

Оценки мощности плоских схем, реализующих монотонные функции.

Калачев Г.В.

В работе доказаны универсальные нижние оценки функции Шеннона мощности плоских схем, а также найден порядок роста функции Шеннона мощности схем, реализующих монотонные функции. В качестве меры мощности рассматривается максимальный потенциал, он равен максимальному количеству выходов элементов, выдающих единицу на заданном входном наборе схемы, где максимум берётся по всем входным наборам. В работе показано, что порядок роста функции Шеннона максимального потенциала для монотонных функций равен $2^{n/2}/\sqrt[4]{n}$, а порядок среднего потенциала равен $2^{n/2}/\sqrt[4]{n^3}$.

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

1. Введение.

В данной работе исследуется сложность реализации монотонных булевых функций плоскими схемами. Плоская схема является моделью чипа с учётом его укладки на плоскость. Обычно в качестве модели, описывающей работу чипа, используют структурные автоматы. Структурный автомат моделирует логическую структуру чипа. По теории автоматов имеется множество работ, например, [1]-[21]. Однако в модели на основе структурного автомата не отражено размещение логических элементов в кристалле, разводка проводов и энергопотребление.

Основная доля площади и энергопотребления для почти всех автоматов приходится на часть схемы, реализующей функцию перехода автомата. Функция перехода является булевой функцией или операторов.

Поэтому с точки зрения теории сложности основной интерес представляет реализация плоскими схемами булевых функций и операторов.

Плоские схемы (или схемы из клеточных элементов), являются моделью микросхемы, в которой учитывается размещение логических элементов на плоскости и разводку проводов, в ней могут быть определены такие меры сложности, как площадь и мощность (энергопотребление). Впервые плоские схемы были введены Кравцовым С.С. в работе [22].

Плоские схемы – один из типов управляющих. К управляющим системам также относятся автоматы, схемы из функциональных элементов (далее СФЭ), контактные схемы и информационные графы. По теории управляющих систем публикуется множество работ, например, [23]-[29]. В теории управляющих систем часто ставится задача минимизации некоторой меры сложности. Основной мерой сложности плоских схем, СФЭ и контактных схем является число элементов схемы (или контактов), эта величина характеризует площадь чипа. Для плоских схем и СФЭ также важным параметром является мощность (или активность) схемы, она характеризует энергопотребление схемы. Для контактных схем аналогом активности является время моделирования. В отличие от схем, информационные графы моделируют не чипы, а структуры данных и алгоритмы поиска в них. Для информационных графов на первое место часто ставится среднее время ответа на запрос, а второй мерой сложности является число рёбер графа (соответствует памяти для хранения базы данных).

В теории управляющих систем часто исследуется зависимость какой-нибудь меры сложности от базиса. О. М. Касим-Заде в [31] показал, например, что существует базис, в котором одновременная минимизация сложности и мощности невозможна. Для информационных графов такого рода результат был получен Е. М. Перпером в работе [24]. Он показал, что для задачи поиска подстрок существует такое базовое множество, что не существует информационного графа, оптимального одновременно по времени и по памяти.

Однако с точки зрения порядка мощности плоских схем базис не играет такой роли. В работе [32] была введена переключательная мощность и было показано, что она сохраняется с точностью до константы при замене базиса. Также было показано, что при отсутствии ограничений на базис эта мера с точностью до константы совпадает с потенциалом, рассматриваемым в этой работе. Переключательная мощность лучше отражает энергопотребление схемы и совпадает с потенциалом без ограничений на базис, его мы и исследуем в данной работе.

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 работе [30] О. В. Черемисин показал, что в классе прямоугольных схем невозможна одновременная минимизация площади и мощности плоских схем, реализующих систему всех конъюнкций. 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 работах [33] и [34] был получен порядок роста мощности плоских схем, реализующих частичные булевы операторы. В работе [35] найден порядок роста максимального потенциала схем, реализующих функции с малым числом единиц в зависимости от ограничений на расположение входов схемы.

В данной работе получен порядок функции Шеннона потенциала монотонных булевых функций от n переменных. В процессе доказательства основного результата также получены универсальные нижние оценки функции Шеннона для среднего и максимального потенциала для произвольного класса булевых функций.

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

2. Определения и обозначения.

2.1. 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.

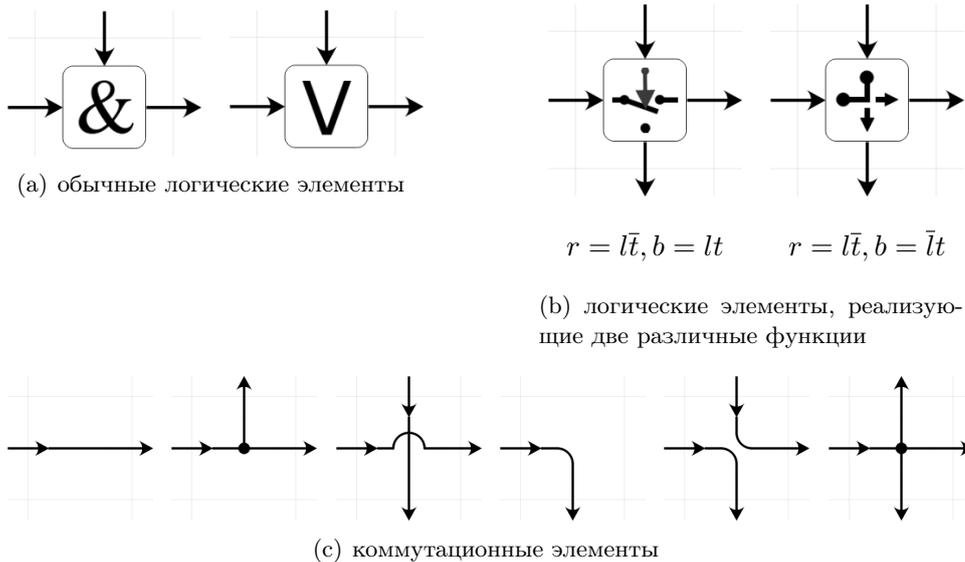


Рис. 1: Примеры клеточных элементов.

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.

Сетью из клеточных элементов на множестве $M \subset \mathbb{Z}^2$ над множеством $E' \subseteq E$ будем называть отображение $K : M \rightarrow E'$, 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 выходом, 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 с носителем M , 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 количество элементов множества M будем называть площадью схемы K и обозначать $S(K)$. 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 .

Минимальную площадь плоской схемы, реализующей оператор F обозначим за $S(F)$.

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. Мы здесь не предполагаем, что схема имеет форму прямоугольника. При доказательстве верхних оценок мы используем прямоугольные схемы, а доказанные нижние оценки верны для схем произвольной формы.

2.2. 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

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

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

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

Пусть $f : \mathcal{D} \rightarrow \{0, 1\}$ — частичная булева функция. Определим средний и максимальный потенциал функции f .

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

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

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

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).

3. Результаты.

Теорема 1. *Для любой булевой функции f , отличной от константы, выполнена оценка*

$$\widehat{U}(f) \geq \frac{\sqrt{S(f)}}{4\sqrt{2}}.$$

Учитывая простую мощностную нижнюю оценку функции Шеннона для площади плоских схем, получим

Следствие 1. *Пусть \mathcal{F} — некоторый класс булевых функций, $\mathcal{F}(n) := \mathcal{F} \cap P_2(n)$. Тогда доля функций $f \in \mathcal{F}(n)$, для которых верна оценка*

$$\widehat{U}(f) \geq C_1 \sqrt{\log |\mathcal{F}(n)| - n \log n},$$

стремится к 1 при $n \rightarrow \infty$. Здесь $C_1 > 0$ — некоторая константа.

Теперь сформулируем универсальную нижнюю оценку для среднего потенциала.

Для булевых функций от n переменных определим

- $|f| := |\{x : f(x) = 1\}|$ — вес булевой функции
- $\text{dist}(f, g) := |f \oplus g|$ — метрика на множестве булевых функций

Пусть \mathcal{F} — класс булевых функций. Обозначим через $\varphi_n(\mathcal{F}, t)$ максимальное количество функций из $\mathcal{F}(n)$, попадающих в шар радиуса 2^nt ,

$$\varphi_n(\mathcal{F}, t) = \max_{f_0 \in P_2(n)} \#\{f \in \mathcal{F}(n) : \text{dist}(f, f_0) \leq 2^nt\}.$$

Теорема 2. *Пусть задан класс функций \mathcal{F} такой, что $n \log n = o(\log |\mathcal{F}(n)|)$ при $n \rightarrow \infty$. Тогда для любой невозрастающей последовательности $\{t_n\}_{n=1}^\infty$, $t_n \in (0, 1]$ доля функций $f \in \mathcal{F}_n$, для которых верна оценка*

$$U(f) \gtrsim t_n \sqrt{\log_2 \frac{|\mathcal{F}_n|}{\varphi_n(\mathcal{F}, t_n)}},$$

стремится к 1 при $n \rightarrow \infty$.

Следующее утверждение можно получить как из предыдущей теоремы, так и из нижней оценки для частичных булевых функций.

Утверждение 1. Если $\mathcal{F}(n)|_{\mathcal{D}_n} = P_2(\mathcal{D}_n)$ для некоторого семейства областей $\mathcal{D}_n \subseteq \{0, 1\}^n$, то при $n \rightarrow \infty$ выполнена оценка

$$U(\mathcal{F}(n)) \asymp \frac{|\mathcal{D}_n|^{3/2}}{2^n}.$$

Теорема 3. Для класса монотонных функций верны следующие оценки.

$$\widehat{U}(M(n)) \asymp \frac{2^{n/2}}{\sqrt[4]{n}},$$

$$U(M(n)) \asymp \frac{2^{n/2}}{n^{3/4}} \text{ при } n \rightarrow \infty.$$

4. Доказательство

4.1. 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 выходных элементов (тех, входы которых являются выходами схемы) не более чем на $r - 1$ по манхэттенской метрике.
- K_r — множество элементов схемы K , лежащие в множестве B_r .

Доказательство теоремы 1. Рассмотрим произвольную функцию $f \in P_2$, отличную от константы и схему K , которая реализует функцию f с наименьшим максимальным потенциалом (из всех схем с одинаковым потенциалом выберем схему с наименьшим количеством узлов).

Тогда в схеме K все входы соответствуют существенным переменным функции f , иначе можно было бы удалить несущественный вход, уменьшив количество узлов схемы и не увеличив максимальный потенциал. Аналогично, каждый узел схемы K зависит существенно от некоторого входа схемы, иначе он равен константе, и его можно удалить, уменьшив число узлов схемы. Здесь существенно, что базис не ограничен, поэтому константный узел можно удалить, изменяя соответствующим образом функцию, реализуемую элементом, для которого этот узел является входом.

Пусть n — количество входов схемы K . Рассмотрим выход схемы α и самый дальний от него узел схемы β , а также вход γ , от которого β существенно зависит. Без ограничения общности будем считать, что на вход β подаётся первая переменная функции. Поскольку α и γ существенно зависят от β , то существуют наборы $a, b \in \{0, 1\}^{n-1}$ такие, что $\varphi_\alpha(0, a) = f(0, a) \neq f(1, a) = \varphi_\alpha(1, a)$, $\varphi_\gamma(0, a) \neq \varphi_\gamma(1, a)$.

Поскольку у наборов $(0, a)$ и $(1, a)$ различается только первая компонента (вход β), а значения в узле α различны, то существует цепочка узлов $[\beta = t_0, t_2, \dots, t_l = \alpha]$ такая, что $\varphi_{t_i}(0, a) \neq \varphi_{t_i}(1, a)$ для всех $i = 0, \dots, l$. Причём $t_i \neq t_j$ при $i \neq j$ и для каждого $i = 0, \dots, l - 1$ узлы t_i и t_{i+1} — соответственно вход и выход некоторого элемента. l не может быть меньше расстояния $\rho_K(\alpha, \beta)$. Это означает, что

$$u_K(0, a) + u_K(1, a) \geq \sum_{i=0}^l (\varphi_{t_i}(0, a) + \varphi_{t_i}(1, a)) = l + 1 \geq \rho_K(\beta, \alpha) + 1.$$

Аналогично получим, что

$$u_K(0, b) + u_K(1, b) \geq \rho_K(\beta, \gamma) + 1.$$

Тогда по неравенству треугольника

$$\begin{aligned} u_K(0, a) + u_K(1, a) + u_K(0, b) + u_K(1, b) &\geq \\ &\geq \rho_K(\beta, \alpha) + \rho_K(\beta, \gamma) + 2 \geq \rho_K(\alpha, \gamma) + 2. \end{aligned}$$

Поскольку круг радиуса r по манхеттенской метрике имеет площадь $< 2(r+1)^2$, а γ — самый дальний узел от α , то вся схема помещается в круг с центром в клетке снаружи схемы, на границе которой находится выход α , радиуса $r := \rho_K(\alpha, \gamma)$. Отсюда $2(r+1)^2 > s \geq S(f)$,

$$\rho_K(\alpha, \gamma) > \frac{\sqrt{s}}{2} - 1 \geq \frac{\sqrt{S(f)}}{2} - 1.$$

Отсюда получаем требуемую оценку

$$\begin{aligned} \widehat{U}(f) = \widehat{U}(K) &\geq \max(u_K(0, a), u_K(1, a), u_K(0, b), u_K(1, b)) \geq \\ &\geq \frac{u_K(0, a) + u_K(1, a) + u_K(0, b) + u_K(1, b)}{4} \geq \\ &\geq \frac{\rho_K(\alpha, \gamma) + 2}{4} > \frac{\sqrt{S(f)/2}}{4} = \frac{\sqrt{S(f)}}{4\sqrt{2}}. \end{aligned}$$

Теорема доказана. □

Доказательство теоремы 2. Каждой функции $f \in \mathcal{F}$ сопоставим некоторую схему K^f , реализующую f с наименьшим средним потенциалом. Введём множество $L(r, n, t) \subseteq \mathcal{F}(n)$ — множество функций, для которых значения на разрезе $(K_r^f | K^f)$ отличны от 0 на области \mathcal{D}_r^f состоящей из не более, чем $R := t \cdot 2^n$ наборов. Для каждой такой функции определим функцию f'_r , которая реализуется схемой $K_r^{f'}$, которая получена из K_r^f заменой всех входов $In(K_r^f | K^f)$ на 0 и удалением всех выходов $Out(K_r^f | K^f)$. По построению, на всех $x \in \{0, 1\}^n \setminus \mathcal{D}_r^f$ $f'_r(x) = f(x)$, поскольку схема $K_r^{f'}$ и подсхема K_r^f схемы K^f на этих наборах функционируют одинаково. Это означает, что $\text{dist}(f, f'_r) \leq |\mathcal{D}_r^f| \leq R$.

Оценим мощность множества $l(r, n, t)$. Каждая $f \in l(r, n, t)$ лежит в шаре радиуса R с центром в некоторой функции f'_r , которая реализуется схемой $K_r^{f'}$. Схема $K_r^{f'}$ помещающейся в круг радиуса r , откуда $S(f'_r) \leq S(K_r^{f'}) = O(r^2)$.

- 1) Существует не более $A^{O(r^2)}$ схем площади $O(r^2)$, где $A > 0$ — некоторая константа.
- 2) Каждая схема определяет функцию с точностью до перестановки переменных. Таким образом, каждой схеме соответствует не более $n!$ различных функций.
- 3) По определению функции φ_n , существует не более $\varphi_n(\mathcal{F}, t)$ функций из \mathcal{F} , которые могут попасть в шар радиуса $t \cdot 2^n$.

Итак,

$$|l(r, n, t)| \leq A^{O(r^2)} n! \varphi_n(\mathcal{F}, t).$$

Введём множество $L(r, n, t) := \bigcup_{i=1}^r l(i, n, t)$. Тогда

$$|L(r, n, t)| \leq r A^{O(r^2)} n! \varphi_n(\mathcal{F}, t) \leq B^{r^2} n! \varphi_n(\mathcal{F}, t),$$

где $B > 0$ — некоторая константа. Тогда при $r = \sqrt{\frac{1}{2 \log_2 B} \log_2 \frac{|\mathcal{F}_n|}{\varphi_n(\mathcal{F}, t)}}$ имеем

$$\begin{aligned} \log_2 |L(r, n, t)| &< \log_2 r + n \log_2 n + \frac{1}{2} \log_2 \frac{|\mathcal{F}_n|}{\varphi_n(\mathcal{F}, t)} + \log_2 \varphi_n(\mathcal{F}, t) = \\ &= \log_2 r + n \log_2 n + \log_2 |\mathcal{F}_n| - r \sqrt{\frac{\log_2 B}{2}} \leq \\ &\leq \log_2 |\mathcal{F}_n| - Cr \text{ при достаточно большом } n. \end{aligned}$$

Здесь C — некоторая константа. Теперь заметим, что для всех $f \in \mathcal{F}_n \setminus L(r, n, t)$ для всех $i = 1, \dots, r$ на разрезе $(K_i^f | K^f)$ есть хотя бы один ненулевой узел более, чем на R наборах, значит $U(K_i^f | K^f) > R/2^n = t$. Отсюда

$$U(f) = U(K^f) \geq \sum_{i=1}^r U(K_i^f | K^f) \geq rt = C_1 t \sqrt{\log_2 \frac{|\mathcal{F}_n|}{\varphi_n(\mathcal{F}, t)}}.$$

Осталось показать, что доля функций $f \in L(r, n, t)$ в классе \mathcal{F}_n стремится к 0.

$$\frac{|L(r, n, t)|}{|\mathcal{F}_n|} = \frac{2^{\log_2 |\mathcal{F}_n| - Cr}}{|\mathcal{F}_n|} = 2^{-Cr} \rightarrow 0 \text{ при } n \rightarrow \infty,$$

поскольку $r = \Omega(\log_2 \frac{|\mathcal{F}_n|}{\varphi_n(\mathcal{F}, t)}) = \omega(n \log n) \rightarrow \infty$ при $n \rightarrow \infty$. Теорема доказана. \square

Доказательство утверждения 1. Сразу отметим, что в случае $|\mathcal{D}_n|^{3/2} < 2^n$ утверждение очевидно и несодержательно, поэтому далее рассматриваем случай $|\mathcal{D}_n|^{3/2} \geq 2^n$.

По теореме [33, Теорема 1], при достаточно большом n существует $f \in P_2(\mathcal{D}_n)$ такая, что $U_{\mathcal{D}_n}(f) \geq C_1 \sqrt{|\mathcal{D}_n|}$, где $C_2 > 0$ — некоторая константа. Поскольку $P_2(\mathcal{D}_n) = \mathcal{F}(n)|_{\mathcal{D}_n}$, то существует функция $f' \in \mathcal{F}$ такая, что $f'|_{\mathcal{D}_n} = f$. Это означает, что

$$C_1 \sqrt{|\mathcal{D}_n|} \leq U_{\mathcal{D}_n}(f) \leq U_{\mathcal{D}_n}(f') \leq \frac{2^n}{|\mathcal{D}_n|} U(f') \leq \frac{2^n}{|\mathcal{D}_n|} U(\mathcal{F}(n)).$$

Отсюда сразу следует требуемая оценка. Утверждение доказано. \square

Доказательство нижней оценки в теореме 3.

Положим $\mathcal{D}_n = \{x \in \{0, 1\}^n : |x| = \lfloor n/2 \rfloor\}$ — множество наборов, находящихся на среднем слое булева куба. Рассмотрим подкласс монотонных функций $M'(n) \subseteq M(n)$, все нижние единицы и верхние нули которых расположены в множестве \mathcal{D}_n . Такие функции полностью задаются своими значениями на \mathcal{D}_n , поэтому $|M'(n)| = C_n^{\lfloor n/2 \rfloor}$. Применяя следствие 1 получим

$$\begin{aligned} \widehat{U}(M(n)) &\geq \widehat{U}(M'(n)) \geq C_1 \sqrt{\log C_n^{\lfloor n/2 \rfloor} - n \log n} = \\ &= \Omega \left(\sqrt{\frac{2^n}{\sqrt{n}}} \right) = \Omega \left(\frac{2^{n/2}}{\sqrt[4]{n}} \right). \end{aligned}$$

Для оценки среднего потенциала воспользуемся утверждением 1. Поскольку все наборы в множестве \mathcal{D}_n несравнимы, то значения монотонной функции на них можно задать произвольно, значит $M'(n)|_{\mathcal{D}_n} = P_2(\mathcal{D}_n)$. Из утверждения 1 получим

$$U(M(n)) \gtrsim C_1 \frac{|\mathcal{D}_n|^{3/2}}{2^n} \asymp \frac{(2^n/\sqrt{n})^{3/2}}{2^n} = \frac{2^{n/2}}{n^{3/4}}.$$

Нижние оценки доказаны. \square

4.2. Реализация монотонных функций.

Как и в предыдущих работах [34] и [35], будем использовать базис $\{\vee, \&, \oplus, 1\}$.

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, повернутых на 90° , 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 $x^\alpha := x \oplus \bar{\alpha}$.
- Если $x = (x_1, \dots, x_k)$ и $\alpha = (\alpha_1, \dots, \alpha_k)$ – 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 $i \equiv \bar{i}_1^{(k)} + 2\bar{i}_2^{(k)} + \dots + 2^{k-1}\bar{i}_k^{(k)} \pmod{2^k}$. j -ю цифру числа i будем обозначать просто \bar{i}_j без верхнего индекса.
- Если $x = (x_1, \dots, x_k)$ – булев вектор, i – неотрицательное целое число, то $x^{\bar{i}} := x^{\bar{i}^{(k)}}$.

Мы будем использовать метод декомпозиции монотонных булевых функций, который использовался в [36, Теорема 10.9] при построении схемы из функциональных элементов для монотонных функций. Нам потребуется аналоги лемм [36, Леммы 10.13-10.15]. Для доказательства нам понадобится несколько определений из [36]. При доказательстве этих лемм будем полагать, что n – чётное.

Пара вершин n -мерного булева куба называется ребром, если эти вершины различаются ровно в одном разряде. Пусть f – монотонная булева функция. Ребро (x, y) называется непостоянным, если $f(x) \neq f(y)$. Будем говорить, что ребро (x, y) проходит в i -м направлении, если наборы x и y различаются в i -м разряде.

Лемма 1 ([36], Лемма 10.12). *У любой n -местной монотонной булевой функции число непостоянных рёбер не превосходит $\frac{n}{2}C_n^{n/2}$.*

Лемма 2 (Аналог леммы 10.13, [36]). *Для любой n -местной монотонной булевой функции и любого k , $1 \leq k \leq n$ найдутся такие направления i_1, \dots, i_k , что число непостоянных рёбер, проходящих в этих направлениях, не превосходит $\frac{k}{2}C_n^{n/2}$.*

Доказательство. Пусть r_i — число непостоянных рёбер, проходящих в i -м направлении. Упорядочим все направления по возрастанию r_i . В качестве i_j возьмём j -й элемент в полученной последовательности. Тогда $r_{i_1} \leq r_{i_2} \leq \dots \leq r_{i_n}$. Для доказательства нам нужно показать, что $\sum_{j=1}^k r_{i_j} \leq \frac{k}{2}C_n^{n/2}$.

Среднее значение первых k элементов не больше среднего значения всех элементов последовательности $(r_{i_j})_{j=1}^n$, то есть

$$\frac{1}{k} \sum_{j=1}^k r_{i_j} \leq \frac{1}{n} \sum_{j=1}^n r_{i_j}.$$

По лемме 1 число непостоянных рёбер не больше $\frac{n}{2}C_n^{n/2}$. Отсюда

$$\sum_{j=1}^k r_{i_j} \leq \frac{k}{n} \sum_{j=1}^n r_{i_j} \leq \frac{k}{n} \cdot \frac{n}{2}C_n^{n/2} = \frac{k}{2}C_n^{n/2}.$$

Лемма доказана. □

Символом $f_{i_1 \dots i_k}^{\alpha_1, \dots, \alpha_k}(x)$, $\alpha_i \in \{0, 1\}$ обозначим функцию от $(n - k)$ переменных, получающуюся из функции f от n переменных подстановкой констант $\alpha_1, \dots, \alpha_k$ вместо аргументов с номерами i_1, \dots, i_k . Символом $x_{i_1 \dots i_k}^{\alpha_1, \dots, \alpha_k}$ обозначим набор длины n , у которого разряды с номерами i_1, \dots, i_k равны $\alpha_1, \dots, \alpha_k$ и который после удаления этих разрядов превращается набор x длины $n - k$. Таким образом, выполнено равенство

$$f_{i_1 \dots i_k}^{\alpha_1, \dots, \alpha_k}(x) = f(x_{i_1 \dots i_k}^{\alpha_1, \dots, \alpha_k}).$$

Лемма 3 (Аналог леммы 10.14, [36]). *Для любой n -местной монотонной булевой функции f и числа k , $1 \leq k \leq n$ найдутся такие i_1, \dots, i_k , что $f_{i_1 \dots i_k}^{1 \dots 1}(x) \neq f_{i_1 \dots i_k}^{0 \dots 0}(x)$ не более чем для $\frac{1}{2}C_n^{n/2}$ различных наборов x длины $n - k$.*

Доказательство. По лемме 2 существуют направления $i_1 \dots i_k$, вдоль которых в сумме проходит не более $\frac{k}{2}C_n^{n/2}$ непостоянных рёбер. За X обозначим множество наборов $x \in \{0, 1\}^{n-k}$, для которых $f_{i_1 \dots i_k}^{1 \dots 1}(x) \neq f_{i_1 \dots i_k}^{0 \dots 0}(x)$.

Рассмотрим произвольный $x \in X$. В k -мерном булевом подкубе $x_{i_1 \dots i_k}^y$, $y \in \{0, 1\}^k$, имеется k непересекающихся по рёбрам цепей из вершины $x_{i_1 \dots i_k}^{0 \dots 0}$ в $x_{i_1 \dots i_k}^{1 \dots 1}$. Поскольку

$$f(x_{i_1 \dots i_k}^{0 \dots 0}) = f_{i_1 \dots i_k}^{0 \dots 0}(x) < f_{i_1 \dots i_k}^{1 \dots 1} = f(x_{i_1 \dots i_k}^{1 \dots 1}),$$

то в каждой из цепей из $x_{i_1 \dots i_k}^{0 \dots 0}$ в $x_{i_1 \dots i_k}^{1 \dots 1}$ есть непостоянное ребро. Таким образом, каждому $x \in X$ соответствует не менее k различных непостоянных рёбер. Причём рёбра, соответствующие разным x не могут совпадать.

Это означает, что число непостоянных рёбер по крайней мере в k раз больше, чем число элементов множества X . Отсюда

$$|X| \leq \frac{1}{k} \cdot \frac{k}{2} C_n^{n/2} = \frac{1}{2} C_n^{n/2}.$$

Лемма доказана. \square

Символом $x_{i_1 \dots i_k}$ обозначим набор длины $n - k$, получающийся из набора x длины n удалением разрядов с номерами i_1, \dots, i_k .

Лемма 4 (Аналог леммы 10.15, [36]). *Пусть n делится на 2. Тогда для любой функции $f \in M(n)$ существуют различные номера i_1, \dots, i_k и функции $p, q \in M(n - k)$ такие, что мощность множества*

$$\mathcal{D} = \left\{ x : \overline{p(x_{i_1 \dots i_k})} q(x_{i_1 \dots i_k}) = 1 \right\}$$

не превосходит $2^{k-1} C_n^{n/2}$, и существует частичная функция $f_{\mathcal{D}} : \mathcal{D} \rightarrow \{0, 1\}$ такая, что

$$f(x) = p(x_{i_1 \dots i_k}) \vee \overline{p(x_{i_1 \dots i_k})} q(x_{i_1 \dots i_k}) f_{\mathcal{D}}(x). \quad (1)$$

Доказательство. По лемме 3 существуют номера $i_1 \dots i_k$, что $f_{i_1 \dots i_k}^{1 \dots 1}(x) \neq f_{i_1 \dots i_k}^{0 \dots 0}(x)$ не более чем для $\frac{1}{2} C_n^{n/2}$ различных наборов x длины $n - k$. Положим

$$p = f_{i_1 \dots i_k}^{0 \dots 0}, \quad q = f_{i_1 \dots i_k}^{1 \dots 1}, \quad \mathcal{D} = \left\{ x \mid \overline{p(x_{i_1 \dots i_k})} q(x_{i_1 \dots i_k}) = 1 \right\}, \quad f_{\mathcal{D}} = f|_{\mathcal{D}}.$$

Для каждому набору $x_{i_1 \dots i_k} \in E k^{n-k}$, для которого $\overline{p(x_{i_1 \dots i_k})} q(x_{i_1 \dots i_k}) = 1$, соответствует 2^k наборов из $|\mathcal{D}|$, получающихся из $x_{i_1 \dots i_k}$ произвольным выбором значений переменных x_{i_1}, \dots, x_{i_k} . Значит

$$|\mathcal{D}| \leq 2^k \cdot \frac{1}{2} C_n^{n/2} = 2^{k-1} C_n^{n/2}.$$

Осталось проверить, что для выбранных p , q и $f_{\mathcal{D}}$ выполнено представление (1).

Для произвольного $x \in \{0, 1\}^{n-k}$ имеем

$$p(x_{i_1 \dots i_k}) = f_{i_1 \dots i_k}^{0 \dots 0}(x_{i_1 \dots i_k}) \leq f(x) \leq f_{i_1 \dots i_k}^{1 \dots 1}(x_{i_1 \dots i_k}) = q(x_{i_1 \dots i_k}).$$

Рассмотрим 3 случая.

- 1) Если $p(x_{i_1 \dots i_k}) = 1$, то $f(x) = 1$, таким образом (1) выполнено.
- 2) Если $q(x_{i_1 \dots i_k}) = 0$, то $p(x_{i_1 \dots i_k}) = f(x) = 0$, значит (1) выполнено.
- 3) Остался случай $p(x_{i_1 \dots i_k}) = 0$, $q(x_{i_1 \dots i_k}) = 1$. Тогда

$$\overline{p(x_{i_1 \dots i_k})}q(x_{i_1 \dots i_k}) = 1,$$

значит $x \in \mathcal{D}$, и определена функция $f_{\mathcal{D}}(x)$, причём $f_{\mathcal{D}}(x) = f(x)$. Таким образом, (1) в этом случае также выполнено.

Лемма доказана. □

В представлении (1) используется частичная булева функция, для её реализации будем использовать схему, построенную в работе [34]. Эта схема является оптимальной (по порядку) по площади, мощности и глубине.

Для удобства реализации функций p и q одной схемой введём операцию слияния двух схем. Неформально, при этой операции элементы каждой схемы раздвигаются, при этом элементы первой схемы размещаются в клетках с чётными координатами, а элементы второй схемы — в клетках с нечётными координатами (см. рисунок 2)

Разместим схемы K_1 и K_2 на плоскости таким образом, чтобы координаты всех элементов были неотрицательными, но для каждой из координат были элементы с нулевыми значениями этой координаты. Слиянием схем K_1 и K_2 будем называть схему $K = K_1 \uplus K_2$ построенную следующим образом. Напомним, что схему мы определяли, как отображение из некоторого множества M в множество $E \cup \{\lambda\}$. Доопределим это отображение на $\mathbb{Z}^2 \setminus M$ значением λ .

- 1) $K(2i, 2j) = K_1(i, j)$.
- 2) $K(2i + 1, 2j + 1) = K_2(i, j)$.

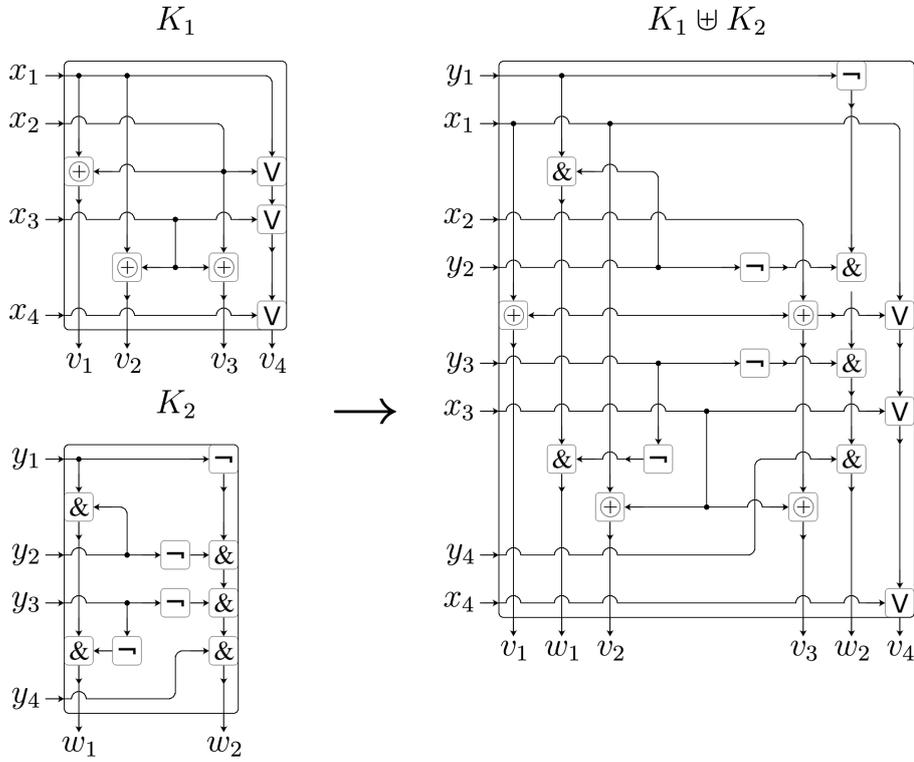


Рис. 2: Пример применения операции слияния.

- 3) Элемент $K(2i + 1, 2j)$ соединяет элементы $K(2i, 2j)$ и $K(2i + 2, 2j)$, если точка $(i + 1/2, j)$ является узлом схемы K_1 , а также соединяет элементы $K(2i + 1, 2j - 1)$ и $K(2i + 1, 2j + 1)$, если точка $(i, j - 1/2)$ является узлом схемы K_2 .
- 4) Элемент $K(2i, 2j + 1)$ соединяет элементы $K(2i - 1, 2j + 1)$ и $K(2i + 1, 2j + 1)$, если точка $(i - 1/2, j)$ является узлом схемы K_2 , а также соединяет элементы $K(2i, 2j)$ и $K(2i, 2j + 2)$, если точка $(i, j + 1/2)$ является узлом схемы K_1 .

Если схема K_1 реализовывала оператор f_1 , а схема K_2 — оператор f_2 , то схема $K_1 \uplus K_2$ реализует оператор $f(x, y) = (f_1(x), f_2(y))$. При этом каждому узлу схем K_1 и K_2 соответствуют 2 узла схемы $K_1 \uplus K_2$. Носителем схемы $K_1 \uplus K_2$ является множество ячеек (i, j) таких, что $(K_1 \uplus K_2)(i, j) \neq \lambda$.

Легко видеть, что параметры схемы $K_1 \uplus K_2$ удовлетворяют неравенствам

$$\begin{aligned} l(K_1 \uplus K_2) &\leq 2 \max(l(K_1), l(K_2)), \\ h(K_1 \uplus K_2) &\leq 2 \max(h(K_1), h(K_2)), \\ U(K_1 \uplus K_2) &\leq 2(U(K_1) + U(K_2)), \\ \widehat{U}(K_1 \uplus K_2) &\leq 2(\widehat{U}(K_1) + \widehat{U}(K_2)). \end{aligned}$$

При этом если K_1 и K_2 были прямоугольными и все входы и выходы схем K_1 и K_2 были слева, то схема $K_1 \uplus K_2$ также будет прямоугольной, и её входы и выходы также будут слева.

Для построения схемы, реализующей монотонную функцию, нам понадобятся вспомогательные блоки, описанные в [34].

У некоторых блоков есть вход, который обозначается z . Внутри блоков используются 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.

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}* .

В [34] параметры нужных нам блоков являются промежуточными результатами. Сформулируем это в виде леммы.

Лемма 5. *Для любого натурального n и константы $k \in \mathbb{N}$ существуют схема $D'_{n,k}$ с $nk + 1$ входом и 2^{nk} выходами, а также схема $D'^{-1}_{n,k}$ с 2^{nk} входом и $nk + 1$ выходом. При этом*

$$D'^{-1}_{n,k}(D'_{n,k}(1, x_1, \dots, x_{nk})) = (1, x_1, \dots, x_{nk}).$$

Блоки $D'_{n,k}$ и $D'^{-1}_{n,k}$ при фиксированном k имеют следующие параметры

$$\begin{aligned} l(D'_{n,k}) &= O(2^n), & h(D'_{n,k}) &= O(n^2) \\ l(D'^{-1}_{n,k}) &= O(2^n), & h(D'^{-1}_{n,k}) &= O(n^2) \end{aligned}$$

Входы и выходы блоков $D'_{n,k}$ и $D'^{-1}_{n,k}$ расположены, как показано на рисунке 3.

Также нам понадобится блок, реализующий частичную функцию вида $zf_{\mathcal{D}}(x)$, где $f_{\mathcal{D}}(x)$ — произвольная частичная булева функция, определённая на множестве \mathcal{D} . Следующая лемма является промежуточным результатом в [34, Доказательство теоремы 1].

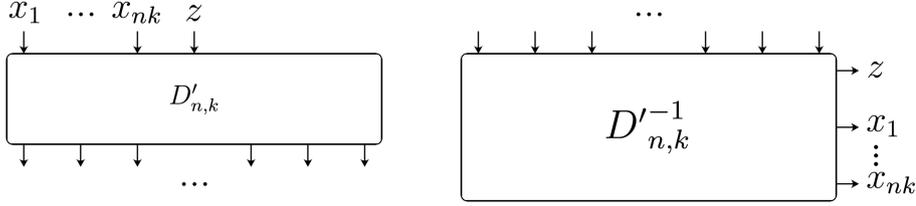


Рис. 3: Блоки $D'_{n,k}$ и $D'^{-1}_{n,k}$.

Лемма 6. Если $\mathcal{D} \subseteq \{0, 1\}^n$, причём $n^2 = O(|\mathcal{D}|)$ при $n \rightarrow \infty$, то для любой частичной функции $f : \mathcal{D} \rightarrow \{0, 1\}$ существует прямоугольная схема $S'_{f_{\mathcal{D}}}$ в базисе из элементов, сохраняющих 0, реализующая оператор f такая, что

$$l(K) = O(\sqrt{|\mathcal{D}|}), \quad h(K) = O(\sqrt{|\mathcal{D}|}), \quad \widehat{U}(K) = O\left(\max\left(n \log_2^2 n, \sqrt{|\mathcal{D}|}\right)\right).$$

Доказательство. Для доказательства этой леммы достаточно рассмотреть схему Q_f из доказательства [34, теорема 1] при $m = 1$ и элемент 1 заменить на вход z . Поскольку все вспомогательные блоки, из которых построена схема Q_f построены из элементов \oplus , $\&$, \vee и проводов, значит единственным элементом, не сохраняющим 0 в Q_f является элемент 1, вместо которого мы сделали вход схемы z . \square

Итак, мы описали все вспомогательные блоки из [34], которые нам понадобятся, и можем приступить к построению схем, реализующих монотонные функции.

Лемма 7. Если n кратно 6, то для произвольной монотонной функции от n переменных существует реализующая её схема M_f со следующими параметрами

$$\begin{aligned} l(M_f) &\leq C_1 \frac{2^{n/2}}{\sqrt[4]{n}}, & h(M_f) &\leq C_1 \frac{2^{n/2}}{\sqrt[4]{n}}, \\ \widehat{U}(M_f) &\leq C_2 \frac{2^{n/2}}{\sqrt[4]{n}}, & U(M_f) &\leq C_3 \frac{2^{n/2}}{n^{3/4}}. \end{aligned}$$

Здесь C_1, C_2, C_3 — некоторые константы.

Доказательство. Будем доказывать лемму индукцией по числу переменных.

База индукции. При $n \leq 18$ множество функций конечно, поэтому можно просто взять константы C_1, C_2 и C_3 достаточно большими, чтобы утверждение леммы выполнялось для оптимальных по площади схем, реализующих эти функции.

Шаг индукции. Возьмём произвольную функцию f от n переменных и применим к ней лемму 4, подставляя $k = 6$. По лемме 4 существуют такие функции $p, q \in M(n-6)$ такие, что

$$f(x) = p(x_{i_1 \dots i_6}) \vee \overline{p(x_{i_1 \dots i_6})} q(x_{i_1 \dots i_6}) f_{\mathcal{D}}(x_{i_1 \dots i_6}), \quad (2)$$

где $\mathcal{D} = \{x : \overline{p(x_{i_1 \dots i_6})} q(x_{i_1 \dots i_6}) = 1\}$, $|\mathcal{D}| \leq 2^5 C_n^{n/2}$.

Поскольку при реализации функции схемой мы можем менять места-ми аргументы функции, выбирая, какой выход какому аргументу соответствует, без ограничения общности будем считать, что $i_1 = 1, \dots, i_6 = 6$. Тогда $x_{i_1 \dots i_6} = (x_7, \dots, x_n)$.

По предположению индукции существуют схемы M_p и M_q , реализующие функции p и q соответственно, с параметрами

$$\begin{aligned} l, h &\leq C_1 \frac{2^{(n-6)/2}}{\sqrt[4]{n-6}} = \frac{1}{8} \sqrt[4]{\frac{n}{n-6}} C_1 \frac{2^{n/2}}{\sqrt[4]{n}} \leq \frac{1}{6} C_1 \frac{2^{n/2}}{\sqrt[4]{n}}, \\ \widehat{U} &\leq C_2 \frac{2^{(n-6)/2}}{\sqrt[4]{n-6}} = \frac{1}{6} C_2 \frac{2^{n/2}}{\sqrt[4]{n}}, \\ U &\leq C_3 \frac{2^{(n-6)/2}}{(n-6)^{3/4}} = \frac{1}{8} \left(\frac{n}{n-6}\right)^{3/4} C_3 \frac{2^{n/2}}{n^{3/4}} \leq \frac{1}{6} C_3 \frac{2^{n/2}}{n^{3/4}}. \end{aligned}$$

По лемме 6 существует схема $S'_{f, \mathcal{D}}$ реализующая функцию $f'_{\mathcal{D}}(z, x) = z f_{\mathcal{D}}(x)$ с параметрами

$$l, h, U, \widehat{U} = O\left(\sqrt{|\mathcal{D}|}\right) = O\left(\sqrt{32C_n^{n/2}}\right) = O\left(\frac{2^{n/2}}{\sqrt[4]{n}}\right) \leq C_4 \frac{2^{n/2}}{\sqrt[4]{n}}.$$

Построим схему M_f , как показано на рисунке 4. В этой схеме блоки M_p и M_q объединены при помощи операции слияния. Фактически, схема M_f реализует функцию f по формуле (2), только в ней добавлены блок конъюнкций, а также блоки $D'_{n/6,6}$ и $D'^{-1}_{n/6,6}$, вычисляющие взаимно обратные операторы, с целью уменьшения потенциала на проводах.

Проверим, что M_f реализует функцию f , и оценим потенциал части схемы M_f , включающей в себя блоки $D'_{n/6,6}$, $D'^{-1}_{n/6,6}$ и $S'_{f, \mathcal{D}}$ и соединяющие их провода.

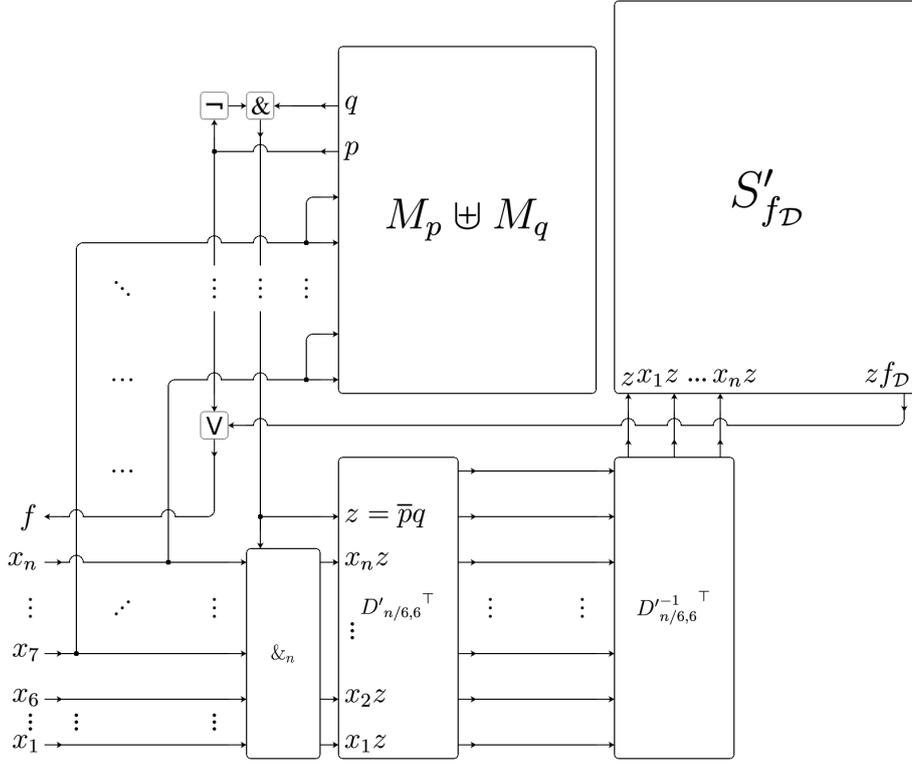


Рис. 4: Схема M_f , реализующая функцию f .

- 1) Если $\overline{p(x_{1,\dots,6})q(x_{1,\dots,6})} = 0$, то $f(x_1, \dots, x_n) = p(x_{1,\dots,6})$. В этом случае на вход блока конъюнкций подаётся 0, поэтому на все выходы этого блока также выдают 0. Значит блоки $D'_{n/6,6}$, $D'^{-1}_{n/6,6}$ и S'_{fD} вместе с соединяющими их проводами неактивны, и их потенциал равен 0. Выход блока S'_{fD} также неактивен, а значит значение на выходе f схемы M_f равно $p = p(x_{1,\dots,6}) = f(x_1, \dots, x_n)$.
- 2) Если $\overline{p(x_{1,\dots,6})q(x_{1,\dots,6})} = 1$, то $p = p(x_{1,\dots,6}) = 0$, поэтому

$$f(x_1, \dots, x_n) = \overline{p(x_{1,\dots,6})q(x_{1,\dots,6})} f_D(x_1, \dots, x_n) = f_D(x_1, \dots, x_n).$$

В этом случае блок конъюнкций пропускает значения x_1, \dots, x_n на вход блока $D'_{n/6,6}$, при этом на вход z этого блока подаётся $\bar{p}q = 1$. Проходя через блоки $D'_{n/6,6}$ и $D'^{-1}_{n/6,6}$, вычисляющие взаимно обратные операторы, значения x_1, \dots, x_n и управляющее значение $z =$

$\bar{p}q = 1$ подаются на вход схемы $S'_{f_{\mathcal{D}}}$. На выходе блок $S'_{f_{\mathcal{D}}}$ выдаёт значение $zf_{\mathcal{D}}(x_1, \dots, x_n) = f_{\mathcal{D}}(x_1, \dots, x_n) = f(x_1, \dots, x_n)$. Значение на выходе f схемы M_f равно $p \vee f_{\mathcal{D}}(x_1, \dots, x_n) = f(x_1, \dots, x_n)$.

В этом случае потенциал блока $S'_{f_{\mathcal{D}}}$ не превосходит его максимального потенциала, то есть $C_4 \frac{2^{n/2}}{\sqrt[4]{n}}$. Потенциалы блоков $D'_{n/6,6}$ и $D'^{-1}_{n/6,6}$ по порядку не превосходят их площади, то есть

$$\begin{aligned} \widehat{U}_{\mathcal{D}}(D'_{n/6,6}) + \widehat{U}_{\mathcal{D}}(D'^{-1}_{n/6,6}) &= O(S(D'_{n/6,6}) + S(D'^{-1}_{n/6,6})) = \\ &= O(2^{n/6} \cdot n^2) = O(2^{n/4}). \end{aligned}$$

Провода, соединяющие блоки $D'_{n/6,6}$ и $D'^{-1}_{n/6,6}$, имеют длину $l(M_p \uplus M_q) \leq 2 \cdot \frac{1}{6} C_1 \frac{2^{n/2}}{\sqrt[4]{n}}$, причём не более 6 из этих проводов активны. Провод, идущий от выхода блока $S'_{f_{\mathcal{D}}}$, имеет ту же длину. Поэтому общий потенциал проводов этой части схемы не превосходит $\frac{7}{3} C_1 \frac{2^{n/2}}{\sqrt[4]{n}}$.

Итак, мы показали, что в обоих случаях схема M_f работает корректно.

Оценим теперь размеры и потенциал всей схемы M_f . При достаточно большом C_1 имеем

$$\begin{aligned} l(M_f) &\leq n + 1 + l(\&_n) + \max \left(l(D'_{n/6,6}{}^{\top}) + l(D'^{-1}_{n/6,6}{}^{\top}), l(M_p \oplus M_q) \right) + \\ &\quad + l(S'_{f_{\mathcal{D}}}) = O(n^2) + 2 \cdot \frac{1}{6} C_1 \frac{2^{n/2}}{\sqrt[4]{n}} + C_4 \frac{2^{n/2}}{\sqrt[4]{n}} \leq C_1 \frac{2^{n/2}}{\sqrt[4]{n}}, \\ h(M_f) &= h(D'_{n/6,6}{}^{\top}) + 1 + \max (h(S'_{f_{\mathcal{D}}}), h(M_p \uplus M_q)) < \\ &< h(S'_{f_{\mathcal{D}}}) + h(D'_{n/6,6}{}^{\top}) + 1 + h(M_p \uplus M_q) = \\ &= C_4 \frac{2^{n/2}}{\sqrt[4]{n}} + O(2^{n/6}) + 2 \cdot \frac{1}{6} C_1 \frac{2^{n/2}}{\sqrt[4]{n}} < C_1 \frac{2^{n/2}}{\sqrt[4]{n}}. \end{aligned}$$

Оценим потенциал оставшейся части схемы, то есть блока $M_p \uplus M_q$, блока конъюнкций и ведущих к ним проводов.

- Ведущие к блоку $M_p \uplus M_q$ провода, а также ведущие от него провода вместе с двумя логическими элементами и блоком конъюнкций помещаются в прямоугольник со сторонами $O(n)$, поэтому их суммарный потенциал составляет $O(n^2)$.

- Пользуясь предположением индукции для оценки потенциала блоков M_p и M_q , получим

$$\begin{aligned}\widehat{U}(M_p \uplus M_q) &\leq 2(\widehat{U}(M_p) + \widehat{U}(M_q)) \leq 4 \cdot \frac{1}{6} C_2 \frac{2^{n/2}}{\sqrt[4]{n}} = \frac{2}{3} C_2 \frac{2^{n/2}}{\sqrt[4]{n}}, \\ U(M_p \uplus M_q) &\leq 2(U(M_p) + U(M_q)) \leq 4 \cdot \frac{1}{6} C_3 \frac{2^{n/2}}{n^{3/4}} = \frac{2}{3} C_3 \frac{2^{n/2}}{n^{3/4}}.\end{aligned}$$

Итак, для всей схемы M_f потенциал вне области \mathcal{D} (где $\bar{p}q = 0$) при достаточно большом C_2 можно оценить следующим образом.

$$\begin{aligned}\widehat{U}_{\overline{\mathcal{D}}}(M_f) &= O(n^2) + \frac{2}{3} C_2 \frac{2^{n/2}}{\sqrt[4]{n}} < C_2 \frac{2^{n/2}}{\sqrt[4]{n}}, \\ U_{\overline{\mathcal{D}}}(M_f) &= O(n^2) + \frac{2}{3} C_3 \frac{2^{n/2}}{n^{3/4}} < C_3 \frac{2^{n/2}}{n^{3/4}}.\end{aligned}$$

Внутри области \mathcal{D} к этому ещё прибавится потенциал $S'_{f_{\mathcal{D}}}$ и вспомогательных блоков.

$$\widehat{U}_{\mathcal{D}}(M_f) = O(n^2) + \frac{2}{3} C_2 \frac{2^{n/2}}{\sqrt[4]{n}} + C_4 \frac{2^{n/2}}{\sqrt[4]{n}} + O(2^{n/4}) < C_2 \frac{2^{n/2}}{\sqrt[4]{n}}.$$

Отсюда сразу получается оценка максимального потенциала. При достаточно большом C_3 выполнена цепочка неравенств

$$\begin{aligned}U(M_f) &= \frac{|\overline{\mathcal{D}}|}{2^n} U_{\overline{\mathcal{D}}}(M_f) + \frac{|\mathcal{D}|}{2^n} U_{\mathcal{D}}(M_f) \leq U_{\overline{\mathcal{D}}}(M_f) + \frac{|\mathcal{D}|}{2^n} \widehat{U}_{\mathcal{D}}(M_f) \leq \\ &\leq O(n^2) + \frac{2}{3} C_3 \frac{2^{n/2}}{n^{3/4}} + \underbrace{\frac{32 C_n^{n/2}}{2^n}}_{\leq C_5/\sqrt{n}} \cdot C_2 \frac{2^{n/2}}{\sqrt[4]{n}} \leq \\ &\leq O(n^2) + \left(\frac{2}{3} C_3 + C_5 C_2 \right) \frac{2^{n/2}}{n^{3/4}} < C_3 \frac{2^{n/2}}{n^{3/4}}.\end{aligned}$$

Лемма доказана. \square

Доказательство верхней оценки теоремы 3. Возьмём произвольную n -местную монотонную функцию f и построим схему с требуемыми параметрами. Введём $6 - (n \bmod 6)$ (всего не более 5) фиктивных переменных и обозначим новую функцию за f' . $n' = n + 6 - (n \bmod 6)$ — количество

переменных функции f' . Тогда n' кратно 6, значит к f' можно применить лемму 7. По лемме существует схема $M_{f'}$, реализующая функцию f' с параметрами

$$\begin{aligned} l(M_{f'}) &\leq C_1 \frac{2^{n'/2}}{\sqrt[4]{n'}} \leq 2^{5/2} \cdot C_1 \frac{2^{n/2}}{\sqrt[4]{n}} = O\left(\frac{2^{n/2}}{\sqrt[4]{n}}\right), \\ h(M_{f'}) &\leq C_1 \frac{2^{n'/2}}{\sqrt[4]{n'}} = O\left(\frac{2^{n/2}}{\sqrt[4]{n}}\right), \\ \widehat{U}(M_{f'}) &\leq C_2 \frac{2^{n'/2}}{\sqrt[4]{n'}} = O\left(\frac{2^{n/2}}{\sqrt[4]{n}}\right), \\ U(M_{f'}) &\leq C_3 \frac{2^{n'/2}}{n'^{3/4}} \leq 2^{5/2} \cdot C_3 \frac{2^{n/2}}{n^{3/4}} = O\left(\frac{2^{n/2}}{n^{3/4}}\right). \end{aligned}$$

Удаляя фиктивные входы из схемы $M_{f'}$, получим схему M_f , реализующую функцию f . Удаление фиктивных входов не увеличивает площадь и потенциал, поэтому для M_f верны те же верхние оценки, что и для $M_{f'}$. Верхняя оценка доказана. \square

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 (MaTIC) // 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 циклической 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] Калачев Г.В. Оценки мощности плоских схем, реализующих функции с ограниченным числом единиц // Интеллектуальные системы. Теория и приложения. — 2017. — Т. 21, № 1. — С. 25–87.
- [36] Чашкин А.В. Лекции по дискретной математике // М.: МГУ Мехмат, 2007.
- [37] Жуков Д.А. О вычислении частичных булевых функций клеточными схемами. // Дискретный анализ и исследование операций.