, \vec{x}) = zf(\vec{x})$, где оператор $f : \{0,1\}^n \to \{0,1\}^m, (m \leqslant n)$ (лемма 11):

$$\ell_1\left(W_f^1\right) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right),\ \ell_2\left(W_f^1\right) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right),$$
$$\ell_3\left(W_f^1\right) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right),\ \hat{U}\left(W_f^1\right) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right).$$

3.2.2 Реализация булева оператора с близкими выходами

Введём дополнительный блок $C_{n,k,t}$ (см. рис. 3.6), реализующий тождественный оператор и «собирающий» выходы вместе.

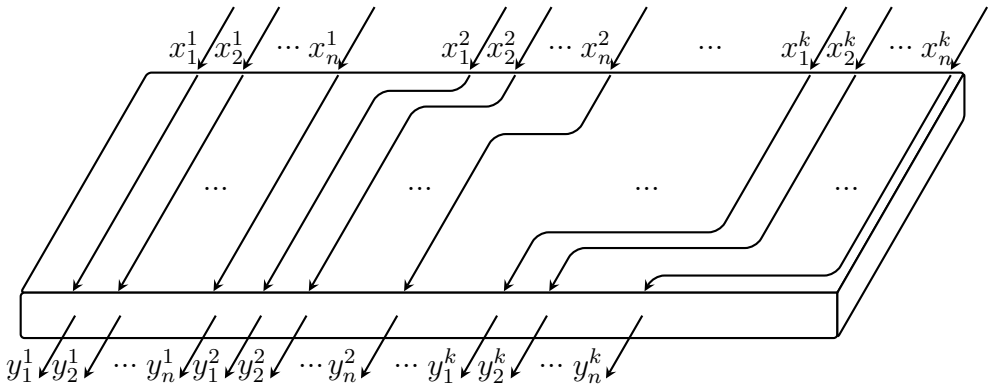


Рисунок 3.6 — Реализация блока $C_{n,k,t}$.

Лемма 39. *Существует объёмная схема $C_{n,k,t}$ высоты 1, имеющая k групп по n входов (всего nk входов), расстояние между каждыми группами равно t и реализующая тождественный оператор. Пусть $G = G_1 \times G_2 \times \ldots \times G_k; G_i \subset \{0,1\}^n, i \in [k]$. Если существует константа C_1 такая, что для любого $i \in [k]$ и для любого $v \in G_i$ выполнено $|v| \leqslant C_1$, то схема $C_{n,k,t}$ имеет следующие характеристики:*

1. $\ell_1(C_{n,k,t}) = \mathcal{O}((n+t)k)$, $\ell_2(C_{n,k,t}) = \mathcal{O}(nk)$, $\ell_3(C_{n,k,t}) = 1$;
2. $\hat{U}_G(C_{n,k,t}) = \mathcal{O}\left((n+t)k^2\right)$.

Доказательство. Оценим параметры схемы $C_{n,k,t}$.

Так как у нас есть k групп по n входов и расстояние между группами, то длину схемы можно оценить

$$\ell_1(C_{n,k,t}) = \mathcal{O}((n+t)k).$$

Ширина увеличивается на 1 всякий раз, когда нам нужно провести какой-то провод влево. Так как таковых проводов $k-1$ группа по n проводов (провода из первой группы не нужно проводить влево), то ширину схемы можно оценить

$$\ell_2(C_{n,k,t}) = \mathcal{O}(nk).$$

Высота схемы $C_{n,k,t}$ равна

$$\ell_3(C_{n,k,t}) = 1.$$

Оценим потенциал схемы $C_{n,k,t}$. Так как на каждую группу входов потенциал ограничен константой C_1, то это означает, что от каждой группы проводов активными будут не более C_1. Таким образом, всего будут активны не более $C_1 k$ проводов. Потенциал каждого провода по порядку оценим как сумму длины и ширины схемы $C_{n,k,t}$. В итоге получаем оценку

$$\hat{U}_G\left(C_{n,k,t}\right) = C_1 k \cdot \left(\mathcal{O}\left(\left(n+t\right)k\right) + \mathcal{O}\left(nk\right)\right) = \mathcal{O}\left(\left(n+t\right)k^2\right).$$

□

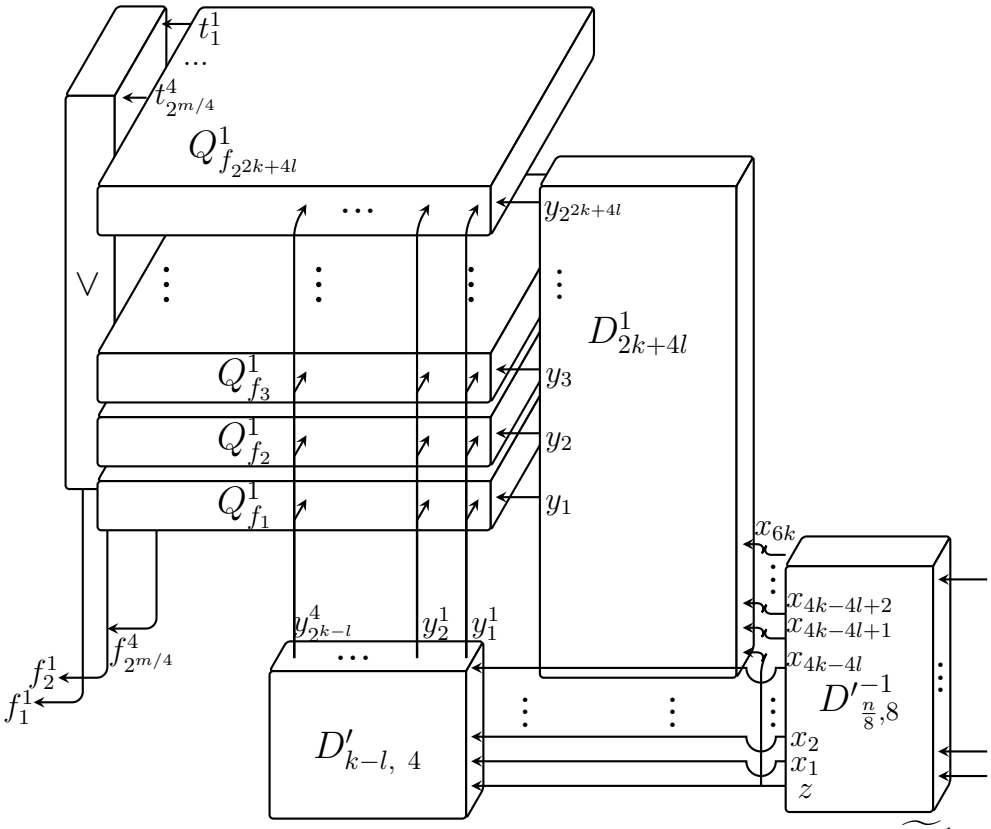


Рисунок 3.7 — Реализация блока $\widetilde{W}_f^1$.

Далее рассмотрим схему $\widetilde{W}_f^1$ (см. рис. 3.7), реализующую булев оператор $f : \{0,1\}^n \to \{0,1\}^m$, $m \leqslant n$. Эта схема отличается от схемы W_f^1 (*Ефимов А.А.*, *[26, лемма 7]*) отсутствием блока $D'^{-1}_{m/4,4}$ и наличием блока $D'^{-1}_{\frac{n}{8},8}$. Покажем, схема $\widetilde{W}_f^1$ имеет те же характеристики, что и схема W_f^1.

Лемма 40. *Для любого булева оператора $f : \{0,1\}^n \to \{0,1\}^m$, $(m \leqslant n)$ существует объёмная схема $\widetilde{W}_f^1$, что на схеме $D'^{-1}_{\frac{m}{4},4} \circ \widetilde{W}_f^1 \circ D^1_{\frac{n}{8},8}$ реализуется оператор $f'(z,\vec{x}) = zf(\vec{x})$, причём схема $\widetilde{W}_f^1$ обладает следующими характеристиками:*

1. $\ell_1\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right)$, $\ell_2\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right)$, $\ell_3\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right)$;
2. $\hat{U}(\widetilde{W}_f^1) = \mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right)$;
3. $V\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(m\cdot 2^n\right)$.

Доказательство. Так как от характеристики схемы $\widetilde{W}_f^1$ должны совпадать с характеристиками W_f^1, а они отличаются удалением блока $D'^{-1}_{m/4,4}$ и добавлением блока $D'^{-1}_{\frac{n}{8},8}$, то достаточно показать, что характеристики блока $D'^{-1}_{\frac{n}{8},8}$ не превышают заявленных характеристик.

$$\ell_1\left(D'^{-1}_{\frac{n}{8},8}\right) = \mathcal{O}\left(8\cdot 2^{\frac{n}{8}}\right) = \mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right).$$
$$\ell_3\left(D'^{-1}_{\frac{n}{8},8}\right) = 1.$$
$$\hat{U}\left(D'^{-1}_{\frac{n}{8},8}\right) = \mathcal{O}\left(8^2\cdot\frac{n^2}{8^2}\cdot 2^{\frac{n}{8}}\right) = \mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right).$$

□

Теперь построим схему $\widetilde{W}_f^1$ для булева оператора $f : \{0,1\}^n \to \{0,1\}^m$, где $n < m \leqslant 2^{n/2}$.

Лемма 41. *Для любого булева оператора $f : \{0,1\}^n \to \{0,1\}^m$, $(n < m \leqslant 2^{n/2})$ существует обвёмная схема $\widetilde{W}_f^1 \in T_{\text{near}}$ со входами $z, x_1, x_2, \ldots, x_n$ на m выходах которой на допустимых наборах $(z \geqslant x_1 \vee \ldots \vee x_n)$ реализуется оператор $f'(z,\vec{x}) = zf(\vec{x})$, причём схема $\widetilde{W}_f^1$ обладает следующими характеристиками:*

1. $\ell_1\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right)$, $\ell_2\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right)$, $\ell_3\left(\widetilde{W}_f^1\right) = \mathcal{O}(\sqrt[3]{m}\cdot 2^{n/3})$;
2. $\hat{U}\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(\frac{m}{n}\cdot\sqrt[3]{m}\cdot 2^{n/3}\right)$;
3. $V\left(\widetilde{W}_f^1\right) = \mathcal{O}(m\cdot 2^n)$.

Доказательство. Рассмотрим случай, когда $n = 8t, k = \sqrt[3]{\frac{m}{n}}$. Отметим, что условие $m \leqslant 2^{n/2} \leqslant n^2\cdot 2^n$ можно переписать как $k = \sqrt[3]{\frac{m}{n}} \leqslant \sqrt[3]{n}\cdot 2^{n/3}$, чем и будем пользоваться в дальнейших оценках. Покажем, что тогда схема, изображенная на рис. 3.8 реализует оператор f.

Мы подаем входные переменные $z, x_1, \ldots, x_n$ на вход блоку дешифраторов $D'_{n/8,8}$. Далее все эти провода в «зашифрованном» виде подводим к каждому

из k^3 соответствующих блоков $\widetilde{W}^1_{f_{i,j,l}}$, которые реализуют оператор $f_{i,j,l}$ от n переменных. Все провода от блока $D'_{n/8,8}$ к блокам $\widetilde{W}^1_{f_{i,j,l}}$ на рис. 3.8 изображены пунктирными линиями для удобства восприятия. После этого выходы каждого блока $\widetilde{W}^1_{f_{i,j,l}}$ подаются в «зашифрованном» виде. Далее, собирая все выходы блоков $\widetilde{W}^1_{f_{i,j,l}}$ с помощью двух ярусов блоков $C_{\alpha,k,\beta}$ и $C_{k,k,\sqrt[3]{n}\cdot 2^{n/3}}$, получаем выходы оператора в «зашифрованном» виде f, но при этом расположенные рядом. В конце «расшифровываем» выходы с помощью блоков $D'^{-1}_{n/4,4k}$.

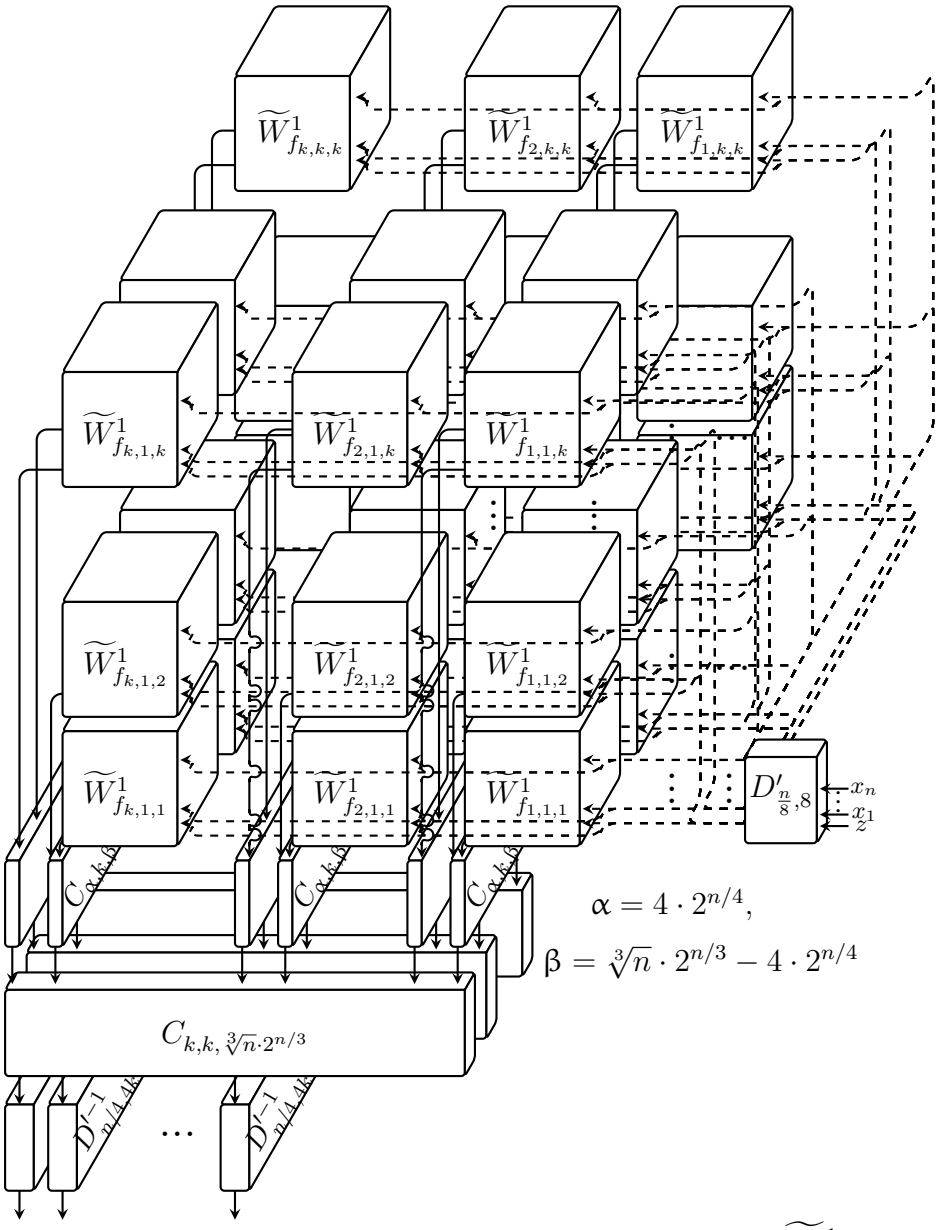


Рисунок 3.8 — Реализация блока $\widetilde{W}^1_f$ $(n < m \leqslant 2^{n/2})$.

Оценим параметры схемы $\widetilde{W}_f^1$.

$$\ell_1\left(\widetilde{W}_f^1\right) = k\cdot\left(\ell_1\left(\widetilde{W}_{f_{i,j,l}}^1\right)+k\right)+\ell_2\left(D_{n/8,8}\right) =$$
$$= \sqrt[3]{\frac{m}{n}}\cdot\left(\mathcal{O}\left(\sqrt[3]{n}\cdot 2^{n/3}\right)+\sqrt[3]{\frac{m}{n}}\right)+\mathcal{O}\left(n^2/16+n\right) =$$
$$= \mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right).$$

$$\ell_2\left(\widetilde{W}_f^1\right) = k\cdot\left(\ell_2\left(\widetilde{W}_{f_{i,j,l}}^1\right)+1\right) = \sqrt[3]{\frac{m}{n}}\cdot\left(\mathcal{O}\left(\sqrt[3]{n}\cdot 2^{n/3}\right)+1\right) =$$
$$= \mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right).$$
$$\ell_3\left(\widetilde{W}_f^1\right) = k\cdot\ell_2\left(\widetilde{W}_{f_{i,j,l}}^1\right)+2\cdot\ell_3\left(C_{k,k,\sqrt[3]{n}\cdot 2^{n/3}}\right) =$$
$$= \sqrt[3]{\frac{m}{n}}\cdot\mathcal{O}\left(\sqrt[3]{n}\cdot 2^{n/3}\right)+\mathcal{O}\left(k^2\right) = \mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right).$$

Оценим объём схемы $\widetilde{W}_f^1$:

$$V\left(\widetilde{W}_f^1\right) \leqslant \ell_1\left(\widetilde{W}_f^1\right)\cdot\ell_2\left(\widetilde{W}_f^1\right)\cdot\ell_3\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(m\cdot 2^n\right).$$

Оценим потенциал схемы.

1. Блок дешифраторов $D'_{n/8,8}$:

$$U_1 \leqslant \hat{U}\left(D'_{n/8,8}\right) = \mathcal{O}\left(8n\cdot 2^{n/8}+n^2/8\cdot 2^{n/8}\right) = \mathcal{O}\left(n^2\cdot 2^{n/8}\right) =$$
$$= \mathcal{O}\left(\frac{m}{n}\cdot\sqrt[3]{m}\cdot 2^{n/3}\right).$$

2. Далее на выходе из блока дешифраторов $D'_{n/8,8}$ будут активны 8 проводов, которые мы подводим к k^3 блокам $\widetilde{W}_{f_{i,j,l}}^1$. Длину каждого активного провода оценим как $\ell_1\left(\widetilde{W}_f^1\right)+\ell_2\left(\widetilde{W}_f^1\right)+\ell_3\left(\widetilde{W}_f^1\right)$. Таким образом, имеем оценку:

$$U_2 \leqslant 8\cdot k^3\cdot\left(\ell_1\left(\widetilde{W}_f^1\right)+\ell_2\left(\widetilde{W}_f^1\right)+\ell_3\left(\widetilde{W}_f^1\right)\right) = \frac{m}{n}\cdot\mathcal{O}\left(\sqrt[3]{m}\cdot 2^{n/3}\right) =$$
$$= \mathcal{O}\left(\frac{m}{n}\cdot\sqrt[3]{m}\cdot 2^{n/3}\right).$$

3. Оценим потенциал всех k^3 блоков $\widetilde{W}_{f_{i,j,l}}^1$:

$$U_3 \leqslant k^3\cdot\hat{U}\left(\widetilde{W}_{f_{i,j,l}}^1\right) = \frac{m}{n}\cdot\mathcal{O}\left(\sqrt[3]{n}\cdot 2^{n/3}\right) = \mathcal{O}\left(\frac{m}{n}\cdot\sqrt[3]{n}\cdot 2^{n/3}\right).$$

4. Далее на выходе каждого блока $\widetilde{W}^1_{f_{i,j,l}}$ будут активны 4 провода, которые мы подводим к блокам $C_{\alpha,k,\beta}$, где $\alpha = 4 \cdot 2^{n/4}$, $\beta = \sqrt[3]{n} \cdot 2^{n/3} - 4 \cdot 2^{n/4}$. Длину каждого активного провода оценим как $\ell_3\left(\widetilde{W}^1_f\right)$. Таким образом, имеем оценку:

$$U_4 \leqslant k^3 \cdot 4 \cdot \ell_3\left(\widetilde{W}^1_f\right) = \frac{m}{n} \cdot \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right) = \mathcal{O}\left(\frac{m}{n} \cdot \sqrt[3]{m} \cdot 2^{n/3}\right).$$

5. Оценим потенциал всех k^2 блоков $C_{\alpha,k,\beta}$. Отметим, что в каждом блоке $C_{\alpha,k,\beta}$ на каждую группу входов подается ровно по 4 активных выхода блока $\widetilde{W}^1_{f_{i,j,l}}$. Таким образом, соблюдены условия леммы 39 и мы имеем оценку:

$$\begin{aligned} U_5 &\leqslant k^2 \cdot \hat{U}\left(C_{\alpha,k,\beta}\right) = \left(\frac{m}{n}\right)^{\frac{2}{3}} \cdot \mathcal{O}\left((\alpha+\beta)\,k^2\right) = \\ &= \left(\frac{m}{n}\right)^{\frac{2}{3}} \cdot \mathcal{O}\left(\sqrt[3]{n} \cdot 2^{n/3} \cdot \left(\frac{m}{n}\right)^{\frac{2}{3}}\right) = \\ &= \left(\frac{m}{n}\right)^{\frac{2}{3}} \cdot \mathcal{O}\left(\sqrt[3]{n} \cdot 2^{n/3} \cdot \left(\frac{m}{n}\right)^{\frac{2}{3}}\right) = \mathcal{O}\left(\frac{m}{n} \cdot \sqrt[3]{m} \cdot 2^{n/3}\right). \end{aligned}$$

6. Оценим потенциал всех $\alpha \cdot k$ блоков $C_{k,k,\sqrt[3]{n} \cdot 2^{n/3}}$. Заметим, что на входе всех блоков активны будут ровно $4 \cdot k^3$ (это количество активных выходов всех блоков $\widetilde{W}^1_{f_{i,j,l}}$, прошедших через верхний ярус тождественных блоков $C_{\alpha,k,\beta}$). Потенциал от каждого провода оценим $l\left(C_{k,k,\sqrt[3]{n} \cdot 2^{n/3}}\right) + w\left(C_{k,k,\sqrt[3]{n} \cdot 2^{n/3}}\right)$. Таким образом, имеем оценку:

$$\begin{aligned} U_6 &\leqslant 4 \cdot k^3 \cdot \left(\mathcal{O}\left(\left(k + \sqrt[3]{n} \cdot 2^{n/3}\right) k\right) + \mathcal{O}\left(\sqrt[3]{n} \cdot 2^{n/3} \cdot k\right)\right) = \\ &= \mathcal{O}\left(\frac{m}{n} \cdot \sqrt[3]{m} \cdot 2^{n/3}\right). \end{aligned}$$

7. Оценим потенциал всех k^2 блоков $D'^{-1}_{n/4,4k}$:

$$\begin{aligned} U_7 &\leqslant k^2 \cdot \hat{U}\left(D'^{-1}_{n/4,4k}\right) = k^2 \cdot \mathcal{O}\left(\frac{n^2}{16} \cdot 16k^2 \cdot 2^{n/4}\right) = \\ &= \mathcal{O}\left(\frac{m}{n} \cdot \sqrt[3]{m} \cdot n^{2/3} \cdot 2^{n/4}\right) = \mathcal{O}\left(\frac{m}{n} \cdot \sqrt[3]{m} \cdot 2^{n/3}\right). \end{aligned}$$

В итоге, имеем следующую оценку потенциала схемы $\widetilde{W}^1_f$:

$$\hat{U}\left(\widetilde{W}^1_f\right) \leqslant U_1 + U_2 + U_3 + U_4 + U_5 + U_6 + U_7 = \mathcal{O}\left(\frac{m}{n} \cdot \sqrt[3]{m} \cdot 2^{n/3}\right).$$

Таким образом, получаем верное утверждение теоремы в случае $n = 8t, k = \sqrt[3]{\frac{m}{n}}$. Если же $n = 8t + r, m = k^3 n + l$, где $1 \leqslant r \leqslant 7, 1 \leqslant l \leqslant$

$\leqslant \left(\left(3k^2+3k+1\right)n-1\right)$, то построим схему для $n'=8t+8, m'=(k+1)^3 n$ и на последние $8-r$ входов подадим константу 0, а лишние выходы доопределим нулем. Заметим, что в данном случае получим искомую схему и константы в оценках увеличатся не более, чем в константу раз, а значит оценки по порядку останутся верными.

□

Далее построим схему $\widetilde{W}_f^1$ для булева оператора $f:\{0,1\}^n \to \{0,1\}^{m_0}$, где $m_0 = 2^{n/2}$, причём выходы схемы $\widetilde{W}_f^1$ будут расположены на одной прямой.

Лемма 42. *Для любого булева оператора $f:\{0,1\}^n \to \{0,1\}^{m_0}$, $(m_0 = 2^{n/2})$ существует объёмная схема $\widetilde{W}_f^1 \in T_{\text{near}}$ со входами $z, x_1, x_2, \ldots, x_n$ на m_0 выходах которой на допустимых наборах $(z \geqslant x_1 \vee \ldots \vee x_n)$ реализуется оператор $f'(z,\vec{x}) = zf(\vec{x})$, причём схема $\widetilde{W}_f^1$ обладает следующими характеристиками:*

1. $\ell_1\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(2^{n/2}\right)$, $\ell_2\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(2^{n/2}\right)$,
   $\ell_3\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(m_0\right) = \mathcal{O}\left(2^{n/2}\right)$;
2. $\hat{U}\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(\frac{m_0}{n}\cdot 2^{n/2}\right)$;
3. $V\left(\widetilde{W}_f\right) = \mathcal{O}\left(m_0 \cdot 2^n\right)$.

Доказательство. Рассмотрим случай, когда $n = 8t$. Обозначим $k_0 = \sqrt[3]{\frac{m_0}{n}} = \frac{2^{n/6}}{n^{1/3}}$. Покажем, что тогда схема, изображенная на рис. 3.9 реализует оператор f.

Мы подаем входные переменные $z, x_1, \ldots, x_n$ на вход блока $\widetilde{W'}_f^1$ (который отличается от блока $\widetilde{W}_f^1$ отсутствием блоков $D'^{-1}_{n/4,4k}$, стоящих на выходах, см. Рис. 3.8), реализующий оператор f с n входами и $m_0 = 2^{n/2}$ выходами. Далее, собирая все «зашифрованные» выходы блока $\widetilde{W'}_f^1$ и расшифровывая их с помощью блоков $D'^{-1}_{n/4,4k_0}$, получаем выходы оператора f.

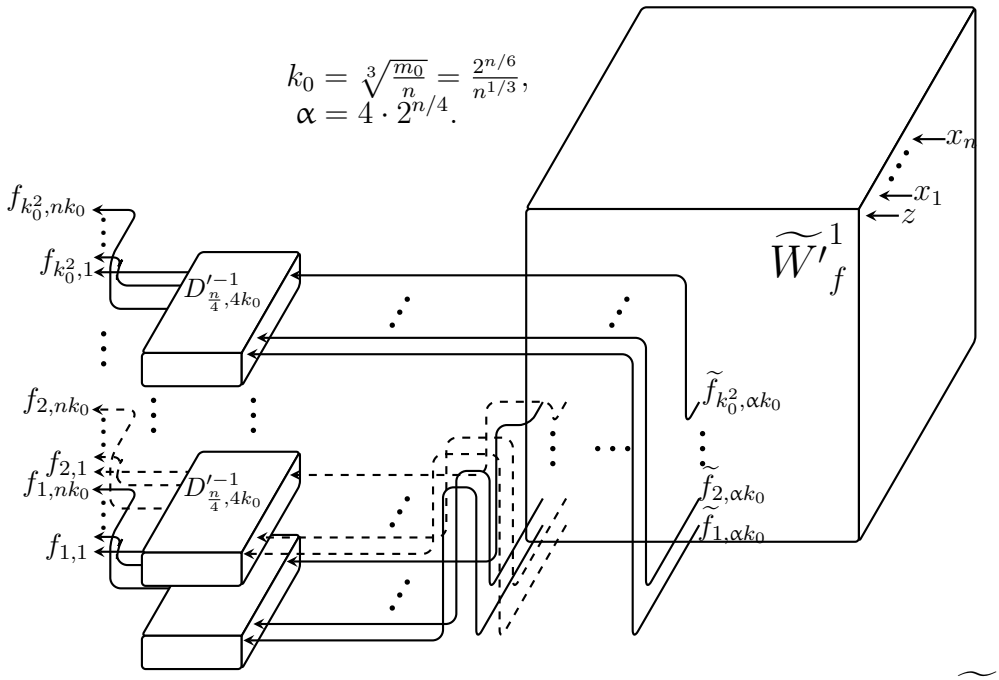


Рисунок 3.9 — Реализация вспомогательного блока $\widetilde{W}^1_f$ ($m_0 = 2^{n/2}$).

Оценим параметры схемы $\widetilde{W}^1_f$.

$$\begin{aligned}
\ell_1\left(\widetilde{W}^1_f\right) &= \ell_1\left(\widetilde{W'}^1_f\right) + \mathcal{O}\left(k_0^2\right) + \ell_2\left(D^{-1}_{n/4,4k_0}\right) = \mathcal{O}\left(\sqrt[3]{m_0}\cdot 2^{n/3}\right) + \\
&+ \mathcal{O}\left(\frac{2^{n/3}}{n^{2/3}}\right) + \mathcal{O}\left(k_0\cdot n^2\right) = \mathcal{O}\left(2^{n/2}\right) + \mathcal{O}\left(n^{1/3}\cdot 2^{n/3}\right) = \\
&= \mathcal{O}\left(2^{n/2}\right).\\
\ell_2\left(\widetilde{W}^1_f\right) &= \ell_2\left(\widetilde{W'}^1_f\right) + \ell_1\left(D^{-1}_{n/4,4k_0}\right) = \mathcal{O}\left(\sqrt[3]{m_0}\cdot 2^{n/3}\right) + \mathcal{O}\left(\alpha k_0\right) = \\
&= \mathcal{O}\left(2^{n/2}\right) + \mathcal{O}\left(\frac{2^{5/12}}{n^{1/3}}\right) = \mathcal{O}\left(2^{n/2}\right).\\
\ell_3\left(\widetilde{W}^1_f\right) &= \ell_3\left(\widetilde{W'}^1_f\right) = \mathcal{O}\left(2^{n/2}\right) = \mathcal{O}\left(m_0\right).
\end{aligned}$$

Оценим объём схемы W^1_f:

$$V\left(\widetilde{W}^1_f\right) \leqslant \ell_1\left(\widetilde{W}^1_f\right)\cdot\ell_2\left(\widetilde{W}^1_f\right)\cdot\ell_3\left(\widetilde{W}^1_f\right) = \mathcal{O}\left(m_0\cdot 2^n\right).$$

Оценим потенциал схемы.

1. Блок $\widetilde{W'}^1_f$:

$$U_1 \leqslant \hat{U}\left(\widetilde{W'}^1_f\right) = \mathcal{O}\left(\frac{m_0}{n}\cdot\sqrt[3]{m_0}\cdot 2^{n/3}\right) = \mathcal{O}\left(\frac{m_0}{n}\cdot 2^{n/2}\right).$$

2. Далее на выходе из блока $\widetilde{W'}^1_f$ среди всех «зашифрованных» выходов $\widetilde{f}_{i,j}$ будут активны ровно $4k_0^3$ (это следует из того, что блок $\widetilde{W'}^1_f$

состоит из k_0^3 блоков $\widetilde{W}^1_{f_{i,j,k}}$, выходы которых шифровались с помощью блока дешифраторов $D'_{n/4,4}$). Длину каждого провода оценим $\ell_1\left(\widetilde{W}^1_f\right) + 3\ell_3\left(\widetilde{W}^1_f\right)$. Таким образом, имеем оценку:

$$U_2 \leqslant 4k_0^3 \cdot \left(\ell_1\left(\widetilde{W}^1_f\right) + 3\ell_3\left(\widetilde{W}^1_f\right)\right) = \mathcal{O}\left(\frac{m_0}{n} \cdot 2^{n/2}\right).$$

3. Оценим потенциал всех k_0^2 блоков $D'^{-1}_{n/4,4k_0}$:

$$U_3 \leqslant k_0^2 \cdot \hat{U}\left(D'^{-1}_{n/4,4k_0}\right) = k_0^2 \cdot \mathcal{O}\left(n^2 \cdot k_0^2 \cdot 2^{n/4}\right) =$$
$$= \mathcal{O}\left(\frac{m_0}{n} \cdot \frac{m_0^{1/3}}{n^{1/3}} \cdot n^2 \cdot 2^{n/4}\right) = \mathcal{O}\left(\frac{m_0}{n} \cdot n^{5/3} \cdot 2^{5n/12}\right) =$$
$$= \mathcal{O}\left(\frac{m_0}{n} \cdot 2^{n/2}\right).$$

4. Оценим потенциал всех проводов, выходящих из блоков $D'^{-1}_{n/4,4k_0}$. В каждом таком блоке nk_0 проводов, длину каждого можно оценить $2nk_0$. Так как в схеме имеется k_0^2 блоков $D^{-1}_{n/4,4k_0}$, то имеем оценку:

$$U_4 \leqslant nk_0 \cdot 2nk_0 \cdot k_0^2 = \mathcal{O}\left(\frac{m_0}{n} \cdot \frac{m_0^{1/3}}{n^{1/3}} \cdot n^2\right) = \mathcal{O}\left(\frac{m_0}{n} \cdot n^{5/3} \cdot 2^{n/6}\right) =$$
$$= \mathcal{O}\left(\frac{m_0}{n} \cdot 2^{n/2}\right).$$

В итоге, имеем следующую оценку потенциала схемы $\widetilde{W}^1_f$:

$$\hat{U}\left(\widetilde{W}^1_f\right) \leqslant U_1 + U_2 + U_3 + U_4 = \mathcal{O}\left(\frac{m_0}{n} \cdot 2^{n/2}\right).$$

Таким образом, получаем верное утверждение теоремы в случае $n = 8t$. Если же $n = 8t + r$, где $r \in [7]$, то построим схему для $n' = 8t + 8$ и на последние $8 - r$ входов подадим константу 0. Заметим, что в данном случае получим искомую схему и константы в оценках увеличатся не более, чем в константу раз, а значит оценки по порядку останутся верными.

□

Теперь построим схему $\widetilde{W}^1_f$ для булева оператора $f : \{0,1\}^n \to \{0,1\}^m$, где $m > 2^{n/2}$.

Лемма 43. *Для любого булева оператора $f : \{0,1\}^n \to \{0,1\}^m, (m > 2^{n/2})$ существует объёмная схема $\widetilde{W}^1_f \in T_{\text{near}}$ со входами $z, x_1, x_2, \ldots, x_n$ на m выходах которой на допустимых наборах $(z \geqslant x_1 \vee \ldots \vee x_n)$ реализуется оператор $f'(z, \vec{x}) = zf(\vec{x})$, причём схема $\widetilde{W}^1_f$ обладает следующими характеристиками:*

1. $\ell_1\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(2^{n/2}\right),\ \ell_2\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(2^{n/2}\right),\ \ell_3\left(\widetilde{W}_f^1\right) = \mathcal{O}(m);$
2. $\hat{U}\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(\frac{m}{n} \cdot 2^{n/2}\right);$
3. $V\left(\widetilde{W}_f\right) = \mathcal{O}\left(m \cdot 2^n\right).$

Доказательство. Рассмотрим случай, когда $n = 8t, m = k \cdot 2^{n/2}$. Покажем, что тогда схема, изображенная на рис. 3.10 реализует оператор f.

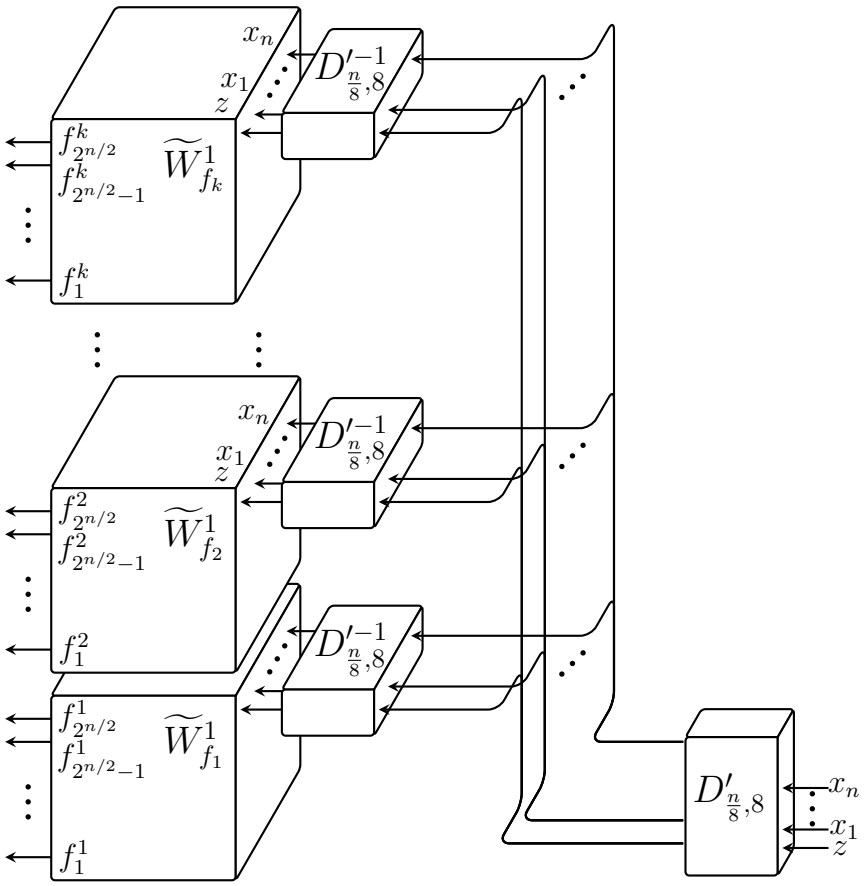


Рисунок 3.10 — Реализация блока $\widetilde{W}_f^1$ $(m > 2^{n/2})$.

Мы подаем входные переменные $z, x_1, \ldots, x_n$ на вход блоку дешифраторов $D'_{n/8,8}$, далее все эти провода подводим к каждому из k блоков обратных дешифраторов $D^{-1}_{n/8,8}$. «Расшифрованные» переменные $z, x_1, \ldots, x_n$ мы подаем на соответствующий блок $\widetilde{W}_{f_i}^1$, реализующий оператор f_i с n входами и $m_0 = 2^{n/2}$ выходами. Далее, собирая все выходы блоков $\widetilde{W}_{f_i}^1$, получаем выходы оператора f.

Оценим параметры схемы $\widetilde{W}_f^1$.

$$\begin{aligned}
\ell_1\left(\widetilde{W}_f^1\right) &= \ell_1\left(\widetilde{W}_{f_i}^1\right) + \ell_2\left(D'^{-1}_{n/8,8}\right) + \mathcal{O}\left(8\cdot 2^{n/8}\right) + \ell_2\left(D'_{n/8,8}\right) = \\
&= \mathcal{O}\left(\sqrt[3]{m_0}\cdot 2^{n/3}\right) + \mathcal{O}\left(n^2/8\right) + \mathcal{O}\left(8\cdot 2^{n/8}\right) + \mathcal{O}\left(n^2/16+n\right) = \\
&= \mathcal{O}\left(2^{n/2}\right) + \mathcal{O}\left(8\cdot 2^{n/8}\right) = \mathcal{O}\left(2^{n/2}\right).\\
\ell_2\left(\widetilde{W}_f^1\right) &= \ell_2\left(\widetilde{W}_{f_i}^1\right) = \mathcal{O}\left(\sqrt[3]{m_0}\cdot 2^{n/3}\right) = \mathcal{O}\left(2^{n/2}\right).\\
\ell_3\left(\widetilde{W}_f^1\right) &= k\cdot\ell_3\left(\widetilde{W}_{f_i}^1\right) = \frac{m}{2^{n/2}}\cdot\mathcal{O}\left(\sqrt[3]{m_0}\cdot 2^{n/3}\right) = \frac{m}{2^{n/2}}\cdot\mathcal{O}\left(2^{n/2}\right) = \\
&= \mathcal{O}(m).
\end{aligned}$$

Оценим объём схемы $\widetilde{W}_f^1$:

$$V\left(\widetilde{W}_f^1\right) \leqslant \ell_1\left(\widetilde{W}_f^1\right)\cdot\ell_2\left(\widetilde{W}_f^1\right)\cdot\ell_3\left(\widetilde{W}_f^1\right) = \mathcal{O}\left(m\cdot 2^n\right).$$

Оценим потенциал схемы.

1. Блок дешифраторов $D'_{n/8,8}$:

$$\begin{aligned}
U_1 \leqslant \hat{U}\left(D'_{n/8,8}\right) &= \mathcal{O}\left(8n\cdot 2^{n/8} + n^2/8\cdot 2^{n/8}\right) = \mathcal{O}\left(n^2\cdot 2^{n/8}\right) = \\
&= \mathcal{O}\left(\frac{m}{n}\cdot 2^{n/2}\right).
\end{aligned}$$

2. Далее на выходе из блока дешифраторов $D'_{n/8,8}$ будут активны 8 проводов, которые мы подводим к блокам $D^{-1}_{n/8,8}$. Таким образом, имеем оценку:

$$U_2 \leqslant 8\cdot\left(\ell_3\left(\widetilde{W}_f^1\right) + k\cdot\mathcal{O}\left(8\cdot 2^{n/8}\right)\right) = \mathcal{O}\left(m\right) = \mathcal{O}\left(\frac{m}{n}\cdot 2^{n/2}\right).$$

3. Оценим потенциал всех k блоков $D'^{-1}_{n/8,8}$:

$$U_3 \leqslant k\cdot\hat{U}\left(D'^{-1}_{n/8,8}\right) = \frac{m}{2^{n/2}}\cdot\mathcal{O}\left(n^2\cdot 2^{n/8}\right) = \mathcal{O}(m) = \mathcal{O}\left(\frac{m}{n}\cdot 2^{n/2}\right).$$

4. Оценим потенциал всех k блоков $\widetilde{W}_{f_i}^1$:

$$U_4 \leqslant k\cdot\hat{U}\left(\widetilde{W}_{f_i}^1\right) = \frac{m}{2^{n/2}}\cdot\mathcal{O}\left(\frac{m_0}{n}\cdot 2^{n/2}\right) = \mathcal{O}\left(\frac{m}{n}\cdot 2^{n/2}\right).$$

В итоге, имеем следующую оценку потенциала схемы $\widetilde{W}_f^1$:

$$\hat{U}\left(\widetilde{W}_f^1\right) = U_1 + U_2 + U_3 + U_4 = \mathcal{O}\left(\frac{m}{n}\cdot 2^{n/2}\right).$$

Таким образом, получаем верное утверждение теоремы в случае $n = 8t, m = k \cdot 2^{n/2}$. Если же $n = 8t + r, m = k \cdot 2^{n/2} + l$, где $r \in [7], l \in [2^{n/2} - 1]$, то построим схему для $n' = 8t + 8, m' = (k+1)2^{n/2}$ и на последние $8 - r$ входов подадим константу 0. Заметим, что в данном случае получим искомую схему и константы в оценках увеличатся не более, чем в константу раз, а значит оценки по порядку останутся верными.

□

В качестве следствия из леммы 40, леммы 41 и леммы 43 докажем теорему 5, для удобства обозначив $K_f = \widetilde{W}_f$.

Теорема 5. *Для любого булева оператора $f : \{0,1\}^n \to \{0,1\}^m$, существует объёмная схема $K_f \in T_{\text{near}}$ со входами $x_1, x_2, \ldots, x_n$ на m выходах которой реализуется оператор f, причём схема K_f обладает следующими характеристиками:*

Если $m \leqslant n$:

1. $\ell_1(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right)$, $\ell_2(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right)$, $\ell_3(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right)$.
2. $\boldsymbol{\hat{U}(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right)}$.
3. $V(K_f) = \mathcal{O}(m \cdot 2^n)$.

Если $n < m \leqslant 2^{n/2}$:

1. $\ell_1(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right)$, $\ell_2(K_f) = \mathcal{O}\left(\sqrt[3]{m} \cdot 2^{n/3}\right)$, $\ell_3(K_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$.
2. $\boldsymbol{\hat{U}(K_f) = \mathcal{O}\left(\frac{m}{n} \cdot \sqrt[3]{m} \cdot 2^{n/3}\right)}$.
3. $V(K_f) = \mathcal{O}(m \cdot 2^n)$.

Если $m > 2^{n/2}$:

1. $\ell_1(K_f) = \mathcal{O}\left(2^{n/2}\right)$, $\ell_2(K_f) = \mathcal{O}\left(2^{n/2}\right)$, $\ell_3(K_f) = \mathcal{O}(m)$.
2. $\boldsymbol{\hat{U}(K_f) = \mathcal{O}\left(\frac{m}{n} \cdot 2^{n/2}\right)}$.
3. $V(K_f) = \mathcal{O}(m \cdot 2^n)$.

Доказательство. Построим схему K_f, используя лемму 40 при $m \leqslant n$, лемму 41 при $n < m \leqslant 2^{n/2}$ или лемму 43 при $m > 2^{n/2}$. Подадим в схеме $\widetilde{W}_f^1$ на вход z константу 1. Полученная таким образом схема K_f реализует оператор $f(x_1, x_2, \ldots, x_n)$ на всех наборах $x_1, x_2, \ldots, x_n$ и её параметры остаются такими же по порядку, как и у схемы $\widetilde{W}_f^1$.

□

В качестве следствия из теорем 4 и 5 докажем утверждение.

Следствие 3. *Для почти всех* $f \in P_2(n,m)$, *при* $m \geqslant n, n \to \infty$, $\log_2(m) = o(2^n)$ *верно равенство:*

$$\boldsymbol{U_{T_{\text{near}}}(f) = \Theta\left(\frac{m}{n} \cdot \left(\min(m, 2^{n/2})\right)^{1/3} \cdot 2^{n/3}\right).}$$

Доказательство. Так как согласно теореме 5 для любого оператора $f \in P_2(n,m)$ существует объёмная схема $K_f \in T_{\text{near}}$, такая, что $\hat{U}\left(\widetilde{W}_f\right) = \mathcal{O}\left(\frac{m}{n} \cdot \sqrt[3]{m} \cdot 2^{n/3}\right)$, то

$$U_{T_{\text{near}}}(f) \leqslant \Theta\left(\frac{m}{n} \cdot \left(\min(m, 2^{n/2})\right)^{1/3} \cdot 2^{n/3}\right).$$

Покажем, что выполнено условие теоремы 4. Так как длина h дерева выходов минимальна, то она равна $\mathcal{O}(m)$, $d = 2^n$. Условия $n \log_2 n = o(d), m = 2^{o(d)}$ выполнены. Тогда условие $\sqrt[3]{md} \geqslant h$ можно переписать как $m \leqslant 2^{n/2}$ (в случае $h = \sqrt[3]{md}$ нижняя оценка одинакова, поэтому его тоже можно включить). Таким образом из теоремы 4 получаем оценку:

$$U_{T_{\text{near}}}(f) \geqslant \Theta\left(\frac{m}{n} \cdot \left(\min(m, 2^{n/2})\right)^{1/3} \cdot 2^{n/3}\right).$$

Соединив вместе две оценки, получим необходимое утверждение.

□

Заключение

Основные результаты работы заключаются в следующем.

1. Получена верхняя оценка функции Шеннона потенциала объёмных схем, реализующих булевы функции и операторы.
2. Получена нижняя оценка функции Шеннона потенциала объёмных схем, реализующих частичные булевы операторы.
3. Получена верхняя оценка функции Шеннона потенциала объёмных схем, реализующих булевы операторы в классе схем с близкими выходами.
4. Получена нижняя оценка функции Шеннона потенциала объёмных схем, реализующих булевы операторы в классе схем с ограничениями на расстояние между выходами.

Дальнейшее изучение объёмных схем предполагает получение верхней оценки потенциала для частичных операторов и, как следствие, получение функции Шеннона потенциала частичных операторов. Особый интерес представляет реализация объёмными схемами различных классов булевых функций, например монотонных, с малым числом единиц и т.д. Также автору видится интересным изучение многомерных схем и получение аналогичных оценок и результатов.

Список литературы

1. *Muller, D. E.* Complexity in Electronics Switching Circuits / D. E. Muller // IRE Transactions on Electronic Computers. — 1956. — EC—5, no. 1. — P. 15—19.
2. *Лупанов, О. Б.* Об одном методе синтеза схем / О. Б. Лупанов // Известия ВУЗ, Радиофизика. Горький, издательство ГУ. — 1958. — № 1. — С. 120—140.
3. *Лупанов, О. Б.* О синтезе некоторых классов управляющих систем / О. Б. Лупанов // Проблемы кибернетики. Наука. Физматгиз. — 1963. — № 10. — С. 64—97.
4. *Вайнцвайг, М. Н.* О мощности схем из функциональных элементов / М. Н. Вайнцвайг // Докл. АН СССР. Наука. — 1961. — 139:2. — С. 320—323.
5. *Касим-Заде, О. М.* Об одной мере сложности схем из функциональных элементов / О. М. Касим-Заде // Проблемы кибернетики. Наука. — 1981. — № 38. — С. 117—179.
6. *Шуткин, Ю. С.* Об одновременной минимизации объёмной и временной сложности контактных и вентильных схем / Ю. С. Шуткин // Интеллектуальные системы. Теория и приложения. — 2010. — 24:1—4. — С. 595—615.
7. *Кравцов, С. С.* О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов / С. С. Кравцов // Проблемы кибернетики. Наука. — 1967. — № 19. — С. 285—293.
8. *Коршунов, А. Д.* Об оценках сложности из объемных функциональных элементов и объёмных схем из функциональных элементов / А. Д. Коршунов // Проблемы кибернетики. Наука. — 1967. — № 19. — С. 275—283.
9. *Сытдыков, Т. Р.* Сложность синтеза многомерных прямоугольных схем / Т. Р. Сытдыков // Интеллектуальные системы. Теория и приложения. — 2019. — 23:3. — С. 61—80.
10. *Сытдыков, Т. Р.* Сложность многослойных d-мерных схем / Т. Р. Сытдыков, Г. В. Калачёв // Интеллектуальные системы. Теория и приложения. — 2021. — 25:2. — С. 131—154.
11. *Шкаликова, Н. А.* О реализации булевых функций схемами из клеточных элементов / Н. А. Шкаликова // Математические вопросы кибернетики. Наука. — 1989. — № 2. — С. 177—197.

12. *Шкаликова, Н. А.* О сложности реализации некоторых функций клеточными схемами / Н. А. Шкаликова // Сборник работ по математической кибернетике. — 1976. — № 1. — С. 102—115.
13. *Шкаликова, Н. А.* О соотношении сложностей плоских и объёмных схем из функциональных элементов / Н. А. Шкаликова // Методы дискретного анализа в оценках сложности управляющих систем. Новосибирск. — 1982. — № 38. — С. 87—107.
14. Об одном подходе к оценке пространственной сложности схем из функциональных элементов / С. А. Ложкин [и др.] // Mathematical Problems in Computation Theory. Banach Center Publications. — 1987. — С. 501—510.
15. *Черемисин, О. В.* Об активности схем из клеточных элементов, реализующих систему всех конъюнкций / О. В. Черемисин // Дискретная математика. — 2003. — 15:2. — С. 113—122.
16. *Калачёв, Г. В.* Порядок мощности плоских схем, реализующих булевы функции / Г. В. Калачёв // Дискретная математика. — 2014. — 26:1. — С. 49—74.
17. *Калачёв, Г. В.* Об одновременной минимизации площади, мощности и глубины плоских схем, реализующих частичные булевы операторы / Г. В. Калачёв // Интеллектуальные системы. Теория и приложения. — 2016. — 20:2. — С. 203—266.
18. *Калачёв, Г. В.* Нижние оценки мощности плоских схем, реализующих частичные булевы операторы / Г. В. Калачёв // Интеллектуальные системы. Теория и приложения. — 2014. — 18:2. — С. 279—322.
19. *Калачёв, Г. В.* Об оценках мощности плоских схем для замкнутых классов булевых функций / Г. В. Калачёв // Интеллектуальные системы. Теория и приложения. — 2016. — 20:3. — С. 52—57.
20. *Калачёв, Г. В.* Оценки мощности плоских схем, реализующих функции с ограниченным числом единиц / Г. В. Калачёв // Интеллектуальные системы. Теория и приложения. — 2017. — 21:1.
21. *Калачёв, Г. В.* Оценки мощности плоских схем, реализующих монотонные функции / Г. В. Калачёв // Интеллектуальные системы. Теория и приложения. — 2017. — 21:2.
22. *Калачёв, Г. В.* Обобщение оценок мощности плоских схем, реализующих частичные булевы операторы / Г. В. Калачёв // Вестник Московского университета. Серия 1: Математика. Механика. — 2018. — 73:3. — С. 60—64.

23. *Калачёв, Г. В.* О нижней оценке максимального потенциала плоских схем с несколькими выходами через площадь / Г. В. Калачёв // Интеллектуальные системы. Теория и приложения. — 2018. — 22:1. — С. 111—117.
24. *Воротников, А. С.* Верхние оценки переключательной мощности плоских схем, реализующих автономные автоматные функции / А. С. Воротников // Интеллектуальные системы. Теория и приложения. — 2021. — 25:4. — С. 96—99.

Публикации автора по теме диссертации

25. *Ефимов, А. А.* Верхняя оценка энергопотребления в классе объемных схем / А. А. Ефимов // Интеллектуальные системы. Теория и приложения. — 2019. — Т. 23:1. — С. 117—132.
26. *Ефимов, А. А.* Верхняя оценка энергопотребления объемных схем, реализующих булевы операторы / А. А. Ефимов // Интеллектуальные системы. Теория и приложения. — 2019. — Т. 23:2. — С. 105—124.
27. *Ефимов, А. А.* Оценки энергопотребления для класса объёмных схем с близкими выходами / А. А. Ефимов // Интеллектуальные системы. Теория и приложения. — 2022. — Т. 26:3. — С. 109—150.
28. *Ефимов, А. А.* Нижняя оценка энергопотребления для класса объёмных схем / А. А. Ефимов // Интеллектуальные системы. Теория и приложения. — 2023. — Т. 27:1. — С. 91—133.