Оценки мощности плоских схем, реализующих функции с ограниченным числом единиц

Г. В. Калачев (МГУ имени М. В. Ломоносова, Москва)

В работе исследуется функция Шеннона мощности плоских схем, которые реализуют функции от n переменных с ограниченным числом единиц. В качестве меры мощности рассматривается максимальный потенциал. Потенциал схемы на входном наборе равен количеству выходов элементов, выдающих единицу на этом входном наборе. В частности, в работе показано, что если количество единиц функции ограничено числом N, причём $\log_2 N \asymp n$, то порядок функции Шеннона равен $N(n - \log_2 N)$. Также было исследовано поведение функции Шеннона в зависимости от ограничений на расположение входов схемы.

Ключевые слова: схемы из функциональных элементов, плоские схемы, клеточные схемы, потенциал, мощность, функция Шеннона, верхние оценки, нижние оценки, булевы функции.

Введение

Данная работа посвящена сложности реализации булевых функций с помощью чипов. Основной моделью, описывающей работу чипа является структурный автомат. Теория автоматов активно развивается и находит применение в различных задачах [1]-[21].Структурный автомат отражает лишь логическую структуру чипа, но не полностью отражает физические характеристики чипа такие, как размещение логических элементов в кристалле, площадь и энергопотребление.

Более точной моделью, которая учитывает размещение элементов структурного автомата на плоскости, является плоская схема (или схема

из клеточных элементов). Понятие плоской схемы ввёл Кравцов С. С. в работе [22]. Нетрудно убедиться в том, что для почти всех автоматов наибольшую сложность в смысле числа элементов представляют функции перехода и выхода автомата, которые являются булевыми функциями или операторами. Поэтому большой интерес представляет исследование сложности реализации плоскими схемами булевых функций и операторов.

Плоские схемы являются примером класса управляющих систем наряду с автоматами, схемами из функциональных элементов (далее СФЭ), контактными схемами и информационными графами. Среди последних работ по теории управляющих систем можно выделить [23]-[29].Обычно для управляющих систем вводится некоторая мера сложности, а иногда и несколько различных мер. При синтезе управляющих систем целью является минимизация сложности управляющей системы, решающей данную задачу. Для плоских схем и СФЭ мерами сложности обычно являются число элементов, глубина и активность (мощность). Для контактных схем это обычно число контактов и время моделирования (аналог активности СФЭ). Для информационных графов это объём (число рёбер графа) и среднее время ответа на запрос.

В некоторых случаях удаётся показать, что одновременная минимизация двух мер сложности невозможна. Такие результаты были доказаны для различных классов управляющих систем. В основном это происходит в случае наличия ограничений на базис. Например, для СФЭ О. М. Касим-Заде в [31] показал, что в некотором базисе невозможно одновременно минимизировать (асимптотически) сложность и мощность. Для информационных графов Е. М. Перпер в [24] показал, что при некоторых ограничениях на базовое множество невозможно построить информационный граф, решающий задачу поиска подстрок с оптимальным временем и оптимальной по порядку памятью.

В случае плоских схем важную роль наряду с базисом играет количество и расположение входов и выходов схемы. В [30] О. В. Черемисин показал, что невозможна одновременная минимизация (по порядку роста) площади и мощности плоских схем, реализующих дешифратор (систему всех конъюнкций). Этот результат остаётся верным вне зависимости от базиса и обусловлен прежде всего тем, что у схемы должно быть очень много выходов, и они все должны быть расположены по периметру схемы. Так как при замене базиса переключательная мощность (наиболее близкая к реальности мера мощности плоских схем, см. [32]), сохраняется с точностью до константы при замене базиса, то мы не вво-

дим никаких ограничений на базис. А поскольку расположение входов и выходов играет большую роль, то в основной интерес представляет исследование сложности плоских схем в зависимости от ограничений на входы и выходы.

С. С. Кравцов [22] показал, что для реализации произвольной булевой функции плоской схемой требуется $O(2^n)$ элементов, причём существуют функции, для реализации которых необходимо $\Omega(2^n)$ элементов. В статье [32] определены две меры мощности схем, и показана связь между ними, а также доказано, что произвольную булеву функцию от n переменных можно реализовать схемой площадью $O(2^n)$ и мощностью $O(2^{n/2})$.

В статье [33] получена нижняя оценка потенциала плоских схем, которые реализуют частичные булевы операторы в зависимости от ограничений на расположение выходов в схеме. В частности было показано, что если не накладывать никаких ограничений, то порядок мощности не меньше $\frac{m\sqrt{d}}{\sqrt{\min(m,\log_2 d)}}$, где d — размер области определения, а m – число выходов. Учитывая верхнюю оценку для того же класса операторов [34], был получен порядок функции Шеннона для потенциала частичных булевых операторов в случае, когда нет ограничений на расположение выходов.

В данной работе исследуется потенциал булевых функций, имеющих не более N единиц, в зависимости от расположения входов схемы. При $N \geq \log_2^2 n$, где n — число аргументов функции, получена зависимость функции Шеннона потенциала в данном классе функций от ограничений на расположение входов схемы. По аналогии с [33], ограничения формулируются в терминах суммарной длины рёбер минимального дерева, соединяющего все входы схемы (в [33] аналогичное ограничение накладывалось на выходы схемы).

Автор выражает глубокую благодарность научному руководителю д.ф.-м.н., профессору Э.Э. Гасанову за постановку задачи и внимание к работе.

Определения и обозначения.

Плоские схемы

Клеточным элементом будем называть булев оператор, у которого в сумме не более четырёх входов и выходов, причём каждому его входу и

каждому выходу сопоставлена некоторая метка из множества $\{l, r, t, b\}$, причём метки не повторяются.

Метки будем также называть сторонами элемента:

- l — левая сторона;
- r — правая сторона;
- t — верхняя сторона;
- b — нижняя сторона.

Клеточный элемент будем изображать в виде единичного квадрата на плоскости. При этом входам и выходам элемента сопоставляются стороны квадрата 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. Множество входов (выходов) элемента e будем обозначать $in(e)$ ($out(e)$).

Входы и выходы элемента будем называть его *контактами*.

Заметим, что это определение немного отличается от обычного тем, что допускается, чтобы на разных выходах реализовывались разные нетождественные функции.

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

Коммутационный элемент соответствует либо проводнику в микросхеме, либо пересечению проводов, либо тождественной функции, служащей для усиления сигнала.

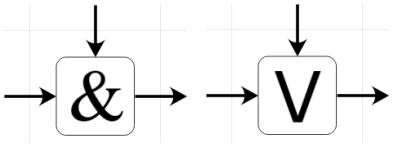
Описывать элемент будем уравнениями, которые задают его оператор, заменяя все переменные в них на сопоставленные им метки (l,r,t или b). Тогда в левой части каждого уравнения будет стоять выходная метка, а в правую будут входить только входные метки.

На рисунке 1 приведены примеры клеточных элементов.

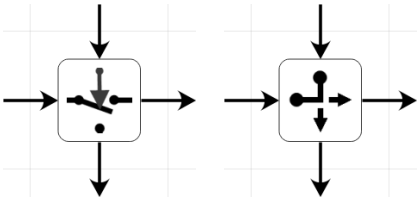
Для удобства введем пустой клеточный элемент — изолирующий (будем обозначать λ).

Всюду далее значок $:=$ будет обозначать «по определению равно».

За E обозначим множество всех клеточных элементов, $N_E := |E|$.

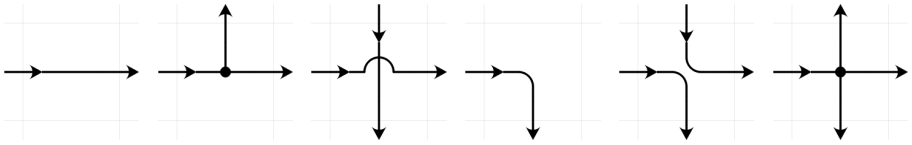


(a) обычные логические элементы



$r = l\bar{t}, b = lt$ $r = l\bar{t}, b = \bar{l}t$

(b) логические элементы, реализующие две различные функции



(c) коммутационные элементы

Рис. 1. Примеры клеточных элементов.

Сетью из клеточных элементов на множестве $M \subset \mathbb{Z}^2$ над множеством $E' \subseteq E$ будем называть отображение $K : M \to E'$, при этом E' будем называть *базисом* сети.

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

Левой, *правой*, *верхней* и *нижней* сторонами элемента e с координатами (x, y) будем называть точки с координатами $(x-\frac{1}{2}, y)$, $(x+\frac{1}{2}, y)$, $(x, y-\frac{1}{2})$ и $(x, y+\frac{1}{2})$ соответственно (на рисунках ось y будет направлена вниз).

Будем говорить, что сеть K из клеточных элементов корректна, если для любых двух 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,
- либо среди них одна является входом, другая — выходом, например, a — выход, а b — вход, в таком случае будем говорить, что выход a *подключён* к входу b;

Множество M будем называть *носителем* сети K.

Введем понятие *графа корректной сети из клеточных элементов* K (будем обозначать G_K). G_K — ориентированный граф, вершинами которого являются входы и выходы элементов схемы. Если выход одного элемента подключён 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 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.

Плоской схемой или *схемой из клеточных элементов* на множестве $M \subset \mathbb{Z}^2$ над базисом $E' \subseteq E$ будем называть корректную сеть из клеточных элементов, в графе которой нет ориентированных циклов. Множество M будем называть *носителем* схемы K.

Далее везде по умолчанию используем базис E, то есть считаем, что у нас есть все клеточные элементы.

Если вход (выход) элемента не подключён к выходу (входу) другого элемента, будем его называть *входом* (*выходом*) схемы.

Контактами схемы будем называть ее входы и выходы. Множество входов (выходов) схемы K будем обозначать $In(K)$ ($Out(K)$).

Узлами схемы K будем называть вершины графа G_K.

Если M — носитель схемы K, то величину $|M|$, равную количеству элементов множества M, будем называть *площадью* схемы K и обозначать $|K|$.

Расстоянием между узлами схемы будем называть расстояние между соответствующими вершинами в G_K. Расстояние от узла a до узла b на схеме K будем обозначать $\rho_K(a, b)$.

Подсхемой схемы K с носителем $M_0 \subseteq M$ будем называть схему $K|_{M_0}$, получающуюся из K выбрасыванием клеточных элементов, соответствующих множеству $M \setminus M_0$. Если схема K фиксирована, то иногда будем говорить просто подсхема M_0.

Каждой плоской схеме K можно сопоставить схему из функциональных элементов $Circ(K)$ следующим образом:

1) каждой функции $f_{s,i}$, которую реализует i-й выход элемента s клеточной схемы, сопоставим функциональный элемент $e_{s,i}$, реализующий $f_{s,i}$; если i-й и j-й выходы являются выходами одной и той же функции, то им будет соответствовать один и тот же функциональный элемент;

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

3) удалим из схемы все тождественные функции, подсоединив их вход ко всем их выходам.

Будем говорить, что схема K *реализует* булев оператор F_K, если схема из функциональных элементов $Circ(K)$ реализует F_K.

Назовём схему K *минимальной* над базисом $E' \subseteq E$, если она обладает минимальной площадью среди всех схем над базисом E', реализующих F_K.

Обозначим $S_{E'}(F)$ площадь минимальной схемы, реализующей оператор F. Если $E' = E$, то будем просто писать $S(F)$.

Будем говорить, что плоские схемы K_1 и K_2 равны и писать $K_1 = K_2$, если существует параллельный перенос плоскости, который позволяет совместить схемы K_1 и K_2, иначе будем говорить, что K_1 и K_2 различны.

Замечание. Обычно, когда рассматривают плоские схемы, предполагается, что они имеют форму прямоугольника, и входы и выходы расположены по периметру. Но здесь мы не накладываем ограничения на геометрию схемы, поскольку схема, реализующая булеву функцию может быть частью большой схемы, реализующей булев оператор. А ограничения на геометрию есть лишь для всей схемы устройства, а не для ее составных частей.

Мощность схем.

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

Везде далее будем считать, что схема K имеет n входов, l узлов и g_i — функция, реализуемая в i-м узле схемы K.

Состоянием схемы K на входном наборе x назовём вектор

$$s_K(x) := (g_1(x), ..., g_l(x)).$$

Если $v = (v_1, ..., v_q) \in \{0,1\}^q$, обозначим $|v| := v_1 + v_2 + ... + v_q$.

Если есть частичная булева функция или оператор f и всюду определённая функция или оператор F, и некоторое доопределение f получается из F добавлением фиктивных переменных и перестановкой аргументов и компонент оператора, то будем писать $F \doteq f$.

Пусть схема K имеет n входов. Тогда

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

Максимальным потенциалом схемы K *на множестве входных наборов* $\mathcal{D} \subseteq \{0,1\}^n$ назовём $\widehat{U}_{\mathcal{D}}(K) := \max\limits_{x \in \mathcal{D}} u_K(x)$.

Средним потенциалом схемы K на множестве входных наборов $D \subseteq \{0,1\}^n$ назовём $U_D(K) := \frac{1}{|D|} \sum\limits_{x \in D} u_K(x)$. В случае $D = \{0,1\}^n$ будем обозначать просто $U(K)$, то есть $U(K) = U_{\{0,1\}^n}(K)$.

Пусть $f : \mathcal{D} \to \{0,1\}$ — частичная булева функция, $\mathcal{D}' \subseteq \{0,1\}^n$, Q — предикат на множестве клеточных схем, выделяющий подмножество допустимых схем. Определим средний и максимальный потенциал функции f.

$$U_{\mathcal{D}',Q}(f) := \min_{K \in Q : F_K \doteq f} U_{\mathcal{D}'}(K), \quad \widehat{U}_{\mathcal{D}',Q}(f) := \min_{K \in Q : F_K \doteq f} \widehat{U}_{\mathcal{D}'}(K).$$

В случае $\{K \in Q : F_K \doteq f\} = \varnothing$ будем считать $U_{\mathcal{D}',Q}(f) = \widehat{U}_{\mathcal{D}',Q}(f) = \infty$.

Введём функции Шеннона для среднего и максимального потенциала в классе $\mathcal{F}$ булевых функций

$$U_{\mathcal{D},Q}(\mathcal{F}) := \max_{f \in \mathcal{F}} U_{\mathcal{D},Q}(f), \quad \widehat{U}_{\mathcal{D},Q}(\mathcal{F}) := \max_{f \in \mathcal{F}} \widehat{U}_{\mathcal{D},Q}(f).$$

С целью сделать формулы менее громоздкими, условимся использовать сокращённые обозначения. В случае $\mathcal{D} = \{0,1\}^n$ индекс $\mathcal{D}$ будем опускать (n — число входов схемы или аргументов функции, определяется из контекста). Также, если на схемы не наложено ограничений ($Q \equiv 1$), то индекс Q будем опускать. Часто предикат будет обозначаться Q_p, где p — некоторое обозначение. В этом случае будем вместо индекса Q_p будем просто писать индекс p.

Например, вместо $U_{\{0,1\}^n,Q_{[l,h]}}(f)$ будем писать просто $U_{[l,h]}(f)$. Из контекста всегда будет понятно, какой из индексов опущен.

Замечание. В работе [32] наряду с потенциалом была введена переключательная мощность. В [32, теорема 1] показана связь между этими мерами мощности, поэтому оценки, полученные в этой работе можно обобщить и на переключательную мощность.

Результаты.

Оценки мощности зависят от расположения входов схемы. Поэтому введём ещё одну характеристику $T_{in}(K)$ – суммарная длина рёбер минимального остовного дерева с вершинами во входах схемы K.

За $F_N^{\mathcal{D}}$ обозначим множество частичных функций $f : \mathcal{D} \to \{0,1\}$, принимающих значение 1 не более чем на N наборах. Положим $F_N^n := F_N^{\{0,1\}^n}$.

Обозначим через $Q_{[l;h]}$ множество клеточных схем K таких, что $T_{in}(K) \in [l;h]$.

Оценки потенциала будут использовать функцию $u_0(h,N,d)$, которая определяется следующим образом

$$u_0(h,N,d) := \frac{R\log_2 d}{\max(h,\sqrt{R})\log_2 \frac{\max(2\log_2 d,h,N)}{\log_2 d}}, \tag{1}$$

где $R := N(\log_2 d - \log_2 N)$.

Замечание. Поскольку доказанные в данной работе оценки верны лишь с точностью до порядка, то в качестве u_0 можно взять любую формулу, совпадающую с (1) по порядку для всех значений параметров, удовлетворяющих ограничениям нижеследующих теорем.

Теорема 1. *Пусть $\mathcal{D}$ — произвольное подмножество $\{0,1\}^n$ мощности d, f_0 — частичная функция из $\mathcal{D}$ в $\{0,1\}$, h и N — некоторые параметры. Тогда если выполнены неравенства*

$$N \le \frac{d}{2} \quad и \quad N\log_2\frac{d}{N} \ge C_0 h\log_2 h,$$

то доля функций $f \in F_N^{\mathcal{D}}$, для которых справедлива нижняя оценка максимального потенциала

$$\widehat{U}_{[0,h]}(f_0 \oplus f) \ge C_1 u_0(h,N,d),$$

составляет не менее $1-\alpha(N,d)$, где $\alpha(N,d) = O(2^{-R/2})$ при $N,d \to \infty$. Здесь C_0, C_1 — некоторые абсолютные константы.

Определим функции $h_1(N,n) = \sqrt{\frac{Nn(n-\log_2 N)}{\log_2 N}}$ и

$$u_1(l,h,N,n) = \begin{cases} u_0(h,N,2^n), & \text{если } h < h_1(N,n); \\ h_1(N,n), & \text{если } l \le h_1(N,n) \le h; \\ l, & \text{если } l > h_1(N,n). \end{cases}$$

Теорема 2. *Для любых натуральных чисел n и N, а также параметров l и $h \geq l$, удовлетворяющих неравенствам*

$$\log^2 n \leq N \leq 2^{n-1} \quad и \quad n \leq h$$

доля функций $f \in F_N^n$, для которых справедлива оценка (по порядку) максимального потенциала

$$\widehat{U}_{[l,h]}(f) \asymp u_1(l,h,N,2^n) \asymp \min_{t\in[l,h]} \max(t, u_0(t,N,2^n)), \ \textit{при } n \to \infty,$$

составляет не менее $1-\alpha(n)$, где $\alpha(n) = O(2^{-C_1 N})$ при $n \to \infty$. Здесь $C_1 > 0$ — некоторая абсолютная константа.

Будем говорить, что свойство $\mathcal{P}$ выполнено для почти всех функций из класса $\mathcal{F}_n$, если доля функций из $\mathcal{F}_n$, удовлетворяющих $\mathcal{P}$, стремится к 1 при $n \to \infty$.

Введём обозначение $Q_{\asymp h} := Q_{[h/2,h]}$.

Подставляя $l = h/2$ в теорему 2, в зависимости от соотношения N и n получим следующие частные случаи теоремы.

Следствие 1. *Существует константа $C_0 > 0$ такая, что если параметры n, N и h удовлетворяют неравенствам*

$$\log^2 n \leq N \leq 2n \quad и \quad 2n \leq h,$$

то для почти всех функций $f \in F_N^n$ справедлива оценка (по порядку) максимального потенциала

$$\widehat{U}_{\asymp h}(f) \asymp \max\left(h, \frac{n^2 N}{h \log_2(h/n)}\right), \ \textit{при } n \to \infty.$$

Следствие 2. *Если параметры N и h удовлетворяют неравенствам*

$$2n < N \leq 2^{n/2} \quad и \quad n \leq h,$$

то для почти всех функций $f \in F_N^n$ справедливы следующие утверждения.

Если $h \leq \sqrt{nN}$, то

$$\widehat{U}_{\asymp h}(f) \asymp \frac{n\sqrt{nN}}{\log_2(N/n)}, \ \textit{при } n \to \infty,$$

Если $h > \sqrt{nN}$, *то*

$$\widehat{U}_{\asymp h}(f) \asymp \max\left(h, \frac{n^2 N}{h \log_2(h/n)}\right), \text{ при } n \to \infty.$$

Следствие 3. *Если параметр* N *удовлетворяет неравенству*

$$2^{n/2} < N \leq 2^{n-1}.$$

то для почти всех функций $f \in F_N^n$ *справедлива оценка (по порядку) максимального потенциала*

$$\widehat{U}_{\asymp h}(f) \asymp \max(h, \sqrt{N(n - \log_2 N)}), \text{ при } n \to \infty.$$

Также из теоремы следует, что при $N < 2^{n/2}$ чтобы для получения оптимального потенциала с ограничением $Q_{\asymp h(n)}$, нужно взять $h(n) = h_1(N, n)$. Отсюда вытекает ещё одно следствие.

Следствие 4. *Если параметр* N *удовлетворяет неравенству*

$$\log_2^2 n < N \leq 2^{n-1}.$$

то для почти всех функций $f \in F_N^n$ *справедлива оценка (по порядку) максимального потенциала*

$$\widehat{U}(f) \asymp h_1(N, n), \text{ при } n \to \infty.$$

Доказательство

Нижние оценки.

Пусть M — подсхема схемы K. Введём несколько обозначений.

- Входы и выходы подсхемы M, не являющиеся входами и выходами схемы K, назовем *граничными контактами* подсхемы M относительно схемы K. Множество граничных контактов будем обозначать $(M|K)$ и называть *разрезом*.

- За $In(M|K)$ обозначим множество входов схемы M, которые лежат на разрезе $(M|K)$ (такие входы будем называть *граничными*), то есть
$$In(M|K) = In(M) \cap (M|K) = In(M) \setminus In(K).$$

- За $In(MK)$ обозначим множество входов схемы M, являющихся входами схемы K. То есть,

$$In(MK) = In(M) \cap In(K) = In(M) \setminus (M|K).$$

- За $Out(M|K)$ обозначим множество выходов схемы M, которые лежат на разрезе $(M|K)$ (такие выходы будем называть *граничными*), то есть

$$Out(M|K) = Out(M) \cap (M|K) = Out(M) \setminus Out(K).$$

- За $Out(MK)$ обозначим множество выходов K_0, которые являются выходами K, то есть

$$Out(MK) = Out(M) \cap Out(K) = Out(M) \setminus (M|K).$$

Для фиксированной схемы K введём следующие обозначения.

- B_r — множество клеток на плоскости, отстоящих от входных элементов (тех, входы которых являются входами схемы) не более чем на $r-1$ по манхеттеновской метрике.
- K_r — множество элементов схемы K, лежащие в множестве B_r.

Лемма 1. *Если $a > b > 0$, то*

$$aH(b/a) \le b\left(\log_2 a - \log_2 b + \frac{1}{\ln 2}\right) \tag{2}$$

Доказательство.

$$\begin{aligned} aH(b/a) =& a\left(-\frac{b}{a}\log_2\frac{b}{a} - \left(1-\frac{b}{a}\right)\log_2\left(1-\frac{b}{a}\right)\right) = \\ =& b\log_2\frac{a}{b} + (a-b)\log_2\frac{a}{a-b} = \\ =& b(\log_2 a - \log_2 b) + (a-b)\frac{1}{\ln 2}\ln\left(1+\frac{b}{a-b}\right) \le \\ \le& b(\log_2 a - \log_2 b) + (a-b)\frac{1}{\ln 2}\frac{b}{a-b} = \\ =& b\left(\log_2 a - \log_2 b + \frac{1}{\ln 2}\right). \end{aligned}$$

□

Часто лемма будет использоваться для случая $a = 2^t$. Тогда (2) можно переписать в виде

$$2^t H(b/2^t) \le b\left(t - \log_2 b + \frac{1}{\ln 2}\right) < b\,(t - \log_2 b + 2)\,. \tag{3}$$

Обычно обозначение $f(x) = O(g(x))$ используется только в асимптотическом смысле. Нам будет удобнее использовать это обозначение в следующем смысле. Если ранее были оговорены некоторые ограничения на переменные $x_1, ..., x_n$, которые можно записать в виде множества допустимых значений P, то

$$f(x_{i_1}, ..., x_{i_k}) = O(g(x_{j_1}, ..., x_{j_m})) \Leftrightarrow$$
$$\Leftrightarrow \exists C > 0 : \forall (a_1, ..., a_n) \in P \left(f(a_{i_1}, ..., a_{i_k}) \le C g(a_{j_1}, ..., a_{j_m})\right).$$

Все функции у нас будут принимать только неотрицательные значения.

Также далее мы будем использовать обозначение $f(x) = \Theta(g(x))$, если $f(x) = O(g(x))$ и $g(x) = O(f(x))$.

0.0.1. Оценки для схем с близко расположенными входами.

Если f – частичная функция или оператор на области $\mathcal{D}$, то обозначим $N_f := \{x \in \mathcal{D} \mid |f(x) \ne 0\}$ — множество, где f отлично от 0. Далее N – число единиц функции f, $\mathcal{D} \subseteq \{0,1\}^n$ – область определения, $k := \lceil \log_2 N \rceil$. Пусть задано некоторое множество Q допустимых клеточных схем.

Зафиксируем функцию $f_0 : \mathcal{D} \to \{0,1\}$. Для функции f зафиксируем схему K^f, реализующую функцию $f_0 \oplus f$, имеющую наименьший средний потенциал на множестве N_f среди всех схем из Q. Для фиксированной площади s и длины разреза $w = |In(K_r^f|K^f) \cup Out(K_r^f|K^f)|$ введём множество $L^0(f_0, Q, N, r, s, w, u)$ функций f, таких, что $|f| \le N$ и средний потенциал на контактах $Out(K_r^f|K^f)$ и на контактах $In(K_r^f|K^f)$ не превосходит u, где среднее значение потенциала считается по всем наборам из N_f.

Пусть функция $f \oplus f_0$ реализуется схемой K с указанными параметрами. Схема $K \setminus K_r$ в свою очередь реализует некоторый оператор $F : \{0,1\}^{|Out(K_r|K)|} \to \{0,1\}^{|Out(K \setminus K_r)|}$. Компоненты и аргументы оператора упорядочим в соответствии с расположением соответствующих граничных контактов $(K_r|K)$ (нумеруются слева направо, сверху вниз);

если выход схемы является выходом $K \setminus K_r$, то соответствующая компонента оператора F будет последней. Таким образом, по схеме K_r и множеству граничных контактов однозначно определяются соответствующие этим контактам аргументы и компоненты оператора F. Определим также разметку l_r контактов схемы K_r. Для контакта α подсхемы K_r определим

$$l_r(\alpha) = \begin{cases} 0, & \alpha \in In(K); \\ 1, & \alpha \in Out(K); \\ 2, & \alpha \in (K_r|K). \end{cases}$$

Поскольку у схемы K только один выход, то может быть не более одного узла с меткой 2. Такую разметку будем называть *правильной*.

По схеме K' и правильной разметке l' её узлов определим функцию $g_{K',l'}(x,y)$.

1) Если есть выход α схемы K', помеченный 2, то $g_{K',l'}(x,y)$ — функция, реализуемая схемой K' на её выходе α, где вектор x подаётся на входы, помеченные 0, y подаётся на входы, помеченные 2.

2) Если метки всех выходов схемы K' отличны от, то $g_{K',l'}(x,y)$ равно последней компоненте вектора y.

Тройке (K_r, l_r, F) сопоставим операторы

$$G^{in}_{K_r,F} : \{0,1\}^n \to \{0,1\}^{|In(K_r|K)|},$$
$$G^{out}_{K_r,F} : \{0,1\}^n \to \{0,1\}^{|Out(K_r|K)|},$$

реализуемые на узлах $In(K_r|K)$ и $Out(K_r|K)$ соответственно, если подключить к граничным узлам $(K_r|K)$ схему, реализующую оператор F.

Убедимся, что $(f + f_0)(x) = g_{K_r,l_r}(x, F(G^{out}_{K_r,F}(x)))$.

1) Если выход схемы K лежит в K_r, то он помечен меткой 2. Оставшаяся часть схемы реализует оператор F, и его значение подаётся на контакты $In(K_r|K)$, помеченные 1. Поэтому схема K на выходе реализует $g_{K_r,l_r}(x, F(G^{out}_{K_r,F}(x)))$, и в то же время она реализует $(f + f_0)(x)$. Значит $(f \oplus f_0)(x) = g_{K_r,l_r}(x, F(G^{out}_{K_r,F}(x)))$.

2) Если выход схемы K не лежит в K_r, значит от лежит в $K \setminus K_r$. В этом случае по определению оператора F его последняя компонента является функцией, реализуемой подсхемой $K \setminus K_r$ на выходе $Out(K)$. С другой стороны, все метки контактов K_r отличны от 2, поэтому $g(x, F(G^{out}_{K_r,F}(x)))$ равно последней компоненте вектора $F(G^{out}_{K_r,F}(x))$, то есть как раз значению на выходе схемы K.

Теперь сопоставим тройке (K_r, l_r, F) оператор F' и функцию F''

$$(F'(y), F''(y)) = \begin{cases} (F(y), 1), & \text{если } \exists x \in N_f : G^{out}_{K_r,F}(x) = y, \\ (\vec{0}, 0), & \text{иначе.} \end{cases}$$

Тогда $F'(y) = F(y)F''(y)$, и

$$f(x)\oplus f_0(x) = (f(x)\oplus f_0(x))F''(G^{out}_{K_r,F}(x))\vee(f(x)\oplus f_0(x))\overline{F''(G^{out}_{K_r,F}(x))} =$$
$$= g_{K_r,l_r}(x, F(G^{out}_{K_r,F}(x)))F''(G^{out}_{K_r,F}(x)) \vee f_0(x)\overline{F''(G^{out}_{K_r,F}(x))} =$$
$$= g_{K_r,l_r}\big(x, F'(G^{out}_{K_r,F}(x))\big)F''(G^{out}_{K_r,F}(x)) \vee \overline{F''(G^{out}_{K_r,F}(x))}f_0(x).$$

Отсюда

$$f(x) = (g_{K_r}(x, F'(G^{out}_{K_r,F}(x))) \oplus f_0(x))\&F''(G^{out}_{K_r,F}(x)).$$

Итак, каждой функции f, реализуемой схемой K^f сопоставим кортеж $T_f = (K^f_r, l^f_r, F'_f, F''_f, \pi_f, \pi^{in}_f)$, где π_f – нумерация узлов $(K^f_r|K^f)$, согласованная с порядком вычисления схемы K^f, π^{in}_f — соответствие входов схемы номерам аргументов функции.

Отметим свойства F'_f и F''_f при условии, что $f \in L^0(f_0, Q, N, r, s, w, u)$. По определению, оператор (F'_f, F''_f) может быть отличен от 0 только на множестве $G^{out}_{K_r,F}(N_f)$, то есть

$$|N_{F'}| \le |G^{out}_{K_r,F}(N_f)| \le |N_f| \le N. \tag{4}$$

По определению L^0 имеем

$$u \ge U_{N_f}(K_r|K) = \frac{1}{|N_f|}\sum_{x\in N_f}\big(|G^{out}_{K_r,F}(x)| + |F(G^{out}_{K_r,F}(x))|\big) \ge$$
$$\ge \frac{1}{N}\sum_{y\in G^{out}_{K_r,F}(N_f)}(|y| + |F'(y)|).$$

Значит

$$\sum_{y\in N_{F'}}(|y| + |F'(y)|) \le \sum_{y\in G^{out}_{K_r,F}(N_f)}(|y| + |F'(y)|) \le Nu. \tag{5}$$

Лемма 2. *Если $f_1 \ne f_2$, то $T_{f_1} \ne T_{f_2}$.*

Доказательство. Допустим, что существуют такие f_1, f_2, что $f_1 \neq f_2$, но $T_{f_1} = T_{f_2} = (K_r, l_r, F', F'', \pi, \pi^{in})$. Это означает, что существуют схемы K^{f_1}, K^{f_2}, реализующие функции f_1 и f_2 соответственно, причём $K_r^{f_1} = K_r^{f_2} =: K_r$. При этом существует набор x, на котором $f_1(x) \neq f_2(x)$ (переменные f_1 и f_2 сопоставляются входам K_r в соответствии с π^{in}). Поскольку разметки совпадают, то в схемах K^{f_1} и K^{f_2} одни и те же контакты K_r являются граничными. Без ограничения общности будем считать, что $f_1(x) = 0$, $f_2(x) = 1$.

Обозначим $G_1 := G^{out}_{K_r,F_1}$, $G_2 := G^{out}_{K_r,F_2}$, $y^1 := G_1(x)$, $y^2 := G_2(x)$. Тогда

$$(g_{K_r}(x, F'(y^1)) \oplus f_0(x))\&F''(y^1) = f_1(x) = 0$$
$$(g_{K_r}(x, F'(y^2)) \oplus f_0(x))\&F''(y^2) = f_2(x) = 1.$$

Это означает, что $y^1 \neq y^2$. Также имеем $F_1''(y^2) = F_2''(y^2) = 1$, поэтому существует $x' \in N_{f_1}$ такой, что $y^2 = G_1(x')$. Это означает, что $F_1'(y^2) = F_1(y^2)$. В свою очередь $F_2'(y^2) = F_2(y^2)$. Поскольку $F_1' = F_2'$, получаем, что $F_1(y^2) = F_2(y^2)$.

Пусть $In'(K_r) = \{s_1, ..., s_p\}$, $Out'(K_r) = \{t_1, ..., t_q\}$, причём нумерация узлов s_i и t_i согласована с нумерацией π (т.е. $i \leq j \leq p \Rightarrow \pi(s_i) < \pi(s_j)$ и $i < j \leq p \Rightarrow \pi(t_i) < \pi(t_j)$). Поскольку схемы K^{f_1} и K^{f_2} выдают различные значения на наборе x, а подсхема K_r у них общая, то это означает, что должны различаться значения на входах подсхемы K_r. Пусть $u \in In'(K_r) \cup Out'(K_r)$ — первый в соответствии с нумерацией π узел, значение на котором различается в схемах K^{f_1} и K^{f_2}. Такой узел существует, поскольку значение на узлах $t_1, ..., t_p$ в схемах K^{f_1} и K^{f_2} равно y^1 и y^2, а эти векторы различны. Возможны 2 случая.

1) $u = t_i \in Out'(K_r)$, то есть u — выход подсхемы K_r. Поскольку все узлы, от которых зависит значение на узле t_i имеют меньшие номера, чем t_i, то значения на них в схемах K^{f_1} и K^{f_2} совпадают. То есть значения на всех входах подсхемы K_r схем K^{f_1} и K^{f_2}, от которых зависит узел u, совпадают, значит и значение на узле u тоже должно совпадать — противоречие.

2) $u = s_i \in In'(K_r)$, то есть u — внутренний вход подсхемы K_r. Пусть $t_1, ..., t_l$ — все узлы из $Out'(K_r)$, которые вычисляются раньше u. Тогда $\pi(t_j) < \pi(u)$ при $j \leq l$, значит значения на этих узлах в схемах K^{f_1} и K^{f_2} совпадают и равны $y_1, ..., y_l$, причём $y_j = y_j^1 = y_j^2$ при $j \leq l$. Значит i-я компонента операторов F_1 и F_2 различается. Поскольку эта компонента не зависит от t_j при $j > l$, можно

записать $F_{k,i}(y) = F_{k,i}(y_1, ..., y_p) = F_{k,i}(y_1, ..., y_l)$. Итак, $F_{1,i}(y^2) = F_{1,i}(y_1^2, ..., y_l^2) = F_{1,i}(y_1, ..., y_l) \neq F_{2,i}(y_1, ..., y_l) = F_{2,i}(y_1^2, ..., y_l^2) = F_{2,i}(y^2)$. Но ранее мы установили, что $F_1(y^2) = F_2(y^2)$ — противоречие.

Итак, в обоих случаях мы получили противоречие. Лемма доказана. □

Положим $Q_{\leq h}$ — множество таких схем K, что $T_{in}(K) \leq h$, где $h \in \mathbb{N}$. Поскольку параметры L^0 всюду далее чаще всего будут одни и те же, то для упрощения записи будем их опускать, полагая $L^0 = L^0(f_0, Q_{\leq h}, N, r, s, w, u)$.

Оценим мощность множества L^0. Определим функцию

$$\hat{l}(h, N, n, r, u) = (r + \log_2 nr)(h + r) + Nu \log_2 \frac{\min(h + r, d/N)}{u}. \qquad (6)$$

Лемма 3.

$$\log_2 |L^0| = O\left(\hat{l}(h, N, n, r, u)\right).$$

Доказательство. По лемме 2 количество различных (с точностью до перестановки переменных) функций, реализуемых схемами с описанными характеристика не больше, чем количество кортежей T_f, где функция $F'_f : \{0,1\}^{w'} \to \{0,1\}^{w''}$, причем $w' + w'' \leq w$.

1) Всего не более, чем A^s различных схем K_r.

2) Не более 3^{w+n} способов выбрать разметку l_r.

3) Количество различных нумераций π не более, чем $w! < 2^{w \log_2 w}$.

4) Посчитаем количество различных операторов F', удовлетворяющих (4) и (5). Каждый такой оператор можно задать таблицей ширины $w' + w'' \leq w$, где в каждой строчке записаны y (w' чисел), затем $F'(y)$ (w'' чисел), причём только для тех y, на которых $F'(y) \neq 0$. Тогда из (4) следует, что в таблице не более N строк. Для удобства дополним её нулевыми строчками так, чтобы было ровно N строк. Чтобы таблица определялась однозначно, упорядочим все строки таблицы лексикографически. Из (5) следует, что во всей таблице не более Nu единиц. Количество таких таблиц при $u < \frac{w}{2}$ можно оценить сверху величиной

$$\sum_{j=0}^{Nu} C^j_{Nw'+w''} \leq 2^{NwH(\frac{Nu}{Nw})} = 2^{NwH(\frac{u}{w})},$$

где $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ — функция энтропии. То есть в тройках T_f может участвовать не более $2^{NwH(\frac{u}{w})}$ различных операторов F'. После задания таблицы входных наборов для F', функция F'' определяется однозначно: если y входит в таблицу и $F'(y) \neq 0$, то $F''(y) = 1$, иначе $F''(y) = 0$.

5) Количество различных соответствий π^{in} не более $n!$.

Теперь оценим $|L^0|$.

$$\log_2 |L^0| \leq \log_2 \left(n! A^s 2^{w\log_2 w} 3^{w+n} 2^{NwH(\frac{u}{w})} \right) =$$
$$= n\log_2 n + w\log_2 w + (n+w)\log_2 3 + O\left(s + NwH\left(\frac{u}{w}\right)\right) \leq$$
$$\leq (w+n)\log_2 3(w+n) + O\left(s + Nu\log_2 \frac{w}{u}\right). \qquad (7)$$

Теперь отдельно рассмотрим случай $u < 1$. В этом случае имеется не более Nu наборов $x \in N_f$ таких, что $u_{Out(K_r)}(x) \neq 0$. На тех наборах x, на которых все выходы $Out(K_r|K)$ подсхемы K_r равны 0, функция f реализуется схемой K_r, на входы $I(K_r|K)$ которой поданы константы и удалены выходы $Out(K_r|K)$. Площадь этой схемы не превышает площади K_r, а значит не превышает s.

Таким образом, f представляется в виде $f = f_r g_r \vee h_r \overline{g}_r$, где $f_r(x) = f_{K_r}(x, F(0))$, $g_r = \bigvee_{z \in Out(K_r|K)} \varphi_z(x)$, h_r — некоторая функция, реализуемая на оставшихся наборах. Здесь важно отметить, что пара функций (f_r, g_r) однозначно определяется по подсхеме K_r и выделенным n входам и одному выходу этой схемы, а функция $h_r\overline{g_r}$ имеет не более Nu единиц.

Таким образом, всего получается не более $A^s w^{n+1}$ пар (f_r, g_r) и не более C_d^{Nu} функций вида $h_r\overline{g}_r$. Отсюда

$$\log_2 |L^0| \leq \log_2 \left(A^s w^{n+1} C_d^{Nu} \right) \leq (n+1)\log_2 w + O(s) + dH\left(\frac{Nu}{d}\right) =$$
$$= n\log_2 w + O\left(s + Nu\log_2 \frac{d}{Nu}\right). \qquad (8)$$

Объединяя оценки (7) и (8), получим

$$\log_2 |L^0| \leq (w+n)\log_2 3(w+n) + O\left(s + Nu\log_2 \min\left(\frac{w}{u}, \frac{d}{Nu}\right)\right) =$$
$$= O\left((w+n)\log_2(w+n) + s + Nu\log_2 \frac{\min(w, d/N)}{u}\right) \qquad (9)$$

Если L^0 пусто, то лемма, очевидно, верна. Поэтому далее полагаем, что L^0 не пусто. Тогда существует схема K, реализующая функцию $f \in L^0$. Поскольку, по определению L_0, $K \in Q_{\leq h}$, то к ней можно применить лемму из [33], чтобы оценить площадь подсхемы K_r и длину разреза $(K_r|K)$. Очевидно, что в [33, леммы 7, 8] можно использовать входы вместо выходов, при этом величина $T(K)$ заменится на $T_{in}(K)$. Из этих лемм получаем

$$s = S(K_r) \leq 8r\varphi(r-1) \leq 8r(T_{in}(K) + r) \leq 8r(h + r).$$

$$w = |(K_r|K)| \leq 8r\varphi(r-1) \leq 8(h + r).$$

С другой стороны, очевидно, что для схемы K

$$s = S(K_r) = O(nr^2), \quad w = |(K_r|K)| = O(nr).$$

Поскольку у схемы n входов, а у каждого элемента не более 3-х входов, то $h \geq \frac{n}{3} - 1$. Отсюда $n = O(h) = O(w)$.

Подставляя эти величины в (9), получим

$$\begin{aligned}
\log_2 |L^0| &= O\left((n+w)\log_2(n+w) + s + Nu\log_2 \frac{\min(w, d/N)}{u}\right) = \\
&= O\left((h+r)\log_2 nr + r\min(h+r, nr) + Nu\log_2 \frac{\min(nr, h+r, d/N)}{u}\right) = \\
&= O\left((r+\log_2 nr)(h+r) + Nu\log_2 \frac{\min(h+r, d/N)}{u}\right).
\end{aligned}$$

Лемма доказана. □

Лемма 4. *Существуют абсолютные константы $C_0 > 0, C_1 > 0$ такие, что при достаточно большом n справедливо следующее. Для заданного подмножества $D \subseteq \{0,1\}^n$ мощности d, заданной функции $f_0 : D \to \{0,1\}$, параметра $h \in \mathbb{N}$ и параметра N, удовлетворяющего неравенствам*

$$N \leq \frac{d}{2} \quad u \quad R := N\log_2 \frac{d}{N} \geq C_0 h\log_2 n,$$

доля таких функций $f \in F_N^D$, для которых

$$U_{N_f, \leq h}(f_0 \oplus f) < C_1 U_0(h, N, d),$$

составляет не более $2^{-R/2}$, *где*

$$U_0(h,N,d)=\begin{cases}\dfrac{\sqrt{R}\log_2 d}{\log_2(2+N/\log_2 d)}, & \text{если } h\le\sqrt{R};\\[2ex] \dfrac{R\log_2 d}{h\log_2(2+h/\log_2 d)}, & \text{если } h>\sqrt{R}.\end{cases}\tag{10}$$

Доказательство. Обозначим $k:=\log_2 d$. Посчитаем количество функций f, которые можно реализовать схемами K такими, что $T_{in}(K)\le h$ так, чтобы потенциал на множестве N_f не превосходил $C_1U_0(h,N,d)$. Положим

$$u=A_1\frac{\log_2 d}{\log_2(2+t)},\ \text{где } t=\begin{cases}N/k, & \text{если } h\le\sqrt{R};\\ h/k, & \text{иначе.}\end{cases}$$

Здесь $A_1>0$ — параметр, который подберём позже.

Тогда при $r_{max}\ge\lceil C_1U_0(h,N,d)/u\rceil$ существует $r\le r_{max}$ такое, что $U_{N_f}(K_r|K)\le u$, то есть $f\in L_0(f_0,Q_{\le h},N,r,s(r),w(r),u)$. Тогда множество всех интересующих нас функций лежит в множестве

$$L_0^{max}:=\bigcup_{r=1}^{r_{max}}L_0(f_0,Q_{\le h},N,r,s(r),w(r),u).$$

Оценим мощность этого множества.

$$|L_0^{max}|\le\sum_{r=1}^{r_{max}}|L^0(f_0,Q_{\le h},N,r,s(r),w(r),u)|=$$
$$=r_{max}2^{O\left(\hat{l}(h,N,n,r_{max},u)\right)},$$

где $\hat{l}(h,N,n,r_{max},u)$ определяется выражением (6).

Поскольку $\log_2 r=O(\hat{l}(h,N,n,r,u))$, то

$$\log_2|L_0^{max}|=\log_2 r_{max}+O(\hat{l}(h,N,n,r_{max},u))=$$
$$=O(\hat{l}(h,N,n,r_{max},u)).\tag{11}$$

Заметим, что для того, чтобы множество схем $Q_{\le h}$ было непусто, должно выполняться $h\ge\frac{n}{3}-1$, поскольку у каждого элемента не более 3-х входов, а расстояние между входами разных элементов не меньше 1.

Рассмотрим 2 случая.

I. $h \le \sqrt{R}$. Тогда $u = A_1 \frac{\log_2 d}{\log_2(2+N/k)}$. В этом случае должно выполнятся

$$r_{max} \ge \frac{C_1 U_0(h,N,d)}{u} = \frac{C_1 k\sqrt{R}\log_2(2+N/k)}{A_1 \log_2(2+N/k)k} = \frac{C_1}{A_1}\sqrt{R}.$$

Положим $r_{max} = C_2\sqrt{R}$, где C_2 — параметр, $1 \ge C_2 \ge C_1/A_1$. Тогда $h \le \sqrt{R} \le r_{max}$, $n = O(h) = O(r_{max})$. Подставляя всё в (11), получаем

$$\begin{aligned}\log_2 |L_0^{max}| = \\ = O\Big((r_{max} + \log_2 n r_{max})(r_{max}+h) + Nu\log_2 \frac{\min(r_{max}, d/N)}{u}\Big) = \\ = O\left(r_{max}^2 + Nu\log_2 \frac{\min(r_{max}, d/N)}{u}\right). \quad (12)\end{aligned}$$

Рассмотрим 2 подслучая.

1) $r_{max} \le d/N$. Тогда $C_2\sqrt{N} \le C_2\sqrt{N\log_2(d/N)} = r_{max} \le d/N$, то есть $N \le (d/C_2)^{2/3}$, значит $d/N \ge \sqrt[3]{C_2^2 d} \ge \sqrt[4]{d}$ при достаточно большом d, отсюда $\log_2 d \le 4\log_2(d/N)$.

$$\frac{r_{max}}{u} \le \frac{C_2\sqrt{R}\log_2(2+N/k)}{A_1\log_2 d} \le \frac{C_2}{A_1}\sqrt{\frac{N}{\log_2 \frac{d}{N}}}\log_2\left(2+\frac{N}{k}\right).$$

$k/3-1 \le n/3-1 \le h \le \sqrt{R}$, поэтому $\frac{1}{\sqrt{\log_2 d/N}} = \sqrt{\frac{N}{R}} \le 3\frac{\sqrt{N}}{k-1} < 4\frac{\sqrt{N}}{k}$ при достаточно большом k. Отсюда получаем

$$\begin{aligned}\frac{r_{max}}{u} \le \frac{C_2}{A_1}\sqrt{N}\frac{4\sqrt{N}}{k}\log_2\left(2+\frac{N}{k}\right) \le \\ \le \frac{4C_2}{3A_1}\frac{N}{k}\left(1+\frac{N}{2k\ln 2}\right) < \frac{4C_2}{A_1}\left(2+\frac{N}{k}\right)^2.\end{aligned}$$

Значит

$$\begin{aligned}u\log_2\frac{r_{max}}{u} < A_1\frac{\log_2 d}{\log_2(2+N/k)}\left(2\log_2\left(2+\frac{N}{k}\right)+A_2\right) \le \\ \le 4A_1\log_2\frac{d}{N}(2+A_2),\end{aligned}$$

где $A_2 \geq \log_2 \frac{4C_2}{A_1} = 2 + \log_2 \frac{C_2}{A_1}$. Подставляя полученное выражение в (12), получим

$$\log_2 |L_0^{max}| = O\left(C_2^2 R + N \cdot 4A_1 \log_2 \frac{d}{N}(2 + A_2)\right) = \\ = O\left(R\left(C_2^2 + A_1\left(2 + A_2\right)\right)\right), \quad (13)$$

2) $r_{max} > d/N$. Тогда $N > (d/C_2)^{2/3} \geq d^{2/3}$. Поэтому при достаточно большом d с одной стороны, $2 + N/\log_2 d \leq N < d$, а с другой стороны, $2 + N/\log_2 d \geq \sqrt{N} > d^{1/3}$. Значит $A_1 < u < 3A_1$. Поскольку $N \leq \frac{d}{2}$, имеем

$$Nu \log_2 \frac{d/N}{u} < 3A_1\left(N \log_2 \frac{d}{N} - N \log_2 A_1\right) \leq \\ \leq 3A_1(1 - \log_2 A_1)R = O\left(A_1 R \log_2 \frac{2}{A_1}\right). \quad (14)$$

Подставляя полученную оценку в (12), получим

$$\log_2 |L_0^{max}| = O\left(C_2^2 R + 3A_1 R \log_2 \frac{2}{A_1}\right). \quad (15)$$

Объединяя (13) и (15), получим

$$\log_2 |L_0^{max}| = O\left(R \max\left(C_2^2 + A_1\left(2 + A_2\right), C_2^2 + A_1 \log_2 \frac{2}{A_1}, \right)\right) \leq A_3 R,$$

где A_3 — константа, удовлетворяющая неравенству

$$A_3 \geq C_O \max\left(C_2^2 + A_1\left(2 + A_2\right), C_2^2 + A_1 \log_2 \frac{2}{A_1}\right) = \\ = C_O\left(C_2^2 + A_1 \max\left(2 + A_2, \log_2 \frac{2}{A_1}\right)\right),$$

C_O — абсолютная константа.

II. $h > \sqrt{R}$. В этом случае $u = A_1 \frac{k}{\log_2(2+h/k)}$, и должно выполняться

$$r_{max} \geq \frac{C_1 U_0(h, N, d)}{u} = \frac{C_1 kR}{h \log_2(2 + h/k)} \cdot \frac{\log_2(2 + h/k)}{A_1 k} = \frac{C_1 R}{A_1 h}.$$

Положим $r_{max} = B_1 \frac{R}{h}$, где B_1 — параметр, $1 \geq B_1 \geq C_1/A_1$. Тогда $r_{max} \leq B_1 \frac{R}{\sqrt{R}} \leq \sqrt{R} < h$. Подставляя всё в (11), получаем

$$\begin{aligned}\log_2 |L_0^{max}| &= O\Big((r_{max} + \log_2 n r_{max})(h + r_{max}) + \\ &\qquad + Nu \log_2 \frac{\min(h + r_{max}, d/N)}{u}\Big) = \\ &= O\left(h\,(r_{max} + \log_2 n) + Nu \log_2 \frac{\min(h, d/N)}{u}\right) = \\ &= O\left(h \log_2 n + B_1 R + Nu \log_2 \frac{\min(h, d/N)}{u}\right). \qquad (16)\end{aligned}$$

Рассмотрим 2 подслучая.

1) $h \leq d/N$. Тогда $\sqrt{R} < h \leq d/N$, отсюда аналогично пункту I.1 получаем $\log_2 d \leq 4 \log_2 (d/N)$.

$$\frac{h}{u} = \frac{h \log_2 (2 + h/\log_2 d)}{A_1 \log_2 d} \leq \frac{1}{A_1} \frac{h}{\log_2 d} \left(2 + \frac{h}{\log_2 d}\right) < \frac{\left(2 + \frac{h}{\log_2 d}\right)^2}{A_1}.$$

Отсюда

$$\begin{aligned}Nu \log_2 \frac{h}{u} &\leq N A_1 \frac{k}{\log_2 (2 + h/k)} \log_2 \frac{\left(2 + \frac{h}{k}\right)^2}{A_1} = \\ &= A_1 N k \left(2 - \frac{\log_2 A_1}{\log_2 (2 + \frac{h}{k})}\right) \leq \\ &\leq 4 A_1 N \log_2 \frac{d}{N} (2 - \log_2 A_1) = 4 R A_1 \log_2 \frac{4}{A_1}.\end{aligned}$$

Подставляя полученную оценку в (16) и учитывая, что $h \log_2 n \leq R/C_0$, получим

$$\log_2 |L_0^{max}(Q_{\geq h}, N, u)| = O\left(\Big(\frac{1}{C_0} + B_1 + 4 A_1 \log_2 \frac{4}{A_1}\Big) R\right). \qquad (17)$$

2) $h < d/N$. Тогда, как и в случае I.2, выполнено (14). Подставляя эту оценку в (16), получим

$$\log_2 |L_0^{max}(Q_{\geq h}, N, u)| = O\left(\Big(\frac{1}{C_0} + B_1 + 3 A_1 \log_2 \frac{2}{A_1}\Big) R\right). \qquad (18)$$

Объединяя случаи II.1 и II.2, из оценок (17) и (18) получим

$$\log_2 |L_0^{max}| = O\left(R\left(\frac{1}{C_0} + B_1 + A_1 \log_2 \frac{4}{A_2}\right)\right) \le B_2 R,$$

Итак, в обоих случаях $\log_2 |L_0^{max}| \le \max(A_3, B_2)R$, где

$$A_3 = C_O\left(C_2^2 + A_1 \max\left(2 + A_2, \log_2 \frac{2}{A_1}\right)\right),$$
$$B_2 = C'_O\left(\frac{1}{C_0} + B_1 + A_1 \log_2 \frac{4}{A_1}\right).$$

Покажем, что число $\max(A_3, B_2)$ можно сделать сколь угодно малым, подобрав подходящие положительные числа C_0, C_1 и C_2. Для этого введём ограничение $\max(A_3, B_2) \le B_3$ и подберём C_0, C_1, C_2, чтобы все введённые по ходу доказательства ограничения выполнялись. Выпишем все ограничения на числа $C_0, C_1, C_2, A_1, C_2, A_2, B_1$.

$$1 \ge C_2 \ge C_1/A_1, \tag{19}$$
$$A_2 \ge 2 + \log_2 \frac{C_2}{A_1}, \tag{20}$$
$$1 \ge B_1 \ge C_1/A_1, \tag{21}$$
$$B_3 \ge C_O\left(C_2^2 + A_1 \max\left(2 + A_2, \log_2 \frac{2}{A_1}\right)\right), \tag{22}$$
$$B_3 \ge C'_O\left(\frac{1}{C_0} + B_1 + A_1 \log_2 \frac{4}{A_1}\right). \tag{23}$$

Здесь B_3, C_O, C'_O — фиксированные константы. Введём также дополнительное ограничение

$$C_2/A_1 \le 1. \tag{24}$$

Будем последовательно подбирать положительные числа C_0, C_1, C_2, A_1, C_2, A_2, B_1 так, чтобы требования $(19 - 24)$ выполнялись.

1) Учитывая (24), полагаем $A_2 = 2$, тогда ограничение (20) выполнено.

2) Положим $C_0 := \frac{3C'_O}{B_3}$, $B_1 := \min\left(1, \frac{B_3}{3C'_O}\right)$, тогда выполнена левая часть (21).

3) Полагаем $A_1 := \max\left\{x \in (0; \min(1, \frac{B_3}{8C_O})] \;\middle|\; x\log_2\frac{4}{x} \le \frac{B_3}{3\max(C_O, C'_O)}\right\}$, тогда $A_1(2+A_2) \le \frac{B_3}{2C_O}$, $A_1\log_2\frac{4}{A_1} \le \frac{B_3}{3C'_O}$ и $A_1\log_2\frac{2}{A_1} \le \frac{B_3}{3C_O}$. Тогда

$$C'_O\left(\frac{1}{C_0} + B_1 + A_1\log_2\frac{4}{A_1}\right) \le C'_O\left(\frac{B_3}{3C'_O} + \frac{B_3}{3C'_O} + \frac{B_3}{3C'_O}\right) = B_3,$$

то есть условие (23) выполнено.

Здесь следует отметить, что определение A_1 корректно, поскольку $x(4 - \log_2 x) \sim -x\log_2 x \to 0$ при $x \to 0$.

4) Полагаем $C_2 := \min\left(1, \sqrt{A_1}, \sqrt{\frac{B_3}{2C_O}}\right)$, тогда выполнено требование (24) и левая часть (19), а также $C_2^2 \le \frac{B_3}{2C_O}$. Поэтому

$$C_O\left(C_2^2 + A_1\max\left(2 + A_2, \log_2\frac{2}{A_1}\right)\right) \le$$
$$\le C_O\left(\frac{B_3}{2C_O} + \max\left(\frac{B_3}{2C_O}, \frac{B_3}{3C_O}\right)\right) = B_3,$$

то есть условие (22) выполнено.

5) Положим $C_1 := \min(A_1B_1, A_1C_2)$, тогда выполнена правая часть условий (19) и (21).

Итак, условия $(19 - 24)$ выполнены, что и требовалось.

Осталось оценить долю функций из F_N^D, лежащих в множестве L_0^{max}. Положим $B_3 = \frac{1}{2}$, тогда

$$\frac{|L_0^{max}|}{|F_N^D|} \le \frac{2^{B_3R}}{C_d^N} \le 2^{R/2}\left(\frac{N}{d}\right)^N = 2^{R/2 - N\log_2\frac{d}{N}} = 2^{-R/2}.$$

Лемма доказана. □

Для доказательства теоремы 1 осталось показать, что $U_0(h, N, d) \asymp u_0(h, N, d)$ в условиях доказанной леммы.

Лемма 5. *Если $N \le d/2$, $h \ge n$ и $N\log_2\frac{d}{N} \ge C_0h\log_2 n$, где C_0 — константа, то $u_0(h, N, d) \asymp U_0(h, N, d)$ при $n \to \infty$.*

Доказательство. Заметим, что при указанных ограничениях, если $d \to \infty$, то $d \ge N \ge C_0\log_2 n$ и $h \ge n$, поэтому $N \to \infty$, $d \to \infty$ и $h \to \infty$ при $n \to \infty$. Обозначим, как в лемме, $R = N\log_2\frac{d}{N}$. Рассмотрим несколько случаев.

1) $h \le C_2\sqrt{R}$ или $h \ge N$. Легко видеть, что в этом случае $U_0 = u_0$ по определению.

2) $\sqrt{R} \le h \le N$. В этом случае $\max(h, \sqrt{R}) = h$. Оценим сверху и снизу $\frac{h}{\log_2 d}$.

$$\frac{N}{\log_2 d} \ge \frac{h}{\log_2 d} \ge \frac{\sqrt{N \log_2 \frac{d}{N}}}{\log_2 d} = \sqrt{\frac{N}{\log_2 d} \cdot \frac{\log_2 \frac{d}{N}}{\log_2 d}} \ge \sqrt{\frac{N}{\log_2 d}}.$$

Рассмотрим 2 подслучая.

а) $N \le \sqrt{d}$. Тогда $\dfrac{N}{\log_2 \frac{d}{N}} \le \dfrac{N}{\log_2 \frac{d}{\sqrt{d}}} = 2\dfrac{N}{\log_2 d}$. Значит

$$\frac{h}{\log_2 d} \ge \sqrt{\frac{N}{2\log_2 \frac{d}{N}} \cdot \frac{\log_2 \frac{d}{N}}{\log_2 d}} = \sqrt{\frac{N}{2\log_2 d}}.$$

б) $d/2 \ge N > \sqrt{d}$. Тогда при достаточно большом d выполнено

$$N \log_2 d \le \frac{N\sqrt{d}}{\log_2^2 d} \le \left(\frac{N}{\log_2 d}\right)^2.$$

Значит

$$\frac{h}{\log_2 d} \ge \sqrt{\sqrt{N \log_2 d}\, \frac{\log_2 \frac{d}{N}}{\log_2 d}} = \sqrt[4]{\frac{N}{\log_2 d}}.$$

Объединяя случаи, получим $\frac{h}{\log_2 d} \ge \min\left(\sqrt{\frac{N}{2\log_2 d}}, \sqrt[4]{\frac{N}{2\log_2 d}}\right)$.

Значит $\max\left(2, \frac{N}{\log_2 d}\right) \ge \max\left(2, \frac{h}{\log_2 d}\right) \succcurlyeq \max\left(2, \sqrt[4]{\frac{N}{\log_2 d}}\right)$. Отсюда

$$\log_2\left(2 + \frac{h}{\log_2 d}\right) \asymp \log_2 \max\left(2, \frac{h}{\log_2 d}\right) \asymp$$
$$\asymp \log_2 \max\left(2, \frac{N}{\log_2 d}\right) \asymp \log_2\left(2 + \frac{N}{\log_2 d}\right).$$

Тогда

$$U_0(h, N, d) = \frac{R \log_2 d}{h \log_2(2 + h/\log_2 \frac{d}{N})} \asymp$$
$$\asymp \frac{R \log_2 d}{\max(h, \sqrt{R}) \log_2(2 + \frac{N}{\log_2 d})} = u_0(h, N, d).$$

Лемма доказана. □

Теорема 1 является прямым следствием доказанной леммы.

Оценки для схем с далеко расположенными входами.

Теперь введём множество $L^1(n, N, r, k)$ функций $f \in F_N^n$ таких, что существует схема $K^{f,r,k}$, реализующая функцию f, такая, что множество $B_r(K)$ имеет k компонент связности, причём $U_{N_f}(K_r|K) \leq \frac{k}{10}$. Обозначим $L^1(n, N) := \bigcup\limits_{k>1, r\in\mathbb{N}} L^1(n, N, r, k)$.

Рассмотрим функцию $f \in L^1(n, N)$. Тогда $f \in L^1(n, N, r, k)$ для некоторого r и некоторого $k \geq 2$. Для краткости обозначим $K := K^{f,r,k}$. Поскольку $B_r(K)$ имеет $k > 1$ компонент связности, и потенциал на границе не больше $k/10$, то для некоторой компоненты связности B'_r множества $B_r(K)$ потенциал на её границе $U_{N_f}(K'_r|K)$ не превосходит $1/10$, где K'_r — часть схемы K, попавшая в B'_r. Разрез $(K'_r|K)$ разбивает схему на две части. Обозначим часть, содержащую выход схемы K за K', а оставшуюся — за K''. В K'' и K' есть по крайней мере по одному входу схемы K, поскольку одна из них совпадает с K'_r, а другая содержит все входы, не входящие в K'_r. Такие входы есть, иначе B'_r было бы единственной компонентой связности $B_r(K)$. Поскольку схема определяет функцию с точностью до перестановки переменных, будем считать, что первые s переменных $x_1, ..., x_s$ подаются на входы K', а оставшиеся $t = n - s$ переменных $y_1, ..., y_t$ подаются на входы K''.

За Z обозначим множество входных наборов из N_f, на которых потенциал на границе $U_{N_f}(K'|K)$ равен 0. Поскольку средний потенциал на границе $< 1/10$, то $1/10 > U_{N_f}(K'|K) \geq \frac{|N_f \setminus Z|}{|N_f|} = 1 - \frac{|Z \cap N_f|}{|N_f|}$, значит $|Z| = |Z \cap N_f| > \frac{9}{10}|N_f| = \frac{9}{10}N$.

Лемма 6. *Пусть* $X := \pi_{x_1,...,x_s}(Z), Y := \pi_{y_1,...,y_t}(Z)$ *— проекции множества* Z *на множества переменных* $\{x_1, ..., x_s\}$ *и* $\{y_1, ..., y_t\}$. *Тогда* $Z = X \times Y$.

Доказательство. Из определения X и Y сразу следует, что $Z \subseteq X \times Y$. Зафиксируем произвольные $\alpha \in X, \beta \in Y$ и покажем, что набор (α, β) лежит в Z. Подадим набор (α, β) на вход схемы K и проверим, что на всех узлах $(K'|K)$ будет 0. Зафиксируем произвольную нумерацию узлов разреза $(K'|K)$, согласованную с порядком их вычисления, обозначим их $z_1, ..., z_l$. Доказывать будем индукцией количеству узлов i, для которых

утверждение верно.

База индукции. $i = 0$ – множество проверяемых узлов пусто, доказывать нечего.

Шаг индукции. Допустим, значение на узлах с номерами $j < i$ равно 0. Проверим, что на узле с номером i значение также равно 0.

Для определённости положим, что z_i — выход подсхемы K'. Тогда значение на нём является функцией от входов схемы K'. Причём z_i зависит только от входов всей схемы $x_1, ..., x_s$ и входов из $(K'|K)$ с номерами, меньшими i. Запишем это в виде $z_i = z_i(x_1, ..., x_s, z_1, ..., z_{i-1}) = z_i(\alpha_1, ..., \alpha_s, 0, ..., 0)$. Поскольку $\alpha \in X$, то существует $\beta' \in Y$ такое, что $(\alpha, \beta') \in Z$, то есть если подать α на $x_1, ..., x_s$, а β' на $y_1, ..., y_t$, то значение на всех узлах $(K'|K)$ равно 0. Отсюда сразу получаем $z_i(\alpha_1, ..., \alpha_s, 0, ..., 0) = 0$, что и требовалось. Аналогично рассматривается случай, когда z_i является входом K''.

Осталось показать, что $f(\alpha, \beta) = 1$. Выход всей схемы является выходом подсхемы K', а значит является функцией от $x_1, ..., x_s$ и $z_1, ..., z_l$, то есть $f(x_1, ..., x_s, y_1, ..., y_t) = g(x_1, ..., x_s, z_1, ..., z_l)$. Тогда $f(\alpha, \beta) = g(\alpha_1, ..., \alpha_s, 0, ..., 0)$. Поскольку $\alpha \in X$, существует β' такое, что $(\alpha, \beta') \in Z$, откуда получаем $1 = f(\alpha, \beta') = g(\alpha_1, ..., \alpha_s, 0, ..., 0) = f(\alpha, \beta)$, что и требовалось. Лемма доказана. □

Таким образом, множество N_f представляется в виде

$$N_f = Z \sqcup Z' = (X \times Y) \sqcup Z',$$

где

$$Z' = N_f \setminus Z \quad \text{и} \quad |Z'| \leq N/10.$$

Другими словами,

$$f(x_1, ..., x_n) = f_X(x_1, ..., x_s) f_Y(x_{s+1}, ..., x_n) \vee f'(x_1, ..., x_n),$$

где $|N_{f'}| = |N_f| - |N_{f_X}||N_{f_Y}| \leq N/10$. Учитывая, что функция задаётся схемой с точностью до перестановки переменных, получим, что множество $L_1(Q, N)$ состоит из функций f, представимых в виде

$$f(x_1, ..., x_n) = f_X(x_{i_1}, ..., x_{i_s}) f_Y(x_{j_1}, ..., x_{j_t}) \vee f'(x_1, ..., x_n), \qquad (25)$$

где $s, t \geq 1$, $\{i_1, ..., i_s, j_1, ..., j_t\} = \{1, ..., n\}$ и $|N_{f'}| = |N_f| - |N_{f_X}||N_{f_Y}| \leq N/10$.

За $l^1(N,s,t)$ обозначим количество функций f веса не более N, представимых в виде

$$f(x_1,...,x_n) = f_X(x_{i_1},...,x_{i_s})f_Y(x_{j_1},...,x_{j_t}), \tag{26}$$

для некоторых индексов $i_1,...,i_s,j_1,...,j_t$ таких, что $\{i_1,...,i_s,j_1,...,j_t\} = \{1,...,s+t\}$. Без ограничения общности будем считать, что $s \le t$.

Лемма 7. *Если $a,b,N \in \mathbb{N}$ и $0 \le N \le a \le b$, то $C_a^N/C_b^N \le \left(\frac{a}{b}\right)^N$.*

Доказательство. При $k < a$ имеем

$$\frac{a-k}{b-k} = \frac{a}{b}\cdot\frac{1-k/a}{1-k/b} = \frac{a}{b}\left(1-k\frac{1/b-1/a}{1-k/b}\right) = \frac{a}{b}\left(1-k\frac{a-b}{a(b-k)}\right) \le \frac{a}{b}.$$

Отсюда

$$\frac{C_a^N}{C_b^N} = \frac{\frac{\prod_{k=0}^{N-1}(a-k)}{N!}}{\frac{\prod_{k=0}^{N-1}(b-k)}{N!}} = \prod_{k=0}^{N-1}\frac{a-k}{b-k} \le \left(\frac{a}{b}\right)^N.$$

Лемма доказана. □

Лемма 8. *Существует константа A такая, что если $1 \le s \le t$, $s+t = n$ и $2^{n-3} \ge N \ge 5\log_2 n$, то*

1) *Если $s \le \log_2 5N$, то $l^1(N,s,t) \le \frac{AN}{2^{4N/5}}C_{2^n}^N$, где $A > 0$ — константа (не зависит от N,s и t).*

2) *Если $s > \log_2 5N$, то $l^1(N,s,t) \le \frac{1}{2^{\frac{N}{2}\log_2 N}}C_{2^n}^N$.*

Доказательство.

I. $s \le \log_2 5N$, тогда $2^s \le 5N$. Рассмотрим 2 случая.

I.I $2^t \le N$. В этом случае есть не более 2^{2^s} способов выбрать функцию f_X, не более 2^{2^t} способов выбрать функцию f_Y и C_n^s способов разбить n переменных на 2 группы из s и t переменных. Отсюда

$$\frac{l(N,s,t)}{C_{2^n}^N} \le \frac{2^{2^s}2^{2^t}C_n^s}{C_{2^n}^N} \le 2^{2N}\left(\frac{N}{2^n}\right)^N = \left(\frac{N}{2^{n-2}}\right)^N = \frac{\left(\frac{N}{2^{n-3}}\right)^N}{2^N} \le \frac{1}{2^N}.$$

I.II $2^s \le 5N$, $N \le 2^t$. В этом случае есть не более 2^{2^s} способов выбрать функцию f_X, не более $\sum_{i=0}^{N} C_{2^t}^i \le (N+1)C_{2^t}^N$ способов выбрать функцию f_Y и C_n^s способов разбить n переменных на 2 группы из s и t переменных. Отсюда

$$\frac{l(N,s,t)}{C_{2^n}^N} \le \frac{N2^{2^s}C_{2^t}^N C_n^s}{C_{2^n}^N} \le N2^{2^s}\left(\frac{2^t}{2^n}\right)^N n^s = \\ = (N+1)2^{2^s - sN + s\log_2 n} \le (N+1)2^{2^s+(1/5-s)N}.$$

1) Если $s \le 5$, то $(N+1)2^{2^s+(1/5-s)N} \le (N+1)2^{32-4N/5} < \frac{2^{33}N}{2^{4N/5}}$.

2) Иначе $s \ge 6$, но $2^s \le 5N$, поэтому $(N+1)2^{2^s+(1/5-s)N} \le (N+1)2^{5N+(1/5-6)N} \le (N+1)2^{-4N/5} < \frac{2N}{2^{4N/5}}$.

II. $2^s \ge 5N$. В этом случае для каждого $N_1 \le N$ есть не более $C_{2^s}^{N_1}$ способов выбрать функцию f_X веса N_1, не более $\sum_{i=0}^{N/N_1} C_{2^t}^i$ способов выбрать функцию f_Y веса не более N/N_1 и C_n^s способов разбить n переменных на 2 группы из s и t переменных. Отсюда

$$\frac{l(N,s,t)}{C_{2^n}^N} \le \sum_{N_1=1}^{N} \frac{C_{2^s}^{N_1}\sum_{N_2=0}^{N/N_1} C_{2^t}^{N_2} C_n^s}{C_{2^n}^N} \le \sum_{N_1=1}^{N} \frac{2^{2^s H(\frac{N_1}{2^s}) + 2^t H(\frac{N/N_1}{2^t})} C_n^s}{C_{2^n}^N}. \quad (27)$$

Найдём максимальное значение функции $g(x) = 2^s H(\frac{x}{2^s}) + 2^t H(\frac{N}{x2^t})$ при $1 \le x \le N$. Учитывая, что $H'(x) = \log_2 \frac{1-x}{x}$, получим

$$g'(x) = \log_2 \frac{2^s - x}{x} - \frac{N}{x^2}\log_2 \frac{2^t - y}{y} = \\ = \frac{1}{x\ln 2}\left(x\ln\frac{2^s-x}{x} - y\ln\frac{2^t-y}{y}\right) = \frac{h(s,x)-h(t,y)}{x\ln 2},$$

где $y = N/x$, $h(s,x) = x\ln\frac{2^s-x}{x}$.

$$h'_x(s,x) = \ln\frac{2^s-x}{x} - \frac{2^s}{x^2}\cdot\frac{x}{\frac{2^s-x}{x}} = \ln\frac{2^s-x}{x} - \frac{2^s}{2^s-x} \ge \\ \ge \ln\frac{2^s - \frac{2^s}{5}}{2^s/5} - \frac{2^s}{2^s - \frac{2^s}{5}} = \ln 4 - \frac{5}{4} > 0.$$

Поскольку $1 \le y \le N \le 2^s/5 \le 2^t/5$, то аналогично получаем $h'_y(t,y) > 0$. Таким образом, $(h(s,x)-h(t,y))'_x = h'_x(s,x) - h'_y(t,y)y'(x) > 0$, поскольку

$y'(x) = -N/x^2 < 0$. То есть функция $g_1(x) = xg'(x)\ln 2$ возрастает на отрезке $[1; N]$. Отсюда следует, что если у функции $g(x)$ есть экстремум в точке $x_0 \in (1; N)$, тогда $g'(x_0) = 0$, а значит и $g_1(x_0) = 0$, а значит $g_1(x) < 0$ при $x < x_0$ и $g_1(x) > 0$ при $x > x_0$, а поскольку знак $g'(x)$ совпадает со знаком $g_1(x)$ на отрезке $[1, N]$, то x_0 – точка минимума функции g. Это означает, что максимум функции g достигается на границе отрезка $[1; N]$.

$$g(1) = 2^s H\left(\frac{1}{2^s}\right) + 2^t H\left(\frac{N}{2^t}\right) \le \left(s + \frac{1}{\ln 2}\right) + N\left(t - \log_2 N + \frac{1}{\ln 2}\right),$$

$$g(N) = 2^s H\left(\frac{N}{2^s}\right) + 2^t H\left(\frac{1}{2^t}\right) \le \left(t + \frac{1}{\ln 2}\right) + N\left(s - \log_2 N + \frac{1}{\ln 2}\right).$$

Тогда $g(x) \le \max(g(1), g(N)) \le s + Nt + \frac{N+1}{\ln 2} - N\log_2 N$.

Подставляя полученную оценку в (27), при достаточно больших N получим

$$\begin{aligned}
\frac{l(N,s,t)}{C_{2^n}^N} &\le \sum_{N_1=1}^{N} \frac{2^{s+Nt+\frac{N+1}{\ln 2} - N\log_2 N} C_n^s}{C_{2^n}^N} \le \\
&\le N 2^{s+Nt+\frac{N+1}{\ln 2} - N\log_2 N + s\log_2 n} \frac{C_N^N}{C_{2^n}^N} \le \\
&\le N 2^{s+Nt+\frac{N+1}{\ln 2} - N\log_2 N + s\log_2 n} \frac{N^N}{2^{nN}} = \\
&= N 2^{s - Ns + \frac{N+1}{\ln 2} + s\log_2 n} = \frac{AN}{2^{(N-1-\frac{N}{5})\log_2 5N - N\log_2 e}} \le \\
&\le \frac{AN}{2^{(\frac{4N}{5}-1)\log_2 5N - N\log_2 e}} < \frac{1}{2^{\frac{N}{2}\log_2 N}}.
\end{aligned}$$

Лемма доказана. □

Теперь мы можем оценить количество функций в $L^1(n, N)$.

Лемма 9. *Если $2^{n-3} \ge N \ge 5\log_2 n$, то $|L^1(n, N)| \le \frac{N^3}{2^{\frac{3}{25}N}} C_{2^n}^N$ при достаточно больших n.*

Доказательство. Используя лемму 8, посчитаем количество $l^1(N, n)$ всех функций f от n переменных веса не более N, представимых в виде

(26) для некоторых $s, t \geq 1$. Обозначим $k := \lfloor \min(n/2, 5\log_2 N) \rfloor$.

$$\frac{l^1(N,n)}{C_{2^n}^N} \leq \sum_{s=1}^{\lfloor n/2 \rfloor} l^1(N,s,n-s) \leq \sum_{s=1}^{k} l^1(N,s,n-s) + \sum_{s=k+1}^{\lfloor n/2 \rfloor} l^1(N,s,n-s) \leq$$
$$\leq k\frac{AN}{2^{4N/5}} + (n-k)\frac{1}{2^{\frac{N}{2}\log_2 N}} \leq \frac{5AN\log_2 N}{2^{4N/5}} + \frac{n}{\underbrace{2^N}_{\geq n^5} \cdot 2^{\frac{N}{2}(\log_2 N - 2)}} \leq \frac{N^2}{2^{4N/5}},$$

если N достаточно велико.

$$|L^1(n,N)| \leq \sum_{N'=0}^{N/10} l^1(N-N',n) C_{2^n-N+N'}^{N'} \leq \sum_{N'=0}^{N/10} C_{2^n}^{N'} C_{2^n}^{N-N'} \frac{(N-N')^2}{2^{4(N-N')/5}} <$$
$$< \sum_{N'=0}^{N/10} \frac{C_{2^n}^{N'} C_{2^n}^{N-N'} (N-N')^2}{2^{4(N-N')/5}}. \quad (28)$$

Чтобы оценить $|L^1(n,N)|/C_{2^n}^N$, оценим $C_{2^n}^{N'} C_{2^n}^{N-N'}/C_{2^n}^N$.

$$\frac{C_{2^n}^{N'} C_{2^n}^{N-N'}}{C_{2^n}^N} = \frac{2^n(2^n-1)\cdot\ldots\cdot(2^n-N'+1)}{N'!} \cdot$$
$$\cdot \frac{2^n(2^n-1)\cdot\ldots\cdot(2^n-N+N'+1)}{(N-N')!} \cdot$$
$$\cdot \frac{N!}{2^n(2^n-1)\cdot\ldots\cdot(2^n-N+1)} =$$
$$= C_N^{N'} \frac{2^n(2^n-1)\cdot\ldots\cdot(2^n-N'+1)}{(2^n-N+N')\cdot\ldots\cdot(2^n-N+1)} <$$
$$< 2^{NH(N'/N)} \left(\frac{2^n-N'}{2^n-N}\right)^{N'} \leq$$
$$\leq 2^{NH(\frac{1}{10})} \left(1 + \frac{N-N'}{2^n-N}\right)^{N'} < 2^{\frac{N}{2}} 2^{N'} \leq 2^{\frac{3}{5}N}.$$

Подставляя эту оценку в (28), получим

$$\frac{|L^1(n,N)|}{C_{2^n}^N} \leq \sum_{N'=0}^{N/10} \frac{(N-N')^2}{2^{4(N-N')/5}} \cdot \frac{C_{2^n}^{N'} C_{2^n}^{N-N'}}{C_{2^n}^N} \leq \frac{\left(\frac{N}{10}+1\right) 2^{\frac{3}{5}N} N^2}{2^{4(N-N/10)/5}} < \frac{N^3}{2^{\frac{3}{25}N}}. \quad (29)$$

Домножая обе части (29) на $C_{2^n}^N$, получим утверждение леммы. Лемма доказана. □

Лемма 10. *Существует константа $C_3 > 0$ такая, что доля функций $f \in F_N^n$, для которых $U_{N_f,\geq h}(f) < C_3 h$, составляет не более $\frac{N^3}{2^{\frac{3}{25}N}}$ при $2^{n-3} \geq N \geq 5\log_2 n$ и достаточно большом n.*

Доказательство. За $Q_{\geq h}$ обозначим множество схем K таких, что $T_{in}(K) \geq h$. Рассмотрим функцию f такую, что $U_{N_f,\geq h}(f) < \frac{1}{10}T_{in}(K^f)$. Положим

$$r_f := \max\left\{r : B_r^f \text{ имеет более 1-й компоненты связности}\right\}.$$

Тогда из [33, лемма 8] следует, что $T_{in}(K^f) = \varphi(r_f) = \sum_{j=0}^{r_f} k_j$, где k_j количество компонент связности B_j^f.

Поскольку границы B_j для различных j не пересекаются, то

$$\sum_{j=0}^{r_f} U_{N_f}(B_j|K^f) \leq U_{N_f}(K^f) = U_{N_f,\geq h}(f) < \frac{1}{10}T_{in}(K^f) = \frac{1}{10}\sum_{j=0}^{r_f} k_j.$$

Поэтому существует такое $j \leq r_f$, что $U_{N_f}(B_j|K^f) < \frac{1}{10}k_j$. Поскольку B_j имеет k_j компонент связности, то существует такая компонента связности B_j' множества B_j, что $U_{N_f}(B_j'|K^f) < \frac{1}{10}$. А это означает, что $f \in L^1(Q_{\geq h}, N)$.

По лемме 9 количество таких функций не превосходит $\frac{N^3}{2^{\frac{3}{25}N}}C_{2^n}^N = \frac{N^3}{2^{\frac{3}{25}N}}|F_n^N|$, что и требовалось. Лемма доказана. □

Определим функцию $m(t, N, n) = \max(t, u_0(t, N, 2^n))$.

Лемма 11. *При $n, N \to \infty$, $N \leq 2^n$ выполнено*

$$h_1(N, n) \asymp u_0(h_1(N, n), N, 2^n) \asymp \inf_{t \geq n} m(t, N, n).$$

Доказательство. В доказательстве леммы в асимптотических оценках всюду полагаем $N, n \to \infty$. Положим $R := N(n - \log_2 N)$. Заметим, что

$$h_1(N, n) = \sqrt{\frac{Nn(n - \log_2 N)}{\log_2 N}} = \sqrt{R\frac{n}{\log_2 N}} \geq \sqrt{R}.$$

Поэтому

$$u_0(h_1(N,n),N,2^n)=\frac{Rn}{h_1(N,n)\log_2\frac{\max(2n,N,h_1(N,n))}{n}}=$$
$$=\frac{\sqrt{Nn(n-\log_2 N)\log_2 N}}{\log_2\frac{\max(2n,N,h_1(N,n))}{n}}=h_1(N,n)\frac{\log_2 N}{\log_2\frac{\max(2n,N,h_1(N,n))}{n}}.$$

Для доказательства леммы нам нужно показать, что $\log_2 N$ по порядку совпадает с $\log_2\frac{\max(2n,N,h_1(N,n))}{n}$.

Рассмотрим 2 случая.

1) $N<h_1(N,n)$. Тогда $N<\frac{n(n-\log_2 N)}{\log_2 N}<n^2$, значит $n-\log_2 N\sim n$. Отсюда $h_1(N,n)\asymp\sqrt{\frac{Nn^2}{\log N}}>2n$ при достаточно большом N,

$$\log_2\frac{\max(2n,N,h_1(N,n)}{n}=\log_2\frac{h_1(N,n)}{n}\asymp\log_2\frac{N}{\log_2 N}\asymp\log_2 N.$$

2) $N\geq h_1(N,n)$. Тогда $N\geq\frac{n(n-\log_2 N)}{\log_2 N}$, значит $N\geq n\sqrt{n}$ при достаточно большом n. Тогда $N/n\geq N/N^{2/3}=N^{1/3}$, значит

$$\log_2\frac{\max(2n,N,h_1(N,n)}{n}=\log_2\frac{N}{n}\asymp\log_2 N.$$

Заметим, что $u_0(t,N,d)$ невозрастает по t. Поэтому при фиксированных N и d существует единственное h_{min} такое, что $h_{min}=u_0(h_{min},N,d)$. При $t=h_{min}(N,d)$ достигается минимум функции $\max(t,u_0(t,N,d))=m(t,N,n)$. Причём $\min(t,u_0(t,N,d))\leq h_{min}\leq\max(t,u_0(t,N,d))$ для всех $t>0$. Тогда

$$h_1\asymp\min(h_1,u_0(h_1,N,2^n))\leq h_{min}\leq\max(h_1,u_0(h_1,N,2^n))\asymp h_1,$$

значит $h_1(N,n)\asymp h_{min}=\inf_{t>0}m(t,N,n)$. Поскольку $h_{min}\asymp h_1(N,n)=n\sqrt{\frac{N(n-\log_2 N)}{n\log_2 N}}=\omega(n)$, то $h_{min}>n$ при достаточно больших n,N, значит $\inf_{t>0}m(t,N,n)=m(h_{min},N,n)=\inf_{t\geq n}m(t,N,n)$. Лемма доказана. □

Доказательство нижней оценки теоремы (2).

Запишем $m(t,N,n)$ в виде

$$m(t,N,n)=\begin{cases}u_0(t,N,d), & t\leq h_{min};\\ t, & t>h_{min}.\end{cases}\qquad(30)$$

В лемме 4 положим $D = \{0,1\}^n$ и $f_0 \equiv 0$. Положим $h_0 := R/C_0 \log_2 n$, где C_0 — константа из леммы 4, $R = N(n - \log_2 N)$.

Определим функцию

$$M(l,h,N,n) = \min_{t\in[l,h]} m(t,N,n).$$

Покажем, что если $h_0, h_{min} \notin (l,h)$, то для почти всех функций $f \in \mathcal{F}_N^n$ выполнено $\widehat{U}_{[0,h]}(f) = \Omega(M(l,h,N,n))$ при $n, N \to \infty$. Далее по умолчанию все асимптотические оценки делаются при $N, n \to \infty$. Рассмотрим 3 случая.

1) $l \geq h_0$. Сравним h_0 и $u_0(h_0, N, 2^n)$. Поскольку $\log_2 n = o(\sqrt{n}) = o(N(n - \log_2 N)) = o(R)$ при $n \to \infty$, то $h_0 = R/C_0 \log_2 n > \sqrt{R} \geq \sqrt{N}$ при достаточно большом n. Поскольку $h_0 \geq n$, то $\log_2 \frac{\max(2n,h_0,N)}{n} \asymp \log_2(2h_0/n)$ при $n \to \infty$.

$$u_0(h_0,N,2^n) = \frac{Rn}{\max(h_0,\sqrt{R})\log_2 \frac{\max(2n,h_0,N)}{n}} \asymp \frac{Rn}{h_0 \log_2 \frac{2h_0}{n}} = \\ = \frac{C_0 n \log_2 n}{\log_2(2h_0/n)} = O(n\log_2 n) = O(h_0)$$

при $n \to \infty$. Для всех $t \in [l,h]$ выполнено $t \geq l \geq h_0$, значит

$$u_0(t,N,2^n) \leq u_0(h_0,N,2^n) = O(h_0) \leq l \leq t.$$

Отсюда $m(t,N,n) = \Theta(t)$, значит

$$M(l,h,N,n) = \min_{t\in[l,h]} m(,N,nt) = \Theta(\min_{t\in[l,h]} t) = \Theta(l).$$

Тогда по лемме 10 доля функций, для которых

$$U_{N_f,\geq t}(f) \geq C_3 t = \Omega(l) = \Omega(M(l,h,N,n)),$$

не меньше $1 - \alpha_1(N)$, где $\alpha_1(N) = O(N^3 2^{-3N/25}) = O(2^{-N/25})$ при $N \to \infty$.

2) $h_{min} \leq l \leq h \leq h_0$. Учитывая (30), получим, что для всех $t \geq l \geq h_{min}$ выполнено $m(t,N,n) = t$, и ситуация полностью аналогична предыдущему случаю.

3) $l \le h \le \min(h_{min}, h_0)$. В этом случае, наоборот, из (30) следует, что $u_0(t, N, 2^n) = m(t, N, n) = M(l, h, N, n)$. Поскольку $h \le h_0$, то можно применить леммы 4 и 5 при $\mathcal{D} = \{0,1\}^n$, $d = 2^n$. Получим, что доля функций $f \in \mathcal{F}_N^n$, для которых

$$U_{N_f, \le h}(f) \ge C_1 U_0(h, N, 2^n) \asymp u_0(h, N, 2^n) = M(l, h, N, n),$$

не меньше $1 - \alpha_2(N)$, где $\alpha_2(N) = O(2^{-N(n-\log_2 N)/2}) = O(2^- N)$ при $N \to \infty$. Здесь мы учли, что при $t \le h \le h_{min}$ функция $m(t, N, n) = u_0(t, N, 2^n)$ невозрастает по t, поэтому $M(l, h, N, n) = m(h, N, n)$.

Если интервал (l, h) содержит точки h_0 или h_{min}, то разбивается этими точками на 2 или 3 части $I_j = [l_j, h_j]$, каждая из которых попадает в один из рассмотренных случаев. Возьмём пересечение множеств функций для которых $U_{N_f, I_j}(f) = \Omega(M(l_j, h_j, N, n))$ для всех отрезков I_j. Доля функций в пересечении не меньше, чем $1 - \alpha(N)$, где $\alpha(N) \le 2\alpha_1(N) + \alpha_2(N) = O(2^{-N/25})$ при $N \to \infty$. Для каждой функции f из этого пересечения будет выполнено

$$\widehat{U}_{[l,h]}(f) \ge U_{N_f, [l,h]}(f) = \min_j U_{N_f, [l_j, h_j]}(f) = \\ = \Omega(\min_j M(l_j, h_j, N, n)) = \Omega(M(l, h, N, n)).$$

Рассмотрим 3 случая.

1) $h_1(N, n) \in [l, h]$. Тогда с учётом леммы 11 получим $M(l, h, N, n) \le m(h_1, N, n) \asymp h_1 \asymp \inf_{t>=n} m(t, N, n) \le M(l, h, N, n)$, то есть $M(l, h, N, n) \asymp h_1(N, n) = u_1(l, h, N, n)$.

2) $h < h_1(N, n)$. Тогда $h \le h_1 \asymp u_0(h_1, N, 2^n) \le u_0(h, N, 2^n) = u_1(l, h, N, n)$, значит $t = O(u_0(t, N, 2^n))$ при $t \le h$, поэтому $M(l, h, N, n) \asymp \min_{t \in [l,h]} u_0(t, N, 2^n) = u_0(h, N, 2^n)$.

3) $l > h_1(N, n)$. Тогда $l \ge h_1 \asymp u_0(h_1, N, 2^n) \ge u_0(l, N, 2^n)$, значит $u_0(t, N, 2^n) = O(t)$ при $t \ge l$, поэтому $M(l, h, N, n) \asymp \min_{t \in [l,h]} t = l = u_1(l, h, N, n)$.

Нижняя оценка доказана. □

Верхняя оценка.

Хотя теоремы формулируются для базиса без ограничений, для наглядности мы будем использовать базис $\{\vee, \&, \oplus, 1\}$. Отрицание неудобно с

точки зрения верхней оценки потенциала схемы, поэтому его мы использовать не будем. Зато у многих блоков будет вход z. На этот вход должна подаваться 1, если хотя бы один из остальных входов равен 1. Внутри блоков будем использовать только элементы, сохраняющие 0. Это гарантирует нам, что на нулевом входном векторе состояние блока будет нулевым, то есть потенциал на нулевом входном векторе равен 0. Далее будем пользоваться тем свойством, что если $f(0,...,0) = \vec{0}$, то $f(\alpha x_1, \alpha x_2, ..., \alpha x_n) = \alpha f(x_1, ..., x_n)$ $(\alpha \in \{0,1\})$.

Будем говорить, что блок(подсхема) K' схемы K *неактивна на входном наборе* $\vec{x}$, если все входы K' равны 0 при подаче $\vec{x}$ на входы схемы K. В противном случае будем говорить, что блок K' *активен на входном наборе* $\vec{x}$.

У каждого блока есть множество *допустимых входных наборов*, на которых он функционирует корректно. Именно на этом множестве мы будем оценивать его мощность. По умолчанию считаем, что

- если у блока есть вход, помеченный z, и остальные входы $x_1, ..., x_n$, то корректными являются те и только те наборы, для которых $z \geq x_1 \vee ... \vee x_n$;
- иначе все входные наборы являются корректными.

Введём длину и ширину схемы K.

Длиной схемы K называется длина наименьшего прямоугольника, содержащего все непустые элементы схемы K, обозначается $l(K)$.

Шириной схемы K называется ширина наименьшего прямоугольника, содержащего все непустые элементы схемы K, обозначается $h(K)$.

Для блоков, повёрнутых на 90 градусов, будем добавлять верхний индекс $\top$ к названию блока, чтобы явно подчеркнуть, что его длина равна ширине исходного блока и наоборот. Вообще говоря, ориентация блока обычно однозначно устанавливается исходя из расположения его входов и выходов. Поэтому отражённые и перевёрнутые блоки будем обозначать так же, как и исходный блок.

Введём также несколько обозначений.

- Если x – булева переменная, α – булева величина, то $x^\alpha := x \oplus \overline{\alpha}$.
- Если $x = (x_1, ..., x_k)$ и $\alpha = (\alpha_1, ..., \alpha_k)$ – булевы вектора, то $x^\alpha := \bigwedge_{i=1}^{k} x_i^{\alpha_i}$.

- Если i – неотрицательное целое число, $k \in \mathbb{N}$, то $\bar{i}^{(k)}$ – булев вектор, составленный первых k цифр в двоичной записи числа i, начиная с младшего разряда. То есть $i \equiv \bar{i}_1^{(k)} + 2\bar{i}_2^{(k)} + ... + 2^{k-1}\bar{i}_k^{(k)} (\mod 2^k)$. j-ю цифру числа i будем обозначать просто $\bar{i}_j$ без верхнего индекса.

- Если $x = (x_1, ..., x_k)$ – булев вектор, i – неотрицательное целое число, то $x^{\bar{i}} := x^{\bar{i}^{(k)}}$.

Реализация булевой функции с ограниченным числом единиц.

В работе [34] была построена схема, реализующая частичную булеву функцию с оптимальными по порядку площадью, мощностью и глубиной. При построении схемы для функции с ограниченным числом единиц, мы будем использовать частичные функции.

Пусть задана функция $f : \{0,1\}^n \to \{0,1\}$, которая принимает значение 1 на d наборах. Обозначим $k := \lceil \log_2 d \rceil$. Определим функции $f' : \{0,1\}^{n+1} \to \{0,1\}$ и $f''_p : D'_{n/p,n}(\{0,1\}^{n+1})$ следующим образом.

$$f'(z, x_1, ..., x_n) = zf(x_1, ..., x_n),$$
$$f'' = f' \circ D'^{-1}_{n/p,p}.$$

В дальнейшем нам понадобится обозначение $\mathcal{G}_n^p := \mathcal{D}'_{n,p}(\{0,1\}^{np+1})$.

Лемма 12. *Если функция f задана на множестве $\mathcal{D} \subseteq \{0,1\}^n$ мощности d, и задано число $p \geq 2$, $p|n$ причём $n^2 2^{p/n} = O(\sqrt{d})$, то функцию f''_p можно реализовать схемой $S'_{f,p}$ с параметрами*

$$l(S'_{f,p}) \asymp h(S'_{f,p}) \asymp \widehat{U}_{\mathcal{G}^p_{n/p}}(S'_{f,p}) \asymp \sqrt{d}.$$

Доказательство. Схема $S'_{f,p}$ реализуется, как показано на рисунке 2. Здесь схема S_f реализует функцию f'. В [34, Теорема 1] строилась схема функции f, и в самой теореме не указны размеры схемы, но из доказательства следует, что f' реализуется той же схемой, что и f, если заменить элемент «константа 1» на вход z. Причём длина, ширина и потенциал схемы равны $O(\sqrt{|\mathcal{D}|})$.

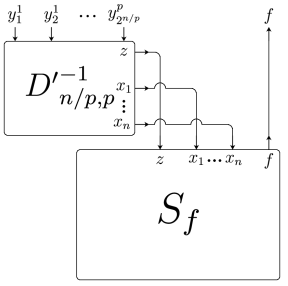


Рис. 2. Реализация схемы $S'_{f,p}$.

Блок $D'^{-1}_{n/p,p}$ имеет параметры

$$\begin{aligned} l(D'^{-1}_{n/p,p}) &= O(p2^{n/p}) = O(n2^{n/p}) = O(\sqrt{d}), \\ h(D'^{-1}_{n/p,p}) &= O((n/p)^2 + n) = O(n^2) = O(\sqrt{d}), \\ \widehat{U}_{\mathcal{G}^p_{n/p}}(D'^{-1}_{n/p,p}) &= O(S(D'^{-1}_{n/p,p})) = O\left(p2^{n/p}((n/p)^2 + n)\right) = \\ &= O\left(\left(\frac{n^2}{p} + np\right)2^{n/p}\right) = O(\sqrt{d}). \end{aligned}$$

Значит

$$\begin{aligned} l(S'_{f,p}) &\le l(S_f) + l(D'^{-1}_{n/p,p}) = O(\sqrt{d}), \\ h(S'_{f,p}) &\le h(S_f) + h(D'^{-1}_{n/p,p}) = O(\sqrt{d}). \end{aligned}$$

Потенциал схемы S'_f складывается из потенциалов блоков S_f, $D'^{-1}_{n/p,p}$ и проводов. Провода занимают площадь $O(n^2)$, значит их потенциал также составляет $O(n^2) = O(\sqrt{d})$.

$$\widehat{U}(S'_{f,p}) \le \widehat{U}_{\mathcal{G}^p_{n/p}}(D'^{-1}_{n/p,p}) + \widehat{U}(S_f) + O(\sqrt{d}) = O(\sqrt{d}).$$

Лемма доказана. □

Далее в громоздких формулах иногда для краткости будем использовать следующие обозначения. За $x_{[i,j]}$ будем обозначать набор $(x_i, x_{i+1}, ..., x_j)$, за $x^{[i,j]}$ — набор $(x^i, x^{i+1}, ..., x^j)$.

Лемма 13. *При $p \ge 2$, $p|n$ и $N \ge n^2$, если*

$$n^2 2^{n/p} \le \sqrt{N},$$

то для произвольной функции $f \in F_N^n$ существует схема $G_{f,p}$, реализующая функцию f_p'' со следующими параметрами.

$$l(G_{f,p}) = O\left((n - \log_2 N)\sqrt{N}\right),$$
$$h(G_{f,p}) = O(\sqrt{N}),$$
$$\widehat{U}_{\mathcal{G}^p_{n/p}}(G_f) = O\left(p(n - \log_2 N)\sqrt{N}\right);$$
$$U_{\mathcal{G}^p_{n/p}}(G_{f,p}) = O\left(p\sqrt{N}\right).$$

Доказательство. Положим $k := \lceil \log_2 N \rceil$. Введём области $D_i \subseteq \{0,1\}^{k+i}$ и частичные функции $f_i : D_i \to \{0,1\}$, $i = 1, ..., n-k$ по следующему правилу.

$D_1 = \{0,1\}^{k+1}$;

$$f_i(x_{[1,k+i]}) = \begin{cases} \text{не определено}, & x_{[1,k+i]} \notin D_i \\ 1, & x_{[1,k+i]} \in D_i \text{ и } \exists x_{[k+i+1,n]} : f(x_{[1,n]}) = 1, \\ 0, & x_{[1,k+i]} \in D_i \text{ и } \forall x_{[k+i+1,n]} (f(x_{[1,n]}) = 0), \end{cases}$$

$D_{i+1} = f_i^{-1}(1) \times \{0,1\} = \{x_{[1,k+i+1]} | x_{[1,k+i]} \in D_i,\ f_i(x_{[1,k+i]}) = 1\}$.

Отметим несколько свойств областей D_i и функций f_i.
Каждой единице функции f_i соответствует единица функции f, то есть $|f_i| \le |f| = N$. Значит $|D_{i+1}| = |f_i^{-1}(1) \times \{0,1\}| = 2|f_i^{-1}(1)| = 2|f_i| \le 2N$.

При произвольном доопределении функций f_i функция f представляется в виде

$$f(x_1, ..., x_n) = \bigwedge_{i=1}^{n-k} f_i(x_1, ..., x_{k+i}).$$

Значит для f' выполнено

$$f'(z, x_1, ..., x_n) = z \bigwedge_{i=1}^{n-k} f_i(x_1, ..., x_{k+i}) = \bigwedge_{i=1}^{n-k} f_i'(z, x_1, ..., x_{k+i}),$$

а для f'' выполнено

$$f_p''(\vec{y}) = f'(D'^{-1}_{n/p,p}(\vec{y})) = \bigwedge_{i=1}^{n-k} f_i'(D'^{-1}_{n/p,p}(\vec{y})). \tag{31}$$

Поскольку $f_i'(\vec{0}) = 0$ и $D'^{-1}_{n/p,p}$ сохраняет 0, то

$$A(\vec{y}) \wedge f_i'(D'^{-1}_{n/p,p}(\vec{y})) = f_i'(D'^{-1}_{n/p,p}(A(y)\&\vec{y})), \tag{32}$$

Построим схему $G_{f,p}$, реализующую функцию f''_p в соответствии с формулой (31), учитывая (32), как показано на рисунке 3. Поскольку функ-

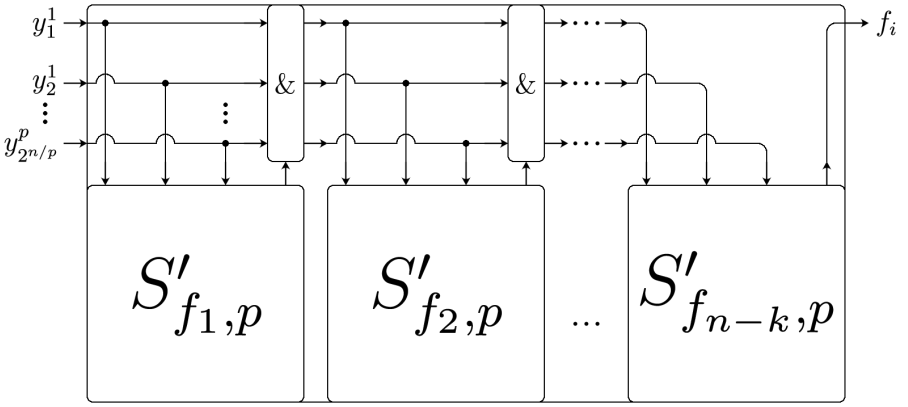


Рис. 3. Схема $G_{f,p}$, реализующая функцию f''.

ции f_i определены на множествах $\mathcal{D}_i$ размера не более $2N$ и $n^2 2^{n/p} \leq \sqrt{N} < \sqrt{|\mathcal{D}_i|}$, то для $\mathcal{D}_i$ и f_i выполнены условия леммы 12, значит все блоки $S'_{f_i,p}$ имеют длину, ширину и потенциал $O(\sqrt{|\mathcal{D}_i|}) = O(\sqrt{N})$.

Оценим параметры схемы $G_{f,p}$.

$$l(G_{f,p}) = \sum_{j=1}^{n-k} l(S'_{f_j}) = O((n-k)\sqrt{N}),$$

$$h(G_{f,p}) = \max_{i=1,\ldots,n-k} h(S'_{f_i,p}) + O(p2^{n/p}) = O(\sqrt{N} + p2^{n/p}) = O(\sqrt{N}).$$

Оценим потенциал схемы.

1) Потенциал проводов. Множеством допустимых наборов для схемы $G_{f,p}$ является область определения функции f'', то есть $\mathcal{G}^p_{n/p} = D'_{n/p,p}(\{0,1\}^{n+1})$, в котором каждый набор имеет не более p единиц.

   Таким образом, не более p из $p2^{n/p}$ проводов, идущих от входов схемы активны. А значит не более p проводов, идущих от каждого из $n-k-1$ блоков конъюнкций, активны. Длина каждого горизонтального участка провода равна $O(l(S'_{f_i,p})) = O(\sqrt{N})$, а длина каждого вертикального участка $O(p2^{n/p}) = O(\sqrt{N})$. Общая длина активных проводов равна $O(p(n-k)\sqrt{N})$.

2) Потенциал блоков конъюнкций. Каждый блок конъюнкций имеет константную длину, а его высота $O(p2^{n/p})$. Значит его площадь $O(p2^{n/p})$. Всего в схеме $(n-k-1)$ таких блоков. Потенциал каждого блока по порядку не больше его площади, то есть $O(p2^{n/p})$. Значит общий потенциал блоков конъюнкций не больше $O((n-k)p2^{n/p}) = O(p(n-k)\sqrt{N})$.

3) Потенциал блоков $S'_{f_i,p}$. Потенциал каждого блока не больше, чем $O(\sqrt{N})$, всего $(n-k)$ блоков, значит суммарный потенциал равен $O((n-k)\sqrt{N})$.

Значит потенциал всей схемы составляет

$$\widehat{U}_{\mathcal{G}^p_{n/p}}(G_{f,p}) = O(p(n-k)\sqrt{N} + (n-k)\sqrt{N}) = O(p(n-k)\sqrt{N}).$$

Чтобы оценить средний потенциал, заметим, что при $i \geq 2$ i-й сегмент схемы активен лишь в том случае, когда $\bigwedge_{j=1}^{i-1} f'_j(z, x_{[1,k+j]}) = 1$. Это происходит лишь на N наборах из возможных 2^{k+i-1}. То есть вероятность того, что i-й сегмент схемы активен, не превосходит $N/2^{k+i-1} \leq 1/2^{i-1}$. Максимальный потенциал каждого сегмента схемы равен $O(p\sqrt{N})$, значит средний потенциал схемы можно оценить сверху

$$p\sqrt{N} + \sum_{i=2}^{n-k} \frac{1}{2^{i-1}} p\sqrt{N} = O(p\sqrt{N}).$$

Лемма доказана. □

Замечание 1. *Построенная в лемме схема имеет сильно вытянутую прямоугольную форму. При необходимости её можно «изогнуть змейкой», чтобы получилась квадратная схема (рис. 4) с длиной и высотой* $O(\sqrt{(n-k)N})$, *при этом каждый провод удлиннится не более, чем в* 4 *раза, поэтому потенциал останется равным* $O\left(p(n-k)\sqrt{N}\right)$.

Оценка потенциала схемы $G_{f,p}$ в $\sqrt{n-k}$ раз выше, чем требуется для доказательства теоремы.

Чтобы уменьшить потенциал, разобьём множество N_f на $s = 2^q$ подмножеств по аналогии с тем, как это делалось в [34, доказательство леммы 12].

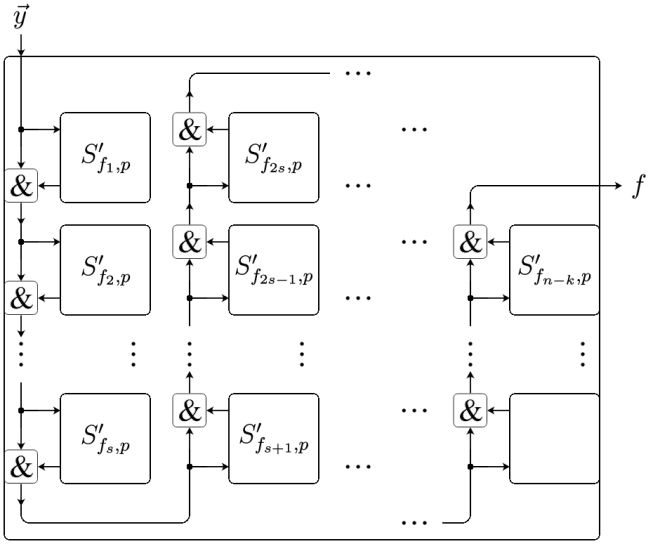


Рис. 4. Квадратная схема $\tilde{G}_{f,p}$, реализующая f''_p.

Лемма 14. *Если* $2^{n-1} \geq N \geq 2^{n/3-1}$, *то для любой функции* $f \in F_N^n$ *существует схема* Q_f, *реализующая функцию* f *с параметрами*

$$\begin{aligned} l(Q_f) &= O(\sqrt{N(n-\log_2 N)}), \\ h(Q_f) &= O(\sqrt{N(n-\log_2 N)}), \\ \widehat{U}(Q_f) &= O(\sqrt{N(n-\log_2 N)}), \\ U(Q_f) &= O(\sqrt{N}). \end{aligned}$$

Доказательство. В доказательстве будем считать, что $8|n$, иначе можно добавить не более 7 фиктивных переменных, порядок оценок от этого не поменяется.

Обозначим $k := \lceil \log_2 N \rceil$, $q := \lceil \log_4(n-k) \rceil$. Для построения схемы Q_f нам понадобится разбить множество N_f примерно на $(n-k)$ одинаковых частей. Для этой цели воспользуемся блоком $I_{n/8,q}$, описанном в [34, доказательство леммы 12], который разобьёт множество N_f на 4^q подмножеств, которые мы обозначим $\mathcal{D}_1, ..., \mathcal{D}_{4^q}$. Роль множества $\mathcal{D}$ у нас будет играть N_f. Поскольку $\frac{n}{8} \leq \frac{1}{4}\log_2 N = \frac{1}{4}\log_2 |N_f|$, то условия [34, леммы 12] выполнены, и можно взять уже посчитанные характеристики блока $I_{n/8,q}$ оттуда.

Выпишем характеристики блока $I_{n/8,q}$. Блок имеет $8 \cdot 2^{n/8}$ входов, которые мы обозначим $\vec{y} = (y_1^1, y_2^1, ..., y_{2^{n/8}}^8)$, и 4^q групп по $8 \cdot 2^{n/8}$ выходов. На j-й группе выходов реализуется функция $\chi_j(D_{n/8,8}^{-1}(\vec{y}))\vec{y}$, если $\vec{y} \neq 0$, и 0, если $\vec{y} = 0$, где $\chi_j(\vec{x})$ — характеристическая функция множества $\mathcal{D}_j$. При этом разбиение мы зададим равномерное, тогда $|\mathcal{D}_j| \leq \lceil N/4^q \rceil \leq N/(n-k)$.

Блок $I_{n/8,q}$ имеет следующие характеристики.

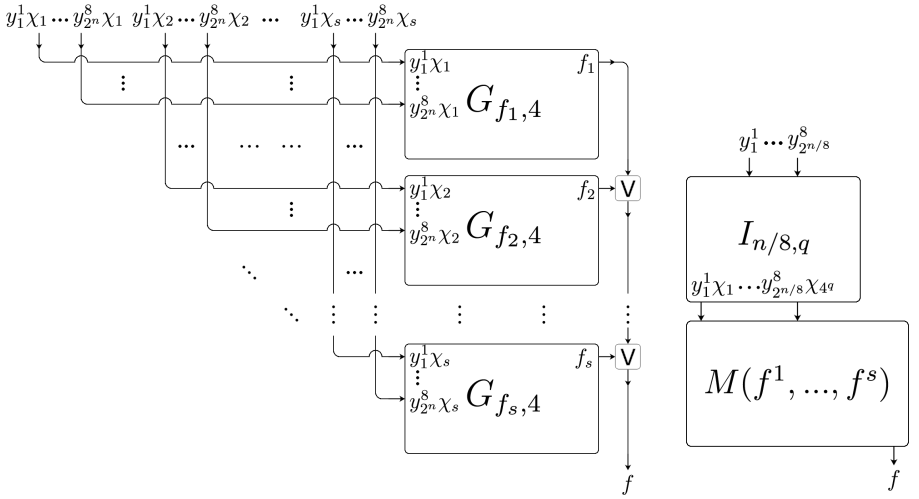
$$\begin{aligned} l(I_{n/8,q}) &= O(2^{n/8} \cdot 4^q) + O(q\sqrt{N}) = \\ &= O((n-k)\sqrt[4]{N} + q\sqrt{N}) = O(\log(n-k)\sqrt{N}), \\ h(I_{n/8,q}) &= O(q2^{n/8}) + O(\sqrt{N}) = O(q\sqrt[4]{N} + \sqrt{N}) = O(\sqrt{N}), \\ \widehat{U}_{\mathcal{G}_{n/8}^8}(I_{n/8,q}) &= O\left(q^2\sqrt{|N_f|}\right) = O(\log^2(n-k)\sqrt{N}). \end{aligned}$$

Если ввести функции $f^i(\vec{y}) := f_8''(\vec{y})\chi_i(D_{n/8,8}^{-1}(\vec{y}))$, то функцию f_8'' можно представить в виде

$$f_8''(\vec{y}) = \bigvee_{i=1}^{s} f^i(\vec{y}) = \bigvee_{i=1}^{s} f^i\Big(\underbrace{\chi_i(D_{n/8,8}^{-1}(\vec{y}))\vec{y}}_{i\text{-я группа выходов блока } I_{n/8,8}} \Big).$$

В соответствии с этим представлением функцию f_8'' можно реализовать схемой, изображённой на рисунке 5.

Теперь опишем блок C_f, изображённый на рисунке 5(b), реализующий функцию f_8''. Этот блок состоит из блока $M(f^1, ..., f^s)$, изображённого на рисунке 5(a), подключённого к блоку $I_{n/8,q}$. Оценим размеры блока $M(f^1, ..., f^s)$. Поскольку $f^s \circ F_{n/8,8} \in F_{N/(n-k)}^n$, то $l(G_{f^i,8}) = O((n - \log_2(N/(n-k)))\sqrt{N/(n-k)})$, $h(G_{f,p}) = O(\sqrt{N/(n-k)})$ по лемме



(a) Блок $M(f^1, ..., f^s)$, реализующий функции $\bigvee_{j=1}^{s} \chi_j {f^j}_8''(\vec{y})$. (b) Блок C_f, реализующий функцию f_8''.

Рис. 5. Реализация функции f_8''.

13. Тогда, учитывая, что $N \geq 2^{n/2}$ получим

$$
\begin{aligned}
l(M(f^1, ..., f^s)) &= O(8 \cdot 2^{n/8} s) + \max_{i=1,...,s} l(G_{f_i,8}) + 1 = \\
&= O\left(8 \cdot 2^{n/8}(n-k)\right) + O\left(\left(n - \log_2 \frac{N}{n-k}\right)\sqrt{\frac{N}{n-k}}\right) = \\
&= O\left((n - k + \log_2(n-k))\sqrt{\frac{N}{n-k}}\right) = O(\sqrt{(n-k)N}), \\
h(M(f^1, ..., f^s)) &= \sum_{i=1}^{s} h(G_{f_i,8}) = O\left(s\sqrt{\frac{N}{n-k}}\right) = O(\sqrt{(n-k)N}).
\end{aligned}
$$

Для схемы C_f имеем

$$\begin{aligned} l(C_f) &= \max\left(l(I_{n/8,q}), l(M(f^1,...,f^s))\right) = \\ &= O\left(\max\left(\log(n-k)\sqrt{N}, \sqrt{(n-k)N}\right)\right) = O(\sqrt{(n-k)N}), \\ h(C_f) &= h(M(f^1,...,f^s)) + h(I_{n/8,q}) = \\ &= O(\sqrt{(n-k)N} + \sqrt{N}) = O(\sqrt{(n-k)N}). \end{aligned}$$

Теперь оценим потенциал блока C_f на наборах $y \in \mathcal{G}^8_{n/8}$. Он складывается из следующих величин.

1) Потенциал блока $I_{n/8,q}$, который оценивается, как $O(\log^2(n-k)\sqrt{N})$.

2) Потенциал проводов в блоке $M(f^1,...,f^s)$, идущих от входов к блокам $G_{f^i,8}$. Поскольку входы блока $M(f^1,...,f^s)$ подключены к выходам блока $I_{n/8,q}$, то для любого входного набора $y \in \mathcal{G}^8_{n/8}$ не более, чем на 8 входах блока M будут единицы. Поскольку длина каждого провода не больше, чем

$$l(M(f^1,...,f^s)) + h(M(f^1,...,f^s)) = O(\sqrt{(n-k)N}),$$

то потенциал будет также не более $O(\sqrt{(n-k)N})$.

3) Потенциал блоков $G_{f^i,8}$. Для фиксированного набора $y \in G^8_{n/8}$ не более одной группы выходов $I_{n/8,q}$ активно, значит не более одного активного блока $G_{f^i,8}$. Тогда суммарный потенциал всех блоков $G_{f^i,8}$ не превосходит

$$\max_{i=1,...,s} U_{\mathcal{G}^8_{n/8}}(G_{f^i,8}) = O\left(8\left(n - \log_2\frac{N}{s}\right)\sqrt{\frac{N}{s}}\right) = O(\sqrt{(n-k)N}).$$

4) Потенциал проводов и дизъюнкций, соединяющих выходы блоков $G_{f^i,8}$ с выходом блока $M(f^1,...,f^s)$. Вся эта часть схемы помещается в прямоугольнике $1 \times h(M(f^1,...,f^s))$. Потенциал не превосходит площади, то есть

$$O(h(M(f^1,...,f^s))) = O(\sqrt{(n-k)N}).$$

Суммарный потенциал схемы можно оценить сверху суммой потенциалов её частей, то есть

$$O(\log^2(n-k)\sqrt{N}) + O(\sqrt{(n-k)N}) = O(\sqrt{(n-k)N}).$$

Для реализации функции f было бы достаточно подключить C_f к блоку дешифраторов $D_{n/8,8}$, но в этом случае мы не получим требуемую оценку среднего потенциала. Поэтому введём ещё одну вспомогательную функцию

$$\hat{f}(x_{[1,k+t]}) = \begin{cases} 1, & \exists \alpha_{[k+t+1,n]} \in \{0,1\} : f(x_{[1,k+t]}, \alpha_{[t+1,n]}) = 1, \\ 0, & \text{иначе}, \end{cases}$$

где $t = \lfloor \log_2(n-k) \rfloor$. Важно, что $\tilde{f}(x_{[1,k+t]}) \geq f(x_{[1,n]})$, поэтому

$$f(x_{[1,n]}) = \tilde{f}(x_{[1,k+t]}) f(x_{[1,n]}).$$

Для удобства можно ввести функцию $\tilde{f}(x_{[1,n]}) = \hat{f}(x_{[1,k+t]})$, зависящую от n переменных, но последние $n-k-t$ переменных фиктивные. При этом сложность схемы можно считать, исходя из количества существенных переменных, поскольку фиктивные входы можно удалить.

Поскольку количество наборов, на которых $\tilde{f}$ равна 1, не превосходит $N \leq 2^k$, то доля наборов, на которых эта функция равна 1, составляет $O(2^{-t}) = O(1/(n-k))$. За счёт этого можно сэкономить множитель $\sqrt{n-k}$ для среднего потенциала, если фильтровать наборы при помощи $\tilde{f}$ перед подачей их на входы C_f.

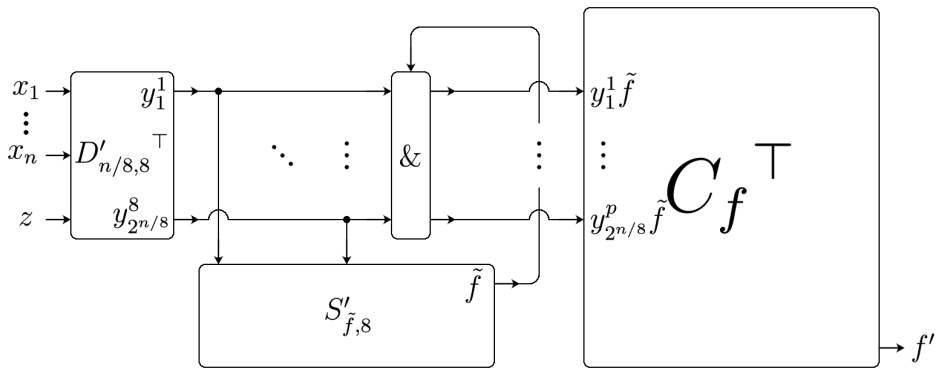


Рис. 6. Блок H_f, реализующий функцию f'.

Схема H_f, реализующая эту идею, изображена на рисунке 6. Функция f' вычисляется по формуле

$$\begin{aligned} f'(\vec{x},z) = f'(\vec{x},z)\tilde{f}(\vec{x}) &= f''_8(D'_{n/8,8}(\vec{x},z)\tilde{f}(\vec{x})) = \\ &= f''_8(D'_{n/8,8}(\vec{x},z)\tilde{f}'(\vec{x},z)) = \\ &= f''_8\Big(D'_{n/8,8}(\vec{x},z)\tilde{f}''_8(D'_{n/8,8}(\vec{x},z))\Big). \end{aligned} \tag{33}$$

Здесь мы использовали, что $f''_8(\vec{x})y = f''_8(\vec{x}y)$, поскольку f''_8 сохраняет 0. Оценим размеры и потенциал схемы H_f. Учитывая ограничения на N, получим

$$\begin{aligned} l(H_f) &= l({D'_{n/8,8}}^{\top}) + l(G_{\tilde{f},8}) + 1 + l(C_f^{\top}) = \\ &= h(D'_{n/8,8}) + l(G_{\tilde{f},8}) + 1 + h(C_f) = \\ &= O(n^2) + O((\underbrace{k + t - \log_2 N}_{\sim t \sim \log_2(n-k)})\sqrt{N}) + O(\sqrt{(n-k)N}) = \\ &= O(\sqrt{(n-k)N}), \\ h(H_f) &\le \max\Big(h({D'_{n/8,8}}^{\top}) + h(G_{\tilde{f},8}), h(C_f^{\top})\Big) = \\ &= \max\Big(l(D'_{n/8,8}) + h(G_{\tilde{f},8}), l(C_f)\Big) = \\ &= O\Big(\max(2^{n/8} + \sqrt{N}, \sqrt{(n-k)N})\Big) = O(\sqrt{(n-k)N}). \end{aligned}$$

Оценим потенциал каждой части схемы H_f. Сначала оценим начальную часть схемы – блок дешифраторов, блок $G_{\tilde{f},8}$, блок конъюнкций и ведущие к ним провода. Обозначим эту часть схемы за H_f^0.

1) Потенциал блока $D'_{n/8,8}$ не превосходит его площади, то есть $O(2^{n/8}n^2)$.

2) Потенциал проводов, идущих из блока $D'_{n/8,8}$ в блоки $G_{\tilde{f},8}$ и блок конъюнкций. каждый провод имеет горизонтальный и вертикальный участок длиной $O(8 \cdot 2^{n/8}) = O(2^{n/8})$. Поскольку есть не более 8 активных проводов, то максимальный потенциал не превосходит $O(2^{n/8})$.

3) Потенциал блока конъюнкций не больше его площади, то есть $O(8 \cdot 2^{n/8}) = O(2^{n/8})$.

4) Максимальный потенциал блока $G_{\tilde{f},8}$ по лемме 13 не превосходит

$$O(8(k+t-\log_2 N)\sqrt{N}) = O(t\sqrt{N}) = O(\log_2(n-k)\sqrt{N}),$$

а средний потенциал не превосходит $O(8\sqrt{N}) = O(\sqrt{N})$.

Теперь просуммируем и получим оценку максимального потенциала подсхемы H_f^0.

$$\widehat{U}(H_f^0) = O(2^{n/8}n^2) + O(2^{n/8}) + O(\log_2(n-k)\sqrt{N}) = O(\log(n-k)\sqrt{N}). \tag{34}$$

Средний потенциал запишем при условии, что $z = 1$.

$$U_{z=1}(H_f^0) = O(2^{n/8}n^2) + O(2^{n/8}) + O(\sqrt{N}) = O(\sqrt{N}). \tag{35}$$

Оставшуюся часть схемы обозначим за H_f^1. Оценим потенциал каждой части подсхемы H_f^1.

1) Потенциал провода, идущего от выхода $G_{\tilde{f},8}$ к блоку конъюнкций. Длина его горизонтального участка составляет $O(l(G_{\tilde{f},8})) = O(\log(n-k)\sqrt{N})$, а длина вертикального участка равна $O(2^{n/8})$. Тогда максимальный потенциал не больше, чем длина провода, то есть
$$O(2^{n/8}) + O(\log(n-k)\sqrt{N}) = O(\log(n-k)\sqrt{N}).$$

2) Провода, идущие от блока конъюнкций к блоку C_f. Не более 8 из этих проводов активны, и длина каждого провода составляет $O(l(G_{\tilde{f},8})) = O(\log(n-k)\sqrt{N})$, поэтому потенциал тоже будет равен $O(\log(n-k)\sqrt{N})$.

3) Блок C_f. Его потенциал равен $O(\sqrt{(n-k)N})$.

Просуммируем и получим оценку максимального потенциала подсхемы H_f^1.

$$\widehat{U}(H_f^1) = O(\log(n-k)\sqrt{N}) + O(\sqrt{(n-k)N}) = O(\sqrt{(n-k)N}). \tag{36}$$

Здесь отметим, что если $\tilde{f}(\vec{x}) = 0$, то при подаче набора $\vec{x}$ на входы H_f, вся подсхема H_f^1 окажется неактивна. Отсюда мы можем получить

оценку среднего потенциала. Средний потенциал считаем при условии, что $z = 1$.

$$U_{z=1}(H_f^1) = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} u_{H_f^1}(\vec{x}, 1) \le \frac{1}{2^n} \sum_{x\in\{0,1\}^n : \tilde{f}(x)=1} \widehat{U}(H_f^1) =$$
$$= \frac{1}{2^{k+t}} \sum_{x\in\{0,1\}^{k+t} : \hat{f}(x)=1} \widehat{U}(H_f^1) \le \underbrace{\frac{1}{2^{k+t}} N}_{\le 2^{-t}} \widehat{U}(H_f^1) =$$
$$= O(2^{-t}\sqrt{(n-k)N}) = O(\sqrt{N/(n-k)}). \quad (37)$$

В итоге получим

$$\widehat{U}(H_f) \le \widehat{U}(H_f^0) + \widehat{U}(H_f^1) =$$
$$= O(\log(n-k)\sqrt{N} + \sqrt{(n-k)N}) = O(\sqrt{(n-k)N}),$$
$$U_{z=1}(H_f) \le U_{z=1}(H_f^0) + U_{z=1}(H_f^1) =$$
$$= O(\sqrt{N}) + O(\sqrt{N/(n-k)}) = O(\sqrt{N}).$$

Схема Q_f получается из схемы H_f подключением константы 1 ко входу z. Все оценки для H_f будут верны и для Q_f, только у Q нет входа z, поэтому $U(Q_f) = U_{z=1}(H_f)$. Лемма доказана. □

Теперь рассмотрим случай, когда $N \le 2^{n/3}$, и входы схемы расположены рядом. Докажем вспомогательную лемму.

Лемма 15. *Если $k = \lceil \log_2 N \rceil$, $t > 0$ и $n = st+2k$, то для любой функции $f \in \mathcal{F}_N^n$ существуют линейные операторы $l_i : \{0,1\}^{2k+t} \to \{0,1\}^{2k}$ и функции $f^i \in \mathcal{F}_N^{2k+t}$ такие, что функцию $f' = zf$ можно вычислить следующим алгоритмом.*

Разобьём переменные функции f на $s+1$ группу $x^0 = (x_1^0, ..., x_{2k}^0) \in \{0,1\}^{2k}$, $x^i = (x_1^i, ..., x_t^i) \in \{0,1\}^t$ при $i = 1, ..., s$.

1) $z_0 := z$, $y^0 = x^0$.

2) Для $i = 1, ..., s$ вычисляем

$$y^i := l_i(z_{i-1}y^{i-1}, z_{i-1}x^i), \qquad z_i := z_{i-1}f^i(z_{i-1}y^{i-1}, z_{i-1}x^i).$$

3) $f'(z, x^0, ..., x^s) = y^s$.

Доказательство. Для всех $i = 1, ..., s$ определим функции

$$g_i(x^{[0,i]}) = \begin{cases} 1, & \text{если } \exists \alpha^{[i+1,s]} \in \{0,1\}^k : (f(x^{[0,i]}, \alpha^{[i+1,s]}) = 1), \\ 0, & \text{иначе.} \end{cases}$$

Также введём множества

$$\mathcal{D}_0 = \{0,1\}^{2k}, \qquad \mathcal{D}_i = g_i^{-1}(1) = \left\{ x^{[0,i]} : g_i(x^{[0,i]}) = 1 \right\}, \ i = 1, ..., s.$$

Заметим, что при $\mathcal{D}_{i-j}$ — проекция множества $\mathcal{D}_i$ на первые $2k + t(i-j)$ компонент при $j < i$, а при $j = i$ совпадает с множеством всех наборов длины $2k$ и содержит в себе проекцию $\mathcal{D}_i$ на первые $2k$ компонент.

Определим частичные функции $\tilde{g}_i$ следующим образом.

$$\tilde{g}_1 = g_1,$$
$$\tilde{g}_i = g_i|_{\mathcal{D}_{i-1}} \text{ при } i \geq 2.$$

Тогда

$$f(x^0, ..., x^s) = g_1(x^0, x^1)...g_s(x^0, ..., x^s) = \tilde{g}_0(x^0)\tilde{g}_1(x^0, x^1)...\tilde{g}_s(x^0, ..., x^s)$$

вне зависимости от доопределения $\tilde{g}_i$ вне области $\mathcal{D}_i$, поскольку там конъюнкция $g_j, j < i$ равна 0.

Определим по индукции линейные операторы $l_i : \{0,1\}^{2k+t} \to \{0,1\}^{2k}, \tilde{l}_i : \{0,1\}^{2k+it} \to \{0,1\}^{2k}$ и функции $f^i \in \mathcal{F}_N^{2k+t}$. При этом требуем, чтобы оператор $\tilde{l}_i$ был инъективным на множестве $\mathcal{D}_i$. Обозначим $\tilde{\mathcal{D}}_i := \tilde{l}_i(\mathcal{D}_i)$.

База индукции.

$$\tilde{l}_0(x^0) = x^0, \qquad f^0 \equiv 1.$$

Оператор $\tilde{l}_0$ тождественный, поэтому он инъективен.

Шаг индукции. Пусть $i \geq 1$ и определён оператор $\tilde{l}_{i-1}$, причём $\tilde{l}_{i-1}$ инъективен на $\mathcal{D}_{i-1}$. Тогда для всех $(x^0, ..., x^{i-1}) \in \mathcal{D}_{i-1}$ положим

$$f^i(\tilde{l}_{i-1}(x^0, ..., x^{i-1}), x^i) = g_i(x^0, ..., x^{i-1}, x^i). \tag{38}$$

Поскольку оператор $\tilde{l}_{i-1}$ по предположению индукции инъективен на множестве $\mathcal{D}_{i-1}$, то (38) корректно задаёт функцию f^i на множестве $\tilde{\mathcal{D}}_{i-1} = \tilde{l}_{i-1}(\mathcal{D}_{i-1})$. Вне этого множества доопределим функцию f^i константой 0.

Тогда определение f^i можно записать следующим образом.

$$f^i(y^{i-1}, x^i) = \begin{cases} g_i(\tilde{l}_{i-1}^{-1}(y^{i-1}), x^i), & \text{если } y^{i-1} \in \tilde{\mathcal{D}}_{i-1}, \\ 0, & \text{если } y^{i-1} \notin \tilde{\mathcal{D}}_{i-1}. \end{cases}$$

Поскольку $\tilde{l}_{i-1}^{-1}$ биективно отображает $\tilde{\mathcal{D}}_{i-1}$ на $\mathcal{D}_{i-1}$, то $|f^{i^{-1}}(1)| = |g_i^{-1}(1)| \leq N$, то есть $f^i \in \mathcal{F}_N^{2k+t}$.

Обозначим $\mathcal{D}'_i := f^{i^{-1}}(1) = (y^{i-1}, x^i) : f^i(y^{i-1}, x^i) = 1$. Поскольку $|\mathcal{D}'_i| \leq N \leq 2^k$, то по лемме [34, лемма 9] существует линейный оператор $l_i : \{0,1\}^{2k+t} \to \{0,1\}^{2k}$, инъективный на $\mathcal{D}'_i$.

Определим

$$\tilde{l}_i(x^0, ..., x^i) := l_i(\tilde{l}_{i-1}(x^0, ..., x^{i-1}), x^i)$$

и покажем, что $\tilde{l}_i$ инъективен на $\mathcal{D}_i$. Допустим, существуют различные векторы $x = (x^0, ..., x^i)$, $x' = (x'^0, ..., x'^i) \in \mathcal{D}_i$ такие, что $\tilde{l}_i(x) = \tilde{l}_i(x')$.

Поскольку $x, x' \in \mathcal{D}_i$ и $\mathcal{D}_{i-1}$ содержит проекцию $\mathcal{D}_i$ на первые $2k + t(i-1)$ компонент, то $(x^0, ..., x^{i-1}), (x'^0, ..., x'^i) \in \mathcal{D}_{i-1}$. Это значит, что

$$y^{i-1} := \tilde{l}_{i-1}(x^0, ..., x^{i-1}) \in \tilde{\mathcal{D}}_{i-1},$$
$$y'^{i-1} := \tilde{l}_{i-1}(x'^0, ..., x'^{i-1}) \in \tilde{\mathcal{D}}_{i-1},$$

отсюда

$$f^i(y^{i-1}, x^i) = g_i(x^0, ..., x^i) = 1,$$
$$f^i(y'^{i-1}, x'^i) = g_i(x'^0, ..., x'^i) = 1,$$

значит (y^{i-1}, x^i), $(y'^{i-1}, x'^i) \in D'_i$. С другой стороны, $l_i(y^{i-1}, x^i) = \tilde{l}_i(x) = \tilde{l}_i(x') = l_i(y'^{i-1}, x'^i)$, но поскольку l_i инъективен на D'_i, то $(y^{i-1}, x^i) = (y'^{i-1}, x'^i)$. Поскольку $x \neq x'$, то $x^{[0,i-1]} \neq x'^{[0,i-1]}$, и при этом $\tilde{l}_{i-1}(x^{[0,i-1]}) = y^{i-1} = y'^{i-1} = \tilde{l}_{i-1}(x'^{[0,i-1]})$.

Получаем противоречие с предположением индукции о том, что оператор $\tilde{l}_{i-1}$ инъективен на $\mathcal{D}_{i-1}$.

Теперь можем выразить частичные функции $\tilde{g}_i(x^{[0,i]}) = f^i(\tilde{l}(x^{[0,i-1]}), x^i)$. Обозначив $y^i := \tilde{l}_i(x^{[0,i]})$ и учитывая определение $\tilde{l}_i$, получим

$$f'(z,x^0,...,x^s) := zf(x^0,...,x^s) = z\tilde{g}_1(x^0,x^1)...\tilde{g}_s(x^0,...,x^s) =$$
$$= zf^1(\tilde{l}_0(x^0),x^1)f^1(\tilde{l}_1(x^0,x^1),x^2)...f^s(\tilde{l}_0(x^0,...,x^{s-1}),x^s) =$$
$$= zf^1(y^0,x^1)f^2(y^1,x^2)...f^s(y^{s-1},x^s).$$

Обозначив $z_i := zf^1(y^0,x^1)f^2(y^1,x^2)...f^i(y^{i-1},x^i)$, получим, что

$$z_i = z_{i-1}f^i(y^{i-1},x^i),$$
$$y^i = l_i(y^{i-1},x^i).$$

Учитывая, что при $z_i = 0$ функция f' равна 0, вне зависимости от сомножителей $f^{i+j}(...), j \geq 1$, то в этих сомножителях можно заменить все переменные на их конъюнкцию с z_i, тогда шаг алгоритма будет выглядеть следующим образом.

$$z_i = z_{i-1}f^i(z_{i-1}y^{i-1}, z_{i-1}x^i),$$
$$y^i = l_i(z_{i-1}y^{i-1}, z_{i-1}x^i).$$

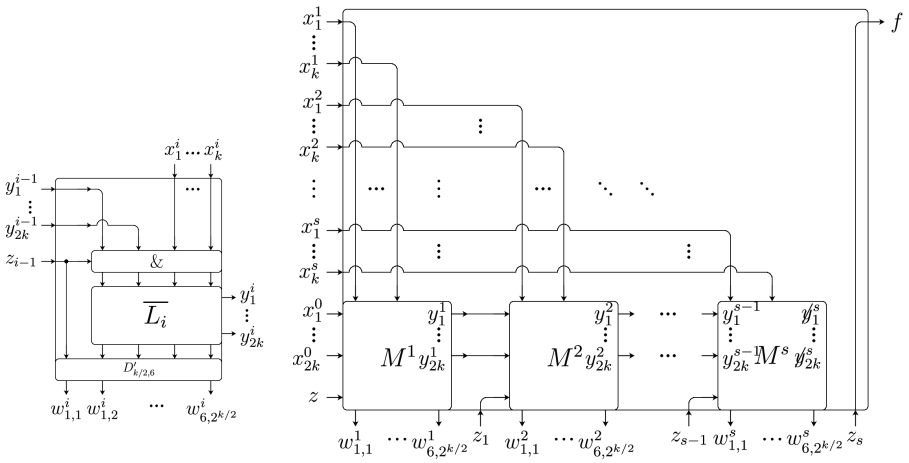
Таким образом, алгоритм, описанный в условии леммы, вычисляет функцию f'. □

Лемма 16. *Если $2^{n-1} \geq N \geq n$, то для любой функции $f \in F_N^n$ существует схема SN_f, реализующая функцию f с параметрами*

$$l(SN_f) = O(\sqrt{Nn}),$$
$$h(SN_f) = O(\sqrt{Nn}),$$
$$\widehat{U}(SN_f) = O\left(\frac{n\sqrt{nN}}{\log\max(2,N/n)}\right),$$

Доказательство. При $N \geq 2^{n/3-1}$ применима лемма 14, и в качестве SN_f можно взять Q_f. Поэтому далее считаем, что $N \leq 2^{n/3}$.

Как и в лемме 15, обозначим $k := \lceil \log_2 N \rceil$. Также определим $k' := \lceil \log_2 \max(2,(N/n))/4 \rceil$. Без ограничения общности будем считать, что $n = k(s+2)$ для некоторого $s = q^2$, $q \in \mathbb{N}$ (иначе можно добавить $O(\sqrt{kn})$ входов и подать на них константу 0). Разобьём входные переменные функции f на группы $x^0,...,x^s$, где $x^0 = (x_1^0,...,x_{2k}^0)$, $x^i = (x_1^i,...,x_k^i)$ при $i \geq 1$.



(a) Вспомогательный блок M^i.

(b) Вспомогательный блок R_n^s.

Рис. 7.

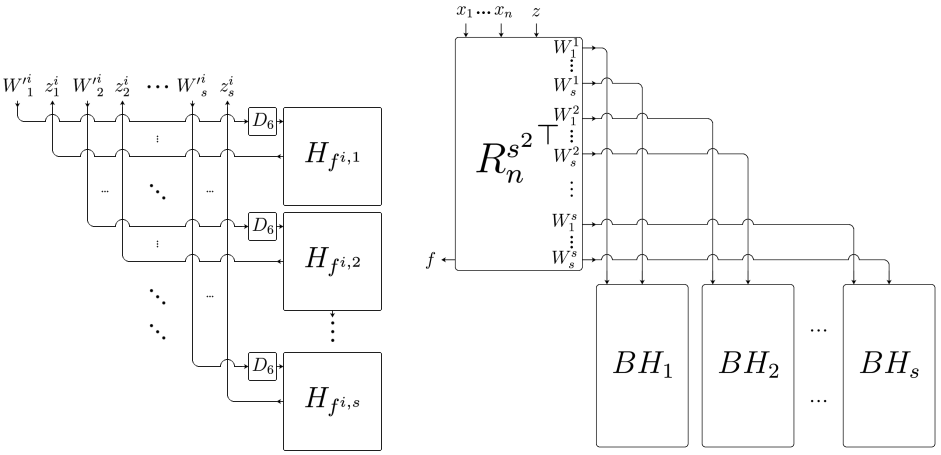
Тогда по лемме 15 при $t = k$ существуют линейные операторы $l_i : \{0,1\}^{3k} \to \{0,1\}^{2k}$ и функции $f^i \in \mathcal{F}_N^{3k}$ такие, что $f' = zf$ может быть вычислена алгоритмом, описанным в условии леммы 15.

Этот алгоритм реализуется схемой SN_f, изображённой на рисунке 8(b) с использованием блоков, изображённых на рисунках 8(a) и 7. Более точно, по сравнению с алгоритмом добавляются ещё блоки $D'_{k',\lceil k/k' \rceil}$ и $D_6 = D'^{-1}_{k',\lceil k/k' \rceil}$. На входы блоков $H_{f^{i,j}}$ сигнал подаётся через пару взаимно обратных операторов $D'_{k',\lceil k/k' \rceil}$ и $D_6 = D'^{-1}_{k',\lceil k/k' \rceil}$, чтобы снизить потенциал на проводах, ведущих от распределительного блока R к блокам $H_{f^{i,j}}$.

Функционирование схемы SN_f.

1) Блок M^i. Этот блок вычисляет $y^i = l_i(z_{i-1}y^{i-1}, z_{i-1}x^i)$ при помощи блока $\overline{L}_i$. Также вектор $(z_{i-1}, z_{i-1}y^{i-1}, z_{i-1}x^i)$ пропускается через блок дешифраторов $D'_{k',6}$ для передачи сигнала по проводам W^i к блоку H_{f^i}, вычисляющему функцию $f^{i\prime}(z_{i-1}, z_{i-1}y^{i-1}, z_{i-1}x^i) = z_{i-1}f^i(z_{i-1}y^{i-1}, z_{i-1}x^i)$.

2) Блок R_n^s включает в себя все блоки M^i и соединяющие их провода.



(a) Блок BH^i, реализующий функции $f^{i,1}, ..., f^{i,s}$. Здесь $D_6 := {D'}^{-1}_{k/2,6}{}^{\top}$.

(b) Блок SN_f, реализующий функцию f'.

Рис. 8. Реализация функции f схемой с близко расположенными входами.

3) Блок SN_f состоит из блока R^s_n и блоков H_{f^i}, подключённым к блоку R^s_n через обратный к блоку дешифраторов преобразователь D_6. Несложно убедиться в том, что схема SN_f вычисляет f' в соответствии с алгоритмом из леммы 15.

Оценки параметров блоков схемы SN_f. Напомним, что $k' = \lceil \log \max(2, N/n)/4 \rceil$, поэтому $2^{k'} = O(\max(1, \sqrt[4]{N/n})) = O(\sqrt[4]{N/n})$ при $N \geq n$.

1) Блок M^i, изображённый на рисунке 5(a).

$$
\begin{aligned}
l(M^i) &\leq \max(l(\overline{L}_i), l(D'_{k',\lceil k/k' \rceil})) = \\
&= O(\max(3k, \lceil k/k' \rceil \cdot 2^{k'})) = O\left(\frac{k}{k'} \sqrt[4]{N/n}\right), \\
h(M^i) &\leq 2k + h(\overline{L}_i) + h(D'_{k',\lceil k/k' \rceil}) = O(k + kk') = O(kk'), \\
\widehat{U}(M^i) &= O(l(M^i)h(M^i)) = O(k^2 \sqrt[4]{N/n}).
\end{aligned}
$$

2) Блок R_n^s, изображённый на рисунке 7.

$$l(R_n^s) = \sum_{i=1}^{s} l(M^i) + O(s) = O\left(s\frac{k}{k'}\sqrt[4]{N/n}\right) =$$
$$= O\left(\frac{n}{k}\frac{k}{k'}\sqrt[4]{\frac{N}{n}}\right) = O\left(\frac{\sqrt[4]{Nn^3}}{k'}\right),$$
$$h(M^i) = \max_{i=1,\ldots,s} h(M^i) + O(n) = O(n + kk') = O(n + \log^2 N),$$
$$\widehat{U}(R_n^s) = O(l(R_n^s)h(R_n^s)) = O\left(\frac{(n+kk')\sqrt[4]{Nn^3}}{k'}\right) =$$
$$= O\left(\frac{n\sqrt{Nn}}{k'}\sqrt[4]{\frac{n}{N}}(1+\frac{kk'}{n})\right) =$$
$$= O\left(\frac{n\sqrt{Nn}}{k'}\frac{\log\max(2,N/n)}{\sqrt[4]{N/n}}\right) = O\left(\frac{n\sqrt{Nn}}{k'}\right).$$

3) Блок BH_i, изображённый на рисунке 8(а). Для этого блока оценим только его размеры, потенциал будем считать сразу для всей схемы SN_f. За $l(W'^j_i)$ обозначим количество проводов в пучке W'^j_i. Поскольку W'^j_i выходит из блока дешифраторов $D'_{k',\lceil k/k'\rceil}$, то $l(W'^j_i) = O(2^{k'}k/k')$.

$$l(BH_i) = \sum_{j=1}^{q} l(W'^i_j) + O(q) + l(D_6) + \max_{j=1,\ldots,q} l(H_{f^{i,j}}) =$$
$$= O\left(q\frac{k}{k'}2^{k'} + kk' + \sqrt{Nk}\right) =$$
$$= O\left(\sqrt{\frac{n}{k}}\frac{k}{k'}\sqrt[4]{\frac{N}{n}} + \log^2 N + \sqrt{Nk}\right) =$$
$$= O\left(\frac{\sqrt{k}}{k'}\sqrt[4]{Nn} + \sqrt{Nk}\right) = O(\sqrt{Nk}),$$
$$h(BH_i) \le \sum_{j=1}^{q}(h(D_6) + h(H_{f^{i,j}})) = O(q(2^{k'}k/k' + \sqrt{Nk})) =$$
$$= O\left(\sqrt{\frac{n}{k}}\left(\sqrt{Nk} + \sqrt[4]{\frac{N}{n}}\frac{k}{k'}\right)\right) = O(\sqrt{Nn}).$$

Теперь оценим параметры всей схемы SN_f, изображённой на рисунке 8(b).

$$l(SN_f) = l({R_n^s}^\top) + \sum_{i=1}^{q} l(BH_i) = h(R_n^s) + O(q\sqrt{Nk}) =$$
$$= O(n + kk') + O\left(\sqrt{\frac{n}{k}}\sqrt{Nk}\right) = O(\sqrt{Nn}),$$
$$h(SN_f) \le h({R_n^s}^\top) + \max_{i=1,\dots,s} h(BH_i) = l(R_n^s) + O(\sqrt{nN}) =$$
$$= O\left(\frac{\sqrt[4]{Nn^3}}{k'} + \sqrt{nN}\right) = O(\sqrt{nN}).$$

Будем оценивать максимальный потенциал частей схемы SN_f.

- Блок R_n^s. Его потенциал мы уже считали, он составляет $O(\frac{n\sqrt{Nn}}{k'})$.
- Провода ${W'}_i^j$. Заметим, что длина каждого пучка проводов ${W'}_i^j$ не больше, чем полупериметр схемы SN_f, то есть $O(\sqrt{nN})$. При этом поскольку каждый такой пучок выходит из блока $D'_{k',\lceil k/k'\rceil}$, то не более $\lceil k/k'\rceil$ проводов могут быть одновременно активны. Поскольку всего s пучков, то суммарный потенциал проводов не превосходит
$$O\left(s\frac{k}{k'}\sqrt{nN}\right) = O\left(\frac{n}{k}\frac{k}{k'}\sqrt{nN}\right) = O\left(\frac{n\sqrt{nN}}{k'}\right).$$
- Провода, идущие от блоков $H_{f^{i,j}}$ к блоку R_n^s. Их s штук, и длина каждого провода также не больше полупериметра схемы, поэтому суммарный потенциал не больше, чем $O(s\sqrt{nN}) = O(n\sqrt{nN}/k) = O(n\sqrt{nN}/k')$.
- Потенциал блоков D_6.
$$U(D_6) = O(l(D_6)h(D_6)) = O\left(\frac{k}{k'}2^{k'}kk'\right) = O\left(k^2\sqrt[4]{\frac{N}{n}}\right).$$
Всего $s = O(n/k)$ таких блоков, поэтому суммарный потенциал равен
$$O\left(\frac{n}{k}k^2\sqrt[4]{\frac{N}{n}}\right) = O\left(n\sqrt[4]{N/n}\log N\right) = O(n\frac{\sqrt{N}}{\log N}) = O\left(\frac{n\sqrt{N}}{k'}\right).$$

- Потенциал блоков $H_{f^{i,j}}$.

$$\widehat{U}(H_{f^{i,j}}) = O(\sqrt{N(3k - \log_2 N)}) = O(\sqrt{Nk}).$$

Всего $s = O(n/k)$ таких блоков, поэтому их суммарный потенциал не превосходит

$$O\left(\frac{n}{k}\sqrt{Nk}\right) = O\left(\frac{n\sqrt{N}}{\sqrt{k}}\right) = O\left(\frac{n\sqrt{nN}}{k'}\right).$$

Сложив потенциалы частей, получим

$$\widehat{U}(SN_f) = O\left(\frac{n\sqrt{nN}}{k'}\right) = O\left(\frac{n\sqrt{nN}}{\log \max(2, N/n)}\right),$$

что и требовалось. Лемма доказана. □

Теперь мы можем приступить к доказательству верхней оценки в теореме 2. Сформулируем её в виде леммы.

Лемма 17. *Если* $2^{n-1} \geq N \geq 4$, *то для параметра* h, *удовлетворяющего условию*

$$\sqrt{Rn/\log_2 N} \geq h \geq n, \quad R = N(n - \log_2 N), \tag{39}$$

и для любой функции $f \in F_N^n$ *существует схема* $SL_f^h \in Q_{[0,C_1 h]}$, *реализующая функцию* f *с параметрами*

$$\begin{aligned} l(SL_f^h) &= O(\max(h, \sqrt{R})), \\ h(SL_f^h) &= O\left(\frac{R}{\max(h, \sqrt{R})}\right), \\ \widehat{U}(SL_f^h) &= O(u_0(h, N, 2^n)), \\ U(SL_f^h) &= O(\max(\sqrt{N}, n)). \end{aligned}$$

Здесь $C_1 > 0$ — *некоторая константа.*

Доказательство. Здесь будем опять использовать алгоритм вычисления функции из леммы 15, только для вычисления функций f^i будем уже использовать блоки SN, построенные в предыдущей лемме.

Как и ранее, обозначим $k = \lceil \log_2 N \rceil$. Заметим, что при $k > n/3$ утверждение леммы напрямую следует из леммы 14, поэтому далее полагаем $k \leq n/3$. Введём параметр $s = \max(1, \lfloor h^2/3R \rfloor)$. Тогда из условия (39) следует, что $s \leq n/3\log_2 N$. Положим $t = \lceil (n - 2k)/s \rceil$. Тогда

$2k + (s-1)t < n \leq 2k + st$. Положим $t' = n - (2k + (s-1)t)$, $n' = 2k + st$. Тогда $1 \leq t' \leq t$.

Заметим, что

$$s \leq \max(1, h^2/3R) = \max\left(1, \frac{Rn}{3R\log_2 N}\right) = \max(1, n/\log_2 N) \leq \frac{n}{k-1}.$$

Отсюда $t \geq \frac{(n-2k)}{s} \geq n/3s \geq k-1$, то есть $k \leq t+1$. С другой стороны, $s \geq n^2/R \geq n/N$, поэтому $t = O(n/s) = O(N)$. Эти оценки понадобятся, когда мы будем оценивать параметры схемы.

Определим функцию

$$\tilde{f}(x_1, ..., x_n, x_{n+1}, ..., x_{n'}) = \begin{cases} f(x_1, ..., x_n), & \text{если } x_{n+1} = ... = x_{n'} = 0, \\ 0, & \text{иначе.} \end{cases}$$

Тогда $\tilde{f} \in \mathcal{F}_N^{n'}$, и к $\tilde{f}$ ней применима лемма 15. Значит существуют линейные операторы $l_i : \{0,1\}^{2k+t} \to \{0,1\}^{2k}$ и функции $f^1, ..., f^s \in \mathcal{F}_N^{2k+t}$ такие, что $\tilde{f}' = z\tilde{f}$ можно вычислить алгоритмом, описанным в условии леммы 15.

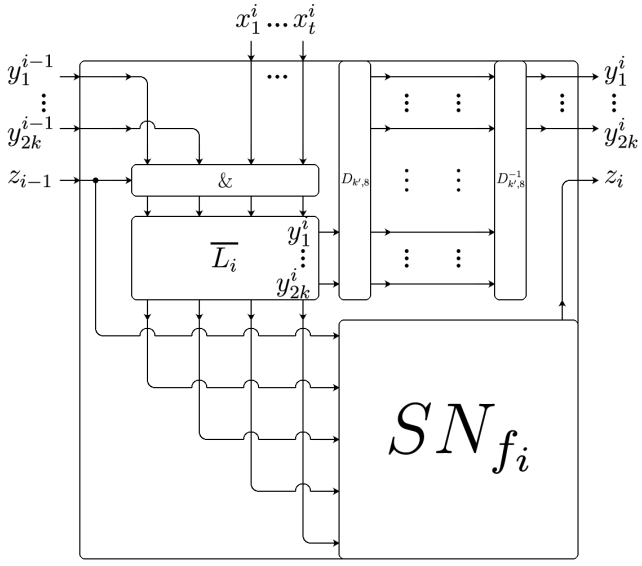


Рис. 9. Блок B_f^i, реализующий функции f^i и l_i.

Несложно убедиться в том, что блок B_f^i, изображённый на рисунке 9, реализует шаг 2 алгоритма из леммы 15 и вычисляет y^i и $z_i f^i$ через

y^{i-1}, x^i и z_{i-1}. Блок $\overline{L_i}$ на выходах $y_1^i, ..., y_{2k}^i$ реализует линейный оператор l_i, снизу реализует тождественные функции от входов. Единственным дополнительным элементом в этой схеме является пара блоков $D_{k',8}$ и $D_{k',8}^{-1}$, $k' = \lceil k/4 \rceil$, вычисляющих взаимно обратные операторы. Эти блоки позволяют уменьшить потенциал проводов, через которые идёт сигнал от выхода блока L_i i-го сегмента схемы (B_f^i) к $(i+1)$-му сегменту схемы (B_f^{i+1}).

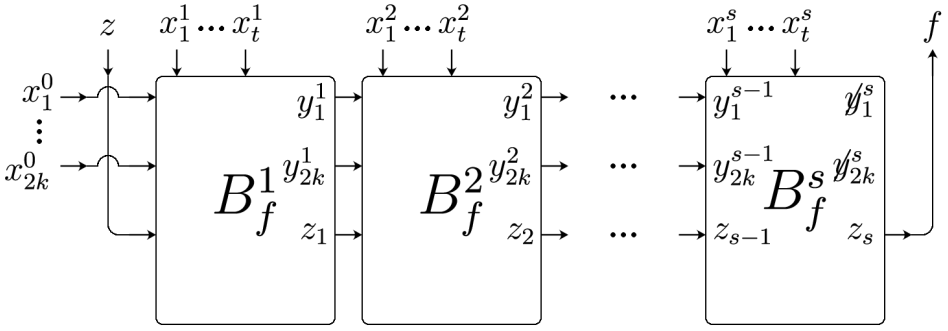


Рис. 10. Схема $SL_{\tilde{f}}^s$, реализующая функцию $\tilde{f}'$.

Сама функция $\tilde{f}'$ реализуется схемой $SL_{\tilde{f}}^s$, изображённой на рисунке 10. В соответствии с шагом 1 алгоритма, на входы $y_1^0, ..., y_{2k}^0$ блока B_f^1 подаётся вектор $x^0 = (x_1^0, ..., x_{2k}^0)$, а на вход z_0 подаётся z. В соответствии с шагом 3, выходом схемы $SL_{\tilde{f}}^s$ является z_s. Ненужные выходы $y_1^s, ..., y_2^s$ блока B_f^s удалены, поскольку не используются. Таким образом, схема SL_f^s реализует функцию $\tilde{f}'$.

Оценка параметров блока B_f^i.

$$\begin{aligned} l(B_i) &= 1 + l(\overline{L_i}) + \max\left(l(SN_{f^i}), l(D_{k',8}^{\top}) + l({D_{k',8}^{-1}}^{\top}) + 1\right) = \\ &= O\left(2k + t + \max\left(\sqrt{N(2k+t)}, {k'}^2\right)\right) = \\ &= O(\max(\sqrt{Nt}, k^2)) = O(\sqrt{Nt}), \\ h(B_i) &= \max\left(2k + 1 + h(\overline{L_i}), h(D_{k',8}^{\top})\right) + h(SN_{f^i}) = \\ &= O(\max(k, 2^{k'})) + O(\sqrt{(2k+t)N}) = O(\sqrt{Nt}). \end{aligned}$$

Потенциал блока B_f^i.

1) Часть схемы, включающая в себя провода от входов, блок $\overline{L}_i$ и провода, идущие от блока L_i имеет длину $O(2k+t) = O(t)$ и ширину $h(D^{\top}_{k',8}) + O(2k+t) = O(2^{k'}+t)$. Потенциал этой части не превосходит её площади, то есть $O(t(2^{k'}+t)) = O(t^2 + \sqrt[4]{N}t)$.

2) Блоки $D_{k',8}$, $D^{-1}_{k',8}$ и соединяющие их провода. $\widehat{U}(D_{k',8}) \le S(D_{k',8}) = O(k'^2 2^{k'})$, $\widehat{U}(D^{-1}_{k',8}) \le S(D^{-1}_{k',8}) = O(k'^2 2^{k'})$. Поскольку на любом наборе активны не более 8 проводов, выходящих из блока $D_{k',8}$, а их длина равна $O(l(SN_{f^i})) = O(\sqrt{Nt})$. В сумме потенциал получается

$$O(k'^2 2^{k'} + \sqrt{Nt}) = O(k^2 \sqrt[4]{N} + \sqrt{Nt}) = O(\sqrt{Nt}).$$

3) Потенциал блока SN_{f^i} по лемме 16 равен

$$O\left(\frac{(2k+t)\sqrt{(2k+t)N}}{\log\max(2, N/(2k+t)}\right) = O\left(\frac{t\sqrt{Nt}}{\log\max(2, N/t)}\right).$$

Заметим, что поскольку $t \ge k \sim \log_2 N$, то $\frac{t}{\log\max(2,N/t)} = \Omega\left(\frac{t}{\log N}\right) = \Omega(1)$, значит $\sqrt{Nt} = O\left(\frac{t\sqrt{Nt}}{\log\max(2,N/t)}\right)$. Также, учитывая, что $t = O(N)$, получим

$$t^2 = \frac{t\sqrt{tN}}{\sqrt{N/t}} = O\left(\frac{t\sqrt{tN}}{\max(1, \log(N/t)}\right) = O\left(\frac{t\sqrt{tN}}{\log\max(2, N/t)}\right). \qquad (40)$$

Таким образом,

$$\widehat{U}(B^i_f) = O(t^2 + \sqrt[4]{N}t) + O(\sqrt{Nt}) + O\left(\frac{t\sqrt{tN}}{\log\max(2, N/t)}\right) = \\ = O\left(\frac{t\sqrt{tN}}{\log\max(2, N/t)}\right).$$

Оценка параметров схемы $SL^s_{\tilde{f}}$. Используя оценки параметров блоков B^i_f, сразу получаются оценки для всей схемы $SL^s_{\tilde{f}}$.

$$\begin{aligned}
l(SL^s_{\tilde{f}}) &= 2 + \sum_{i=1}^{s} l(B^i_f) = O(s\sqrt{Nt}) = \\
&= O(\sqrt{s}\sqrt{Nn}) = O(\sqrt{\max(1, h^2/R)}\sqrt{R}) = \\
&= O(\sqrt{\max(R, h^2)}) = O(\max(h, \sqrt{R})), \\
h(SL^s_{\tilde{f}}) &= \max_{i=1,\ldots,s} h(B^i_f) = O(\sqrt{Nt}) = O\left(\frac{\sqrt{Nn}}{\sqrt{s}}\right) = \\
&= O\left(\frac{R}{\sqrt{s}\sqrt{R}}\right) = O\left(\frac{R}{\max(h, \sqrt{R})}\right), \\
\widehat{U}(SL^s_{\tilde{f}}) &\le O(h(SL^s_{\tilde{F}})) + \sum_{i=1}^{s} \widehat{U}(B^i_f) = O(\sqrt{Nt}) + O\left(s\frac{t\sqrt{tN}}{\log\max(2, N/t)}\right) = \\
&= O\left(\frac{st\sqrt{tN}}{\log\max(2, N/t)}\right) = O\left(\frac{nR}{\max(h, \sqrt{R})\log\max(2, Ns/n)}\right).
\end{aligned}$$

Остаётся заметить, что

$$\begin{aligned}
Ns/n &= \Theta\left(\frac{N\max(1, h^2/R)}{n}\right) = \\
&= \Theta\left(\frac{\max(N, Nh^2/Nn)}{n}\right) = \Theta\left(\max\left(\frac{N}{n}, \frac{h^2}{n^2}\right)\right).
\end{aligned}$$

Значит

$$\log\max(1, Ns/n) = \Theta\left(\log\max\left(2, \frac{N}{n}, \frac{h^2}{n^2}\right)\right) = \Theta\left(\log\frac{\max(2n, N, h)}{n}\right).$$

Отсюда получаем требуемую оценку

$$\widehat{U}(SL^s_{\tilde{f}}) = O\left(\frac{nR}{\max(h, \sqrt{R})\log\frac{\max(2n,h,N)}{n}}\right) = O(u_0(h, N, 2^n)).$$

Теперь, чтобы вычислить функцию f, достаточно подать 0 на входы $x^s_{t'+1}, \ldots, x^s_t$ и 1 на вход z.

Чтобы получить требуемый средний потенциал, определим функцию

$$g(x_1, \ldots, x_{3k-1}) = \begin{cases} 1 & \text{если } \exists \alpha_{3k}, \ldots, \alpha_n : f(x_1, \ldots, x_{3k-1}, \alpha_{3k}, \ldots, \alpha_n) = 1, \\ 0, & \text{иначе.} \end{cases}$$

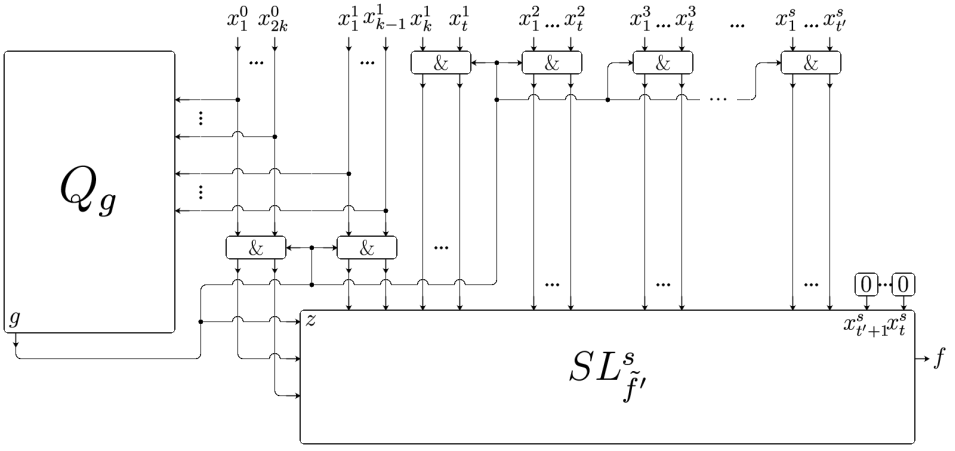


Рис. 11. Схема SF_f^h, реализующая функцию f'.

и построим схему SF_f^h, как показано на рисунке 11. Заметим, что $g \in \mathcal{F}_N^{3k-1}$, поэтому по лемме 14 существует схема Q_g, реализующая функцию g такая, что

$$\begin{aligned} l(Q_g) &= O(\sqrt{N(3k-1-\log_2 N)}) = O(\sqrt{Nk}), \\ h(Q_g) &= O(\sqrt{N(3k-1-\log_2 N)}) = O(\sqrt{Nk}), \\ U(Q_g) &= O(\sqrt{N}). \end{aligned}$$

Схема SF_f^h реализует функцию

$$\begin{aligned} F(x_1^0, ..., x_{2k}^0, x_1^1, ..., x_t^1, ..., x_1^s, ..., x_{t'}^s) = \\ = \tilde{f}'(g, gx_1^0, ..., gx_{2k}^0, gx_1^1, ..., gx_t^1, ..., gx_1^s, ..., gx_{t'}^s, 0, ..., 0) = \\ = g\tilde{f}(gx_1^0, ..., gx_{2k}^0, gx_1^1, ..., gx_t^1, ..., gx_1^s, ..., gx_{t'}^s, 0, ..., 0) = \\ = gf(x_1^0, ..., x_{2k}^0, x_1^1, ..., x_t^1, ..., x_1^s, ..., x_{t'}^s). \end{aligned}$$

Здесь $g = g(x_1^0, ..., x_{2k}^0, x_1^1, ..., x_{k-1}^1)$. Рассмотрим 2 случая.

1) Если $f(x_1^0, ..., x_{t'}^s) = 1$, то $g = 1$, значит и $F = 1 = f$.

2) Если $f(x_1^0, ..., x_{t'}^s) = 0$, то $F = gf = 0 = f$.

Итак, схема SF_f^h реализует функцию f. Оценим её параметры.

$$\begin{aligned} l(SF_f^h) &= l(Q_g) + l(SL^s_{\tilde{f}'}) + 2k + 1 = \\ &= O(\sqrt{Nk}) + O\left(\max(h, \sqrt{R})\right) = O\left(\max(h, \sqrt{R})\right). \\ h(SF_f^h) &\le h(Q_g) + h(SL^s_{\tilde{f}'}) = O(\sqrt{Nk}) + O(\sqrt{Nt}) = \\ &= O(\sqrt{Nt}) = O\left(\frac{R}{\max(h, \sqrt{R})}\right). \end{aligned}$$

Потенциал схемы SF_f^h складывается из потенциала блоков Q_g, $SL^s_{\tilde{f}'}$, потенциала проводов и блоков конъюнкций. Оценим суммарную длину проводов. Провод, идущий от блока Q_f и его ответвления имеют суммарную длину $O(h(Q_f) + l(SF_f^h)) = O(\max(h, \sqrt{R}))$. Остальные провода вместе с блоками конъюнкций заминают площадь $O(n(2k + t))$, и их потенциал тоже не превосходит $O(n(2k + t)) = O(nt)$. В сумме имеем

$$\begin{aligned} \widehat{U}(SF_f^h) &\le \widehat{U}(Q_g) + \widehat{U}(SL^s_{\tilde{f}'}) + O(nt) + O(\max(h, \sqrt{R})) = \\ &= O(\sqrt{kN} + u_0(h, N, 2^n) + nt + \max(h, \sqrt{R})) = \\ &= O(u_0(h, N, 2^n) + nt). \end{aligned}$$

Покажем, что $nt = O(u_0(h, N, 2^n))$. Используя оценку (40), получим

$$\begin{aligned} nt = t^2\frac{n}{t} &= O\left(\frac{n}{t} \cdot \frac{t\sqrt{tN}}{\log \max(2, N/t)}\right) = \\ &= O\left(\frac{n\sqrt{tN}}{\log \max(2, N/t)}\right) = O(u_0(h, N, 2^n)). \end{aligned}$$

Осталось оценить средний потенциал. Отметим, что часть схемы, которая отделена от входов блоками конъюнкций, может быть активна только в случае, когда $g = 1$. Поскольку все входные наборы равновероятны, то и все значения на первых $3k - 1$ входах тоже равновероятны. Поскольку $g \in \mathcal{F}_N^{3k-1}$, то

$$P\{g = 1\} \le \frac{N}{2^{3k-1}} = O\left(\frac{N}{N^3}\right) = O\left(\frac{1}{N^2}\right).$$

Средний потенциал проводов, идущих к блоку Q_g и блокам конъюнкций не превосходит $O(k^2 + n)$. Сами блоки конъюнкций тоже имеют площадь

и потенциал $O(n)$, поскольку каждому входу соответствует одна конъюнкция.

Таким образом,

$$U(SF_f^h) \le U(Q_g) + O(k^2+n) + P\{g=1\}\,\widehat{U}(SL_f^h) = \\ = O(\sqrt{N} + n + \log_2^2 N + u_0(h,N,2^n)/N^2).$$

Заметим, что

$$u_0(h,N,2^n) \le \frac{nR}{\max(h,\sqrt{R}} \le R \le nN,$$

поэтому $u_0(h,N,2^n)/N^2 \le n/N$, значит

$$U(SF_f^h) \le O(\sqrt{N} + n + \log_2^2 N + n/N) = O(\sqrt{N}+n) = O(\max(\sqrt{N}, n)).$$

Проверим, что $SF_f^h \in Q_{\le C_1 h}$. Все входы расположены на верхней стороне, а длина схемы составляет $O(\max(h,\sqrt{R}))$. Рассмотрим 2 случая.

1) $h > \sqrt{R}$. Тогда $T_{in}(SF_f^h) = O(\max(h,\sqrt{R})) = O(h)$.

2) $h \le \sqrt{R}$. Тогда $s = \max(1, \lfloor h^2/3R \rfloor) = 1$, значит есть только входы $x_1^0, ..., x_{2k}^0, x_1^1, ..., x_t^1$, которые расположены рядом. В этом случае $T_{in}(SF_f^h) = O(n) = O(h)$.

Итак, в обоих случаях $T_{in}(SF_f^h) = O(h)$, значит $SF_f^h \in Q_{\le C_1 h}$ для некоторой константы C_1. Лемма доказана. □

Замечание. Ограничение $T_{in}(K) \ge l$ преодолевается путём отдаления самого крайнего входа от остальных на расстояние $l - T_{in}(K)$. При этом потенциал новой схемы K' меняется не более, чем на l, то есть

$$\widehat{U}(K') \le \widehat{U}(K) + l = O(\max(\widehat{U}(K), l).$$

Теперь докажем верхнюю оценку в теореме 2.

Доказательство верхней оценки теоремы 2. Рассмотрим 2 случая.

1) $h \ge h_1(N,n)$. В этом случае $Q_{\le h_1(N,n)} \subseteq Q_{\le h}$, поэтому для любой функции $f \in \mathcal{F}_N^n$ по лемме 17 существует схема $K \in Q_{\le h_1(N,n)}$ такая, что

$$\widehat{U}(K) = O(u_0(h_1(N,n), N, 2^n)) = O(h_1(N,n)).$$

Если $l > h_1(N,n)$, то, согласно замечанию, существует схема $K' \in Q_{[l,h]}$ такая, что

$$\widehat{U}(K') = O(\max(l, \widehat{U}(K))) = O(\max(l, h_1(N,n))) = O(u_1(l,h,N,n)).$$

2) $h \leq h_1(N,n)$. Здесь, опять же, по лемме 17 существует схема $K \in Q_{\leq h_1(N,n)}$ такая, что

$$\widehat{U}(K) = O(u_0(h_1(N,n), N, 2^n)) = O(u_0(h, N, 2^n)).$$

Согласно замечанию, существует схема $K' \in Q_{[l,h]}$ такая, что

$$\begin{aligned}\widehat{U}(K') &= O(\max(l, \widehat{U}(K))) = \\ &= O(\max(l, u_0(h, N, 2^n))) = O(u_1(l, h, N, n)).\end{aligned}$$

Верхняя оценка доказана. □

Список литературы

[1] Алешин С.В. Полугруппы и группы автоматов // Интеллектуальные системы. — 2013. — Т. 17, вып. 1–4. — С. 129–141.

[2] Александров Д.Е. Эффективные методы реализации проверки содержания сетевых пакетов регулярными выражениями // Интеллектуальные системы. — 2014. — Т. 18, вып. 1. — С. 37–60.

[3] Титова Е.Е. Конструирование движущихся изображений клеточными автоматами // Интеллектуальные системы. — 2014. — Т. 18, вып. 1. — С. 153–180.

[4] Бабин Д.Н. Частотные регулярные языки // Интеллектуальные системы. — 2014. — Т. 18, вып. 1. — С. 205–210.

[5] Иванов И.Е. О некоторых свойствах автоматов с магазинной памятью // Интеллектуальные системы. — 2014. — Т. 18, вып. 1. — С. 243–252.

[6] В.Б.Кудрявцев. Кафедра математической теории интеллектуальных систем (МаТИС) // Интеллектуальные системы. — 2014. — Т. 18, вып. 2. — С. 5–30.

[7] Часовских А.А. Условия полноты линейно-p-автоматных функций // Интеллектуальные системы. — 2014. — Т. 18, вып. 3. — С. 203–252.

[8] Александров Д.Е. Об оценках автоматной сложности распознавания классов регулярных языков // Интеллектуальные системы. — 2014. — Т. 18, вып. 4. — С. 161–190.

[9] Дементьев В.М. О звездной высоте регулярного языка и цикличе-ской сложности минимального автомата // Интеллектуальные системы. — 2014. — Т. 18, вып. 4. — С. 215–222.

[10] Кучеренко И.В. О минимизации монофункциональных классов бинарных клеточных автоматов с неразрешимым свойством обратимости. — 2014. — Т. 18, вып. 4. — С. 227–295.

[11] Якимец К.К. Об инвариантности характеристик конфигураций однородных структур. — 2014. — Т. 18, вып. 4. — С. 347–356.

[12] Иванов И.Е. О сохранении периодических последовательностей автоматами с магазинной памятью с однобуквенным магазином // Интеллектуальные системы. — 2015. — Т. 19, вып. 1. — С. 145–160.

[13] Летуновский А.А. Выразимость линейных автоматов относительно расширенной суперпозиции // Интеллектуальные системы. — 2015. — Т. 19, вып. 1. — С. 161–170.

[14] Гербус В.Г. О связи функций автомата и автоматной функции // Интеллектуальные системы. — 2015. — Т. 19, вып. 2. — С. 109–116.

[15] Миронов А.М. Критерий реализуемости функций на строках вероятностными автоматами Мура с числовым выходом // Интеллектуальные системы. — 2015. — Т. 19, вып. 2. — С. 149–160.

[16] Терехина И.Ю. Модель невлияния для квантовых автоматов // Интеллектуальные системы. — 2015. — Т. 19, вып. 2. — С. 183–190.

[17] Бабин Д.Н., Летуновский А.А. О возможностях суперпозиции, при наличии в базисе автоматов фиксированной добавки из булевых функций и задержки // Интеллектуальные системы. — 2015. — Т. 19, вып. 3. — С. 71–78.

[18] Бабин Д.Н. Автоматы с суперпозициями, пример нерасширяемости до предполного класса // Интеллектуальные системы. — 2015. — Т. 19, вып. 3. — С. 87–94.

[19] Э.Э.Гасанов, А.А.Мастихина Прогнозирование общерегулярных сверхсобытий автоматами // Интеллектуальные системы. — 2015. — Т. 19, вып. 3. — С. 127–154.

[20] Иванов И.Е. Нижняя оценка на максимальную длину периода выходной последовательности автономного автомата с магазинной памятью // Интеллектуальные системы. — 2015. — Т. 19, вып. 3. — С. 175–194.

[21] А.А.Часовских. Критериальные системы в классах линейно-автоматных функций над конечными полями // Интеллектуальные системы. — 2015. — Т. 19, вып. 3. — С. 195–207.

[22] Кравцов С.С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов. // Проблемы кибернетики. Вып. 19. М.: Наука, 1967. С. 285–293.

[23] Гасанов Э.Э., Ефремов Д.В. Фоновый алгоритм решения двумерной задачи о доминировании // Интеллектуальные системы. — 2014. — Т. 18, вып. 3. — С. 133–158.

[24] Е. М. Перпер. Нижние оценки временной и объёмной сложности задачи поиска подслова // Дискретная математика, 2014, том 26:2, 58–70.

[25] Шуткин Ю.С. Моделирование схемных управляющих систем // Интеллектуальные системы. — 2014. — Т. 18, вып. 3. — С. 253–261.

[26] Перпер Е.М. Порядок сложности задачи поиска в множестве слов вхождений подслова // Интеллектуальные системы. — 2014. — Т. 19, вып. 1. — С. 99–116.

[27] Плетнев А.А. Информационно-графовая модель динамических баз данных и ее применение// Интеллектуальные системы. — 2014. Т. 18, Вып. 1. — С. 111-140.

[28] Плетнев А.А. Динамическая база данных, допускающая параллельную обработку произвольных потоков запросов// Интеллектуальные системы. — 2015. Т. 19, Вып. 1. — С. 117–145.

[29] Плетнев А.А. Логарифмическая по сложности параллельная обработка автоматами произвольных потоков запросов в динамической

базе данных// Интеллектуальные системы. — 2015. Т. 19, Вып. 1. — С. 171–213.

[30] Черемисин О. В. Об активности схем из клеточных элементов, реализующих систему всех конъюнкций // Дискретная математика. — 2003. — Т. 15, вып. 2. — С. 113—122

[31] Касим-Заде О. М. О влиянии базиса на мощность схем из функциональных элементов. - Москва : ИПМ, 1979. - 28 с. : схем.; 21 см. - (Препринт / Ин-т прикл. математики им. М.В. Келдыша АН СССР; №122).

[32] Калачев Г. В. Порядок мощности плоских схем, реализующих булевы функции // Дискретная математика. — 2014. — Т. 26, № 1. — С. 49–74.

[33] Калачев Г. В. Нижние оценки мощности плоских схем, реализующих частичные булевы операторы // Интеллектуальные системы. Теория и приложения. — 2014. — Т. 18, № 2. — С. 279–322.

[34] Калачев Г. В. Об одновременной минимизации площади, мощности и глубины плоских схем, реализующих частичные булевы операторы // Интеллектуальные системы. Теория и приложения. — 2016. — Т. 20, № 2. — С. 203–266.

[35] Чашкин А.В. Лекции по дискретной математике // М.: МГУ Мехмат, 2007.

[36] Жуков Д.А. О вычислении частичных булевых функций клеточными схемами. // Дискретный анализ и исследование операций. Апрель – июнь 2004. Серия 1. Том 11, №2, С. 32 – 40