

# ПРЕПРИНТЫ ПОМИ РАН

## ГЛАВНЫЙ РЕДАКТОР

С.В. Кисляков

## РЕДКОЛЛЕГИЯ

В.М.Бабич, Н.А.Вавилов, А.М.Вершик, М.А.Всемирнов, А.И.Генералов, И.А.Ибрагимов,  
Л.Ю.Колотилина, Б.Б.Лурье, Ю.В.Матияевич, Н.Ю.Нецветаев, С.И.Репин, Г.А.Серегин

Учредитель: Санкт-Петербургское отделение Математического института  
им. В. А. Стеклова Российской академии наук

Свидетельство о регистрации средства массовой информации: ЭЛ №ФС 77-33560 от 16  
октября 2008 г. Выдано Федеральной службой по надзору в сфере связи и массовых  
коммуникаций

Контактные данные: 191023, г. Санкт-Петербург, наб. реки Фонтанки, дом 27

телефоны:(812)312-40-58; (812) 571-57-54

e-mail: [admin@pdmi.ras.ru](mailto:admin@pdmi.ras.ru)

<http://www.pdmi.ras.ru/preprint/>

Заведующая информационно-издательским сектором Симонова В.Н

## СХЕМНАЯ СЛОЖНОСТЬ МОД-ФУНКЦИЙ<sup>1</sup>

**А. А. Кожевников      А. С. Куликов**

Санкт-Петербургское отделение  
Математического института им. В. А. Стеклова  
Российской академии наук

<http://logic.pdmi.ras.ru/{~arist,~kulikov}>

**Г. Н. Ярославцев**

Академический физико-технологический университет  
Российской академии наук

<http://logic.pdmi.ras.ru/~grigory>

30 ноября 2008

### Аннотация

В 1977-м году Стокмайер показал, что любая схема над полным бинарным базисом для некоторого класса симметрических функций, содержащего все функции  $\text{MOD}_m^n$  ( $m \geq 3$ ), содержит хотя бы  $2.5n - c$  гейтов. Он также представил оптимальную схему для  $\text{MOD}_4^n$ . В данной работе мы приводим модифицированное доказательство Стокмайера, дающее нижнюю оценку  $2.5n - c$  для другого класса, содержащего не только симметрические функции. Этот класс, в частности, содержит функцию  $\text{MOD}_3^n$ . Мы также даём очень простое доказательство нижней оценки  $7n/3 - c$  для класса функций, задаваемых полиномами Жегалкина высокой степени. Основной идеей является комбинированная мера сложности, присваивающая разные веса гейтам разных типов. В конце работы мы также приводим схему размера  $3n$  для функции  $\text{MOD}_3^n$  и описываем способ, с помощью которого она была найдена.

---

<sup>1</sup>Исследования частично поддержаны Российском фондом фундаментальных исследований (гранты 06-01-00502-а и 08-01-00640-а).

ГЛАВНЫЙ РЕДАКТОР

С. В. Кисляков

РЕДКОЛЛЕГИЯ

В. М. Бабич, Н. А. Вавилов, А. М. Вершик, М. А. Всемиров, А. И. Генералов, И. А. Ибрагимов,  
А. А. Иванов, Л. Ю. Колотилина, В. Н. Кублановская, Г. В. Кузьмина, П. П. Кулиш, Б. Б. Лурье,  
Ю. В. Матиясевич, Н. Ю. Нецветаев, С. И. Репин, Г. А. Серегин, В. Н. Судаков, О. М. Фоменко

# 1 Введение

Доказательство нижних оценок на схемную сложность явно заданных булевых функций является одной из самых известных и трудных задач современной теоретической информатики. Несмотря на то, что из соображений мощности легко следует, что почти все булевы функции имеют экспоненциальный размер, нам до сих пор неизвестно ни одной функции, требующей схем суперлинейного размера. Более того, известно всего несколько доказательств линейных оценок. Именно, Шнорр [10] доказал нижнюю оценку  $2n - c$  для класса функций, для которых при подстановке констант любым двум переменным можно получить хотя бы три разные подфункции. Далее Пол [9] доказал нижнюю оценку  $2.5n - c$  для модифицированной версии функции индексации. Стокмайер [11] доказал ту же оценку для класса симметрических функций, удовлетворяющих некоторому простому условию. И наконец, Блюм [3] слегка модифицировал функцию Пола и доказал нижнюю оценку  $3n - o(n)$  для неё. Эта оценка была опубликована в 1984-м году и до сих пор остаётся лучшей из известных для схем над полным бинарным базисом  $B_2$ . Рекордная оценка  $5n - o(n)$  для базиса  $U_2 = B_2 \setminus \{\oplus, \equiv\}$  представлена в 2001-м году Ивамой и др. [6].

Все упомянутые выше оценки были доказаны методом удаления гейтов. Основная идея этого метода состоит в следующем: рассматривается булева функция от  $n$  переменных из определённого класса функций и показывается, что любая оптимальная схема содержит комбинацию гейтов, которую можно удалить присваиванием значений переменным. Обычно гейт удаляется, потому что один из его входов становится константой. В некоторых случаях можно также удалить гейт путём перестраивания схемы. Хотя этот метод является по сути единственным известным методом для доказательства нетривиальных нижних оценок для обычной схемной сложности, многие авторы обращают внимание на то, что получение нелинейных нижних оценок таким методом вряд ли возможно.

В данной статье рассматривается схемная сложность MOD-функций. Интересно отметить, что для формул и схем над базисами  $U_2$  и  $B_2$  известно, что сложность  $\text{MOD}_m^n$ , где  $m = 3$  или  $m \geq 5$ , не меньше сложности  $\text{MOD}_4^n$ . Однако ни для какой из этих моделей не известно, правда ли, что  $\text{MOD}_3^n$  или  $\text{MOD}_5^n$  строго сложнее, чем  $\text{MOD}_4^n$ . В таблице 1 представлены известные верхние и нижние оценки для  $\text{MOD}_m^n$  в различных моделях вычислений (через  $C$  и  $L$  мы обозначаем схемную и формульную сложность, соответственно).

Мы вводим класс функций  $\text{GMOD}_m^n$ , состоящий из всех булевых функций  $f(x_1, \dots, x_n)$ , значение которых зависит от  $\sum_{i=1}^n \alpha_i x_i \pmod{m}$ . Сначала мы замечаем, что любая функция из  $\text{GMOD}_m^n$ , для простого  $m \geq 3$ , задаётся полиномом высокой степени над  $\text{GF}(2)$ . С использованием этого факта мы приводим доказательство нижней оценки  $7n/3 - c$  на схемную сложность любой такой функции. Доказательство такое же простое, как доказательство нижней оценки  $2n - c$  Шнорра [10]. Ключевая идея

$m$		$L_{U_2}$	$L_{B_2}$	$C_{U_2}$	$C_{B_2}$
2	нижняя	$\Theta(n^2)$ [1]	$n$	$3n + c$ [10]	$n - 1$
	верхняя				
3	нижняя	$\Omega(n^2)$ [1]	$\Omega(n \log n)$ [5]	$4n + c$ [13]	$2.5n + c$ [11]
	верхняя	$O(n^{2.58})$ [4]	$O(n^2)$ [12]	$7n + o(n)$ [2]	$5n + o(n)$ [2]
4	нижняя	$\Theta(n^2)$ [1]	$\Omega(n \log n)$ [5]	$4n + c$ [13]	$2.5n + c$ [11]
	верхняя	$O(n^2 \log^2 n)$ [5]		$5n$ [13]	
$\geq 5$	нижняя	$\Omega(n^2)$ [1]	$\Omega(n \log n)$ [5]	$4n + c$ [13]	$2.5n + c$ [11]
	верхняя	$O(n^{4.57})$ [8]	$O(n^{3.13})$ [8]	$7n + o(n)$ [2]	$5n + o(n)$ [2]

Таблица 1: Известные нижние и верхние оценки для функций  $\text{MOD}_m^n$  в различных моделях вычислений.

этого доказательства состоит в комбинированной мере сложности, которая присваивает различные веса гейтам различных типов. Другая интересная особенность этого доказательства состоит в том, что в нём не только анализируется верхняя часть схемы, но также используется некоторая информация о свойствах схемы в целом.

Затем мы приводим доказательство нижней оценки  $2.5n - c$  для класса функций, содержащего  $\text{GMOD}_3^n$ , которое является модификацией доказательства Стокмайера [11]. Отметим, что Стокмайер доказал нижнюю оценку  $2.5n - c$  для всех функций  $\text{MOD}_m^n$ , где  $(m \geq 3)$ , но его доказательство работает только для симметрических функций. Основное отличие класса  $\text{GMOD}_m$  от класса  $\text{MOD}_m$  состоит в том, что  $\text{GMOD}_m$  инвариантен относительно подстановок типа  $x_i = x_j$ .

В конце статьи мы приводим схему размера  $3n$  для класса  $\text{GMOD}_3^n$ , которая была найдена с использованием SAT-солверов.

## 2 Общая постановка задачи

### 2.1 Класс $\text{GMOD}_m^n$

Через  $B_n$  обозначим множество всех булевых функций  $f: \{0, 1\}^n \rightarrow \{0, 1\}$ . Функция  $f \in B_n$  называется симметрической, если её значение зависит только от суммы входных битов. То есть должен существовать вектор  $v \in \{0, 1\}^{n+1}$  такой, что  $f(x_1, \dots, x_n) = v_s$ , где  $s = \sum_{i=1}^n x_i$ . Типичной симметрической функцией является функция  $\text{MOD}_{m,k}^n$ , определяемая следующим образом:

$$\text{MOD}_{m,k}^n(x_1, \dots, x_n) = 1 \Leftrightarrow \sum_{i=1}^n x_i \equiv k \pmod{m}.$$

Мы также рассматриваем функции, зависящие не просто от  $\sum x_i$ , но от произвольной линейной комбинации с целыми коэффициентами  $\sum \alpha_i x_i$ . Через  $\text{GMOD}_m^n$  обозначим класс функций  $f \in B_n$ , для которых существуют целые числа  $1 \leq \alpha_1, \dots, \alpha_n \leq m - 1$  и целое число  $k$  такое, что

$$f(x_1, \dots, x_n) = 1 \Leftrightarrow \sum_{i=1}^n \alpha_i x_i \equiv k \pmod{m}.$$

Заметим, что если  $f \in \text{GMOD}_m^n$  и  $c \in \{0, 1\}$ , тогда

$$\text{либо } f|_{x_i=x_j \oplus c} \in \text{GMOD}_m^{n-1}, \text{ либо } f|_{x_i=x_j \oplus c} \in \text{GMOD}_m^{n-2}.$$

Легко видеть, что для простого  $p$  и  $n \geq p^2 + 2$  и для любой  $f \in \text{GMOD}_p^n$ ,  $f$  не является константой и есть хотя бы три различных функции среди

$$f|_{x_i=0, x_j=0}, f|_{x_i=0, x_j=1}, f|_{x_i=1, x_j=0}, f|_{x_i=1, x_j=1}.$$

### 2.2 Степень булевых функций

Любая булева функция  $f: \{0, 1\}^n \rightarrow \{0, 1\}$  легко может быть представлена в виде полилинейного полинома над  $\text{GF}(2)$ , т.е. в виде хог (суммы) конъюнкций (мономов). Такой полином называется полиномом Жегалкина. Хорошо известно, что такое представление единственно. Таким образом, в дальнейшем изложении мы обозначаем единственный полилинейный полином над  $\text{GF}(2)$ , представляющий  $f$ , через  $\chi(f)$ . Важной характеристикой функции  $f$  является степень  $\chi(f)$ , обозначаемая как  $\deg(f)$ . Понятно, что если схема содержит мало гейтов типа- $\wedge$ , то она не может вычислять функцию высокой степени.

**Лемма 2.1.** *Любая схема, вычисляющая булеву функцию  $f: \{0, 1\}^n \rightarrow \{0, 1\}$ , содержит хотя бы  $(\deg(f) - 1)$  гейтов типа- $\wedge$ .*

Несложно показать, что для любой  $f \in \text{GMOD}_p^n$ ,  $\deg(f) \geq n - p$ , для простого  $p$  и  $n \geq p^2$ . Для доказательства этого факта нужно заметить, что для булевой функции  $f: \{0, 1\}^n \rightarrow \{0, 1\}$ ,  $\deg(f) = n$  тогда и только тогда, когда  $|f^{-1}(1)|$  нечётно. Это легко доказать по индукции, заметив, что

$$f^{-1}(1) = (f|_{x_i=1})^{-1}(1) \cup (f|_{x_i=0})^{-1}(1), \quad (1)$$

$$\chi(f) = x_i \cdot \chi(f|_{x_i=1}) + (1 - x_i) \cdot \chi(f|_{x_i=0}). \quad (2)$$

Затем нужно показать, что для любой  $f \in \text{GMOD}_p^n$ ,  $|f^{-1}(1)|$  нечётно. Это также может быть показано по индукции с использованием равенства (2). Обозначим через  $c_f \in \{0, 1\}$  коэффициент монома  $x_1 \dots x_n$  в  $\chi(f)$ . Из равенства (2) тогда следует, что  $c_f = c_{f'} \oplus c_{f''}$  для некоторых  $f', f'' \in \text{GMOD}_p^{n-1}$ .

### 2.3 Схемы в базисе $B_2$

Схема представляет собой ориентированный ациклический граф с вершинами, имеющими входящую степень 0 или 2. Вершины, имеющие входящую степень 0, соответствуют переменным  $\{x_1, \dots, x_n\}$  и называются входами. Вершины со входящей степенью 2 вычисляют функции из  $B_2$  и называются гейтами. Также есть гейты, соответствующие выходам схемы. Размером схемы называется число гейтов, из которых она состоит. Мы называем функцию  $f \in B^n$  вырожденной, если она не зависит существенно от некоторых своих переменных, то есть существует такая переменная  $x_i$ , что подфункции  $f|_{x_i=0}$  и  $f|_{x_i=1}$  равны. Легко видеть, что гейт, вычисляющий вырожденную функцию из  $B_2$ , может быть легко удалён из схемы без увеличения её размера (при удалении этого гейта, возможно, придётся изменить функции, вычисляемые в его потомках). Множество функций в базисе  $B_2$  содержит десять невырожденных функций  $f(x, y)$ :

- восемь функций вида  $((x \oplus a) \wedge (y \oplus b)) \oplus c$ , где  $a, b, c \in \{0, 1\}$ ; мы называем их функциями типа- $\wedge$ ;
- две функции вида  $x \oplus y \oplus a$ , где  $a \in \{0, 1\}$ , которые называются функциями типа- $\oplus$ .

Основное отличие между этими двумя типами функций состоит в том, что функцию типа- $\wedge$  всегда можно сделать константой путём присваивания константы любому из её входов (например, после замены входа  $x$  на константу  $a$  на выходе гейта получается константа  $c$ ; в таком случае мы говорим, что гейт стал тривиальным), в то время как для функций типа- $\oplus$  это невозможно. Таким образом, если есть переменная, входящая в два гейта типа- $\oplus$ , то путём присваивания любого значения этой переменной можно удалить только эти два гейта. Однако если хотя бы один из двух потомков переменной является гейтом типа- $\wedge$ , то присваиванием соответствующего значения этой переменной можно удалить оба эти гейта, а также всех потомков этого гейта типа- $\wedge$ . Именно по этой причине на данный момент лучшие нижние оценки для схем в базисе  $U_2$  лучше, чем оценки для схем в базисе  $B_2$ .

## 3 Нижняя оценка $7n/3$

В этом разделе мы приводим доказательство нижней оценки  $7n/3 - c$ , которое настолько же просто, как и доказательство Шнорра оценки  $2n - c$  [10]. Сначала мы определяем класс функций, который является классом, использованным Шнорром, но с дополнительным ограничением на степень. С помощью этого ограничения мы получаем нижнюю оценку (показанную в лемме 2.1) на число гейтов типа- $\wedge$  в любой схеме, которая вычисляет функцию из данного класса. Затем мы вводим меру сложности схем путём присваивания различных весов гейтам типа- $\oplus$  и типа- $\wedge$  и доказываем нижнюю оценку для неё, используя потом эту нижнюю оценку для получения нижней оценки на схемную сложность.

**Определение 3.1.** Пусть  $S_{k,d}^n$  — это класс всех функций  $f \in B_n$  со следующими свойствами:

1. если  $n \geq k$ , то для любых двух переменных  $x_i$  и  $x_j$  получаются хотя бы три различных подфункции  $f$  при присваивании значений  $x_i$  и  $x_j$ ;
2. если  $n \geq k$ , то для любой переменной  $x_i$  и любой константы  $c \in \{0, 1\}$ ,  $f|_{x_i=c} \in S_{k,d}^{n-1}$ ;

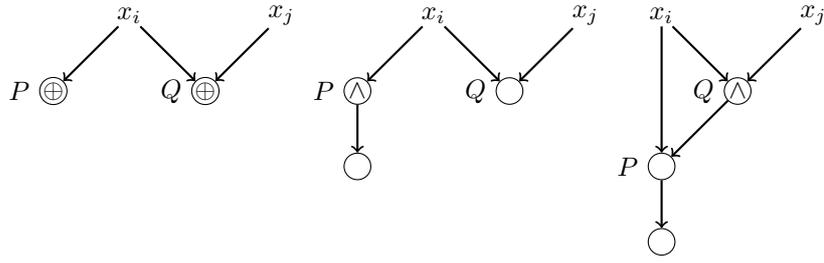


Рис. 1: Различные случаи в лемме 3.1.

3.  $\deg(f) \geq n - d$ .

Для доказательства приведённой нижней оценки мы используем следующую меру схемной сложности:  $\mu(C) = 3X(C) + 2A(C)$ , где  $X(C)$  и  $A(C)$  обозначают, соответственно, число гейтов типа- $\oplus$  и типа- $\wedge$  в  $C$ .

**Лемма 3.1.** Для любой схемы  $C$ , вычисляющей функцию  $f \in S_{k,d}^n$ ,

$$\mu(C) \geq 6(n - k - 1).$$

*Доказательство.* Доказательство ведётся индукцией по  $n$ . Случай  $n \leq k + 1$  очевиден. Предположим, что  $n > k + 1$  и пусть  $C$  есть оптимальная (относительно меры  $\mu$ ) схема, вычисляющая  $f$ . Мы показываем, что можно присвоить значение одной из переменных таким образом, что  $\mu$  уменьшится хотя бы на 6. Поскольку получившаяся подфункция принадлежит  $S_{k,d}^{n-1}$ , то необходимое неравенство выполняется по предположению индукции. Заметим, что получившаяся функция не является константой. Таким образом, если гейт становится константой в результате подстановки, то этот гейт не является выходом схемы, и хотя бы один его потомок тоже удаляется.

Пусть  $Q$  есть топ-гейт схемы  $C$ , а  $x_i$  и  $x_j$  суть входящие в него переменные. Поскольку при подстановке значений этим переменным получается хотя бы три различных подфункции, то хотя бы одна из этих переменных должна входить хотя бы ещё в один гейт. Не умаляя общности, мы считаем, что  $x_i$  входит также в гейт  $P \neq Q$ . Если и  $P$  и  $Q$  являются гейтами типа- $\oplus$ , то мы просто присваиваем значение переменной  $x_i$ . При этом  $\mu$  уменьшается хотя бы на 6. Если один из гейтов  $P$  и  $Q$  есть гейт типа- $\wedge$ , то мы присваиваем  $x_i$  значение, которое делает этот гейт тривиальным. Таким образом, удаляются оба гейта  $P$  и  $Q$  и хотя бы один из их потомков (даже в случае, если  $Q$  есть рассматриваемый гейт типа- $\wedge$  и  $P$  является его единственным потомком, то мы удаляем  $Q$ ,  $P$  и всех потомков  $P$ ). На рис. 1 показано несколько возможных случаев (заметим, что здесь так же, как и в следующем разделе, показаны только типы гейтов, а не конкретные функции, которые в них вычисляются). Легко видеть, что  $\mu$  снова уменьшается хотя бы на 6.  $\square$

**Лемма 3.2.** Для любой  $f \in S_{k,d}^n$ ,  $C(f) \geq 7n/3 - c(k, d)$ .

*Доказательство.* Число гейтов в схеме  $C$  равно  $X(C) + A(C)$ . Необходимое неравенство следует из следующих двух неравенств:

$$\begin{aligned} 3X(C) + 2A(C) &\geq 6n - 6(k + 1), \\ A(C) &\geq n - (d + 1). \end{aligned}$$

$\square$

Замечая, что  $\text{GMOD}_p^n \subseteq S_{p^2,p}^n$  мы получаем необходимую нижнюю оценку.

**Следствие 3.3.** Для любой  $f \in \text{GMOD}_p^n$ ,  $C(f) \geq 7n/3 - O(1)$ .

## 4 Нижняя оценка $2.5n$ для $\text{GMOD}_3^n$

Вначале мы определяем класс  $T_k^n$ , который аналогичен классу  $S_{k,d}^n$ .

**Определение 4.1.** Пусть  $T_k^n$  — это класс всех функций  $f \in B_n$ , обладающих следующими свойствами:

1. если  $n \geq k$ , то для любых двух переменных  $x_i$  и  $x_j$  получается хотя бы три различных подфункции  $f$  при присваивании значений  $x_i$  и  $x_j$ ;
2. если  $n \geq k$ , то для любой переменной  $x_i$  и для любой константы  $c \in \{0, 1\}$ ,  $f|_{x_i=c} \in T_k^{n-1}$ ;
3. если  $n \geq k$ , то для любых двух переменных  $x_i$  и  $x_j$  существует константа  $c \in \{0, 1\}$  такая, что  $f|_{x_i=x_j \oplus c} \in T_k^{n-1}$  и  $f|_{x_i=x_j \oplus c \oplus 1} \in T_k^{n-2}$ , то есть последняя подфункция не зависит ни от  $x_i$ , ни от  $x_j$ .

**Теорема 4.1.** Для любой схемы  $C$ , вычисляющей функцию  $f \in T_k^n$ ,

$$C(f) \geq 2.5n - 2.5(k + 2).$$

Перед доказательством теоремы мы определяем понятие хог-цепи, которое было впервые введено Полом [9]. Для гейта  $G_0$  схемы  $C$  мы говорим, что существует хог-цепь длины  $k$  в  $G_0$  тогда и только тогда, когда есть  $k$  гейтов  $G_1, \dots, G_k$  в  $C$  таких, что

1. для  $1 \leq i \leq k$ ,  $G_i$  является гейтом типа- $\oplus$ ;
2. для  $1 \leq i \leq k$ ,  $G_i$  является единственным потомком  $G_{i-1}$ ;
3. в  $G_k$  нет хог-цепи, то есть  $G_k$  либо является выходом  $C$ , либо имеет исходящую степень 2, либо его единственный потомок является гейтом типа- $\wedge$ .

*Доказательство.* Доказательство снова проводится индукцией по  $n$ . Для  $n \leq k+2$  утверждение верно. Пусть теперь  $n > k+2$ . Мы либо удалим три гейта и получим подфункцию из  $T_k^{n-1}$ , либо же удалим пять гейтов и получим подфункцию из  $T_k^{n-2}$ .

Рассмотрим оптимальную схему  $C$ , вычисляющую функцию  $f$ .

**Случай 1.**  $C$  содержит переменную исходящей степени хотя бы 3. Присваивая ей константу, получаем функцию в  $T_k^{n-1}$  и удаляем хотя бы три гейта.

**Случай 2.**  $C$  содержит переменную исходящей степени 2, которая имеет потомка типа- $\wedge$ . Присваиваем этой переменной константу, которая делает потомка типа- $\wedge$  тривиальным. Легко видеть, что при этом удаляется хотя бы три гейта.

**Случай 3.** Каждая переменная в  $C$  имеет либо исходящую степень 1, либо исходящую степень 2. Рассмотрим топ-гейт  $Q$  схемы  $C$  и входящие в него переменные  $x_i$  и  $x_j$ . Хотя бы одна из переменных  $x_i$  и  $x_j$  должна входить в какой-то другой гейт, поскольку в противном случае присваиванием значений этим переменным можно получить не более двух различных подфункций. Не умаляя общности мы предполагаем, что  $x_i$  входит в гейт  $P$ . Тогда оба гейта  $P$  и  $Q$  должны быть типа- $\oplus$  (иначе применим случай 2). Таким образом, любой топ-гейт схемы  $C$  является гейтом типа- $\oplus$ .

**Случай 3.1.** Гейт  $Q$  имеет исходящую степень хотя бы 2. В таком случае мы заменяем  $x_i$  на  $x_j \oplus c$ , подбирая константу  $c$  таким образом, чтобы получившаяся подфункция принадлежала  $T_k^{n-1}$ . В результате удаляется гейт  $Q$  и все его потомки, то есть хотя бы три гейта.

**Случай 3.2.** Гейт  $Q$  имеет исходящую степень 1. Предположим, что исходящая степень  $x_j$  также равна 2, в противном случае анализ только упрощается, см. рис. 2.

Сначала мы заменяем  $x_j$  на  $x_i \oplus c$  таким образом, чтобы получившаяся подфункция принадлежала  $T_k^{n-2}$ . Получившаяся подфункция не зависит ни от  $x_i$ , ни от  $x_j$ , однако схема всё ещё содержит переменную  $x_i$ . Это означает, что  $x_i$  можно заменить на любую функцию, не зависящую от  $x_i$ . После замены  $x_j = x_i \oplus c$  переменная  $x_i$  входит в два гейта типа- $\oplus$  (в случае, если  $x_j$  имеет исходящую степень 1 в исходной схеме,  $x_i$  будет входить только в один гейт в получившейся схеме). Обозначим

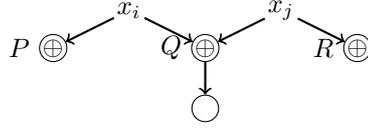


Рис. 2: Главный случай в доказательстве Теоремы 4.1.

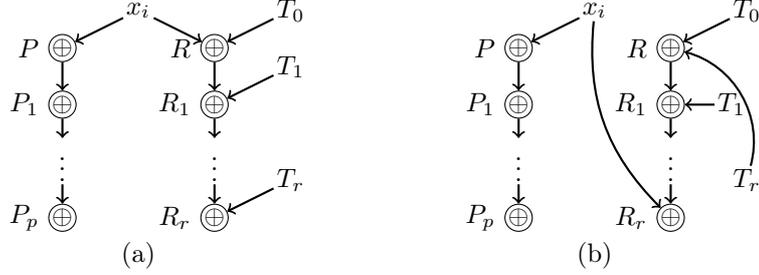


Рис. 3: Удаление хог-цепи.

эти два гейта через  $P$  и  $Q$  и рассмотрим хог-цепи  $P_1, \dots, P_p$  и  $R_1, \dots, R_r$ , начинающиеся в  $P$  и  $R$  соответственно ( $p$  и  $r$  могут быть равны нулю), см. рис. 3(a). Не умаляя общности мы предполагаем, что не существует пути из  $P_p$  в  $R_r$ . Это означает отсутствие пути из  $x_i$  в  $T_k$  ( $0 \leq k \leq r$ ). Действительно, любой путь из  $x_i$  должен проходить через  $P_p$  или через  $R_r$ . Однако наличие пути из  $x_i$  в  $T_k$  через  $R_r$  привело бы к существованию цикла в схеме, в то время как путь через  $P_p$  мог бы быть продолжен до  $R_r$ , что противоречит нашему исходному предположению.

Тогда мы перестраиваем схему как показано на рис. 3(b) и затем заменяем  $x_i$  на функцию, которая вычисляется на другом входе  $R_r$ , или её отрицание. Как показано выше, эта функция не зависит от  $x_i$ . Поскольку в перестроенной схеме нет хог-цепи в  $R_r$  (это означает, что либо исходящая степень  $R_r$  равна хотя бы двум, либо единственный потомок  $R_r$  это гейт типа- $\wedge$ ), то хотя бы три гейта будут удалены.

Если исходящая степень  $x_j$  равна 1, то после подстановки  $x_j$  значения  $x_i \oplus c$  исходящая степень  $x_i$  становится равна 1. Тогда мы удаляем хог-цепь в этом гейте и затем заменяем  $x_i$  на функцию, которая вычисляется в другом входе этого гейта. Эта функция не зависит от  $x_i$ , так что подстановка корректна.  $\square$

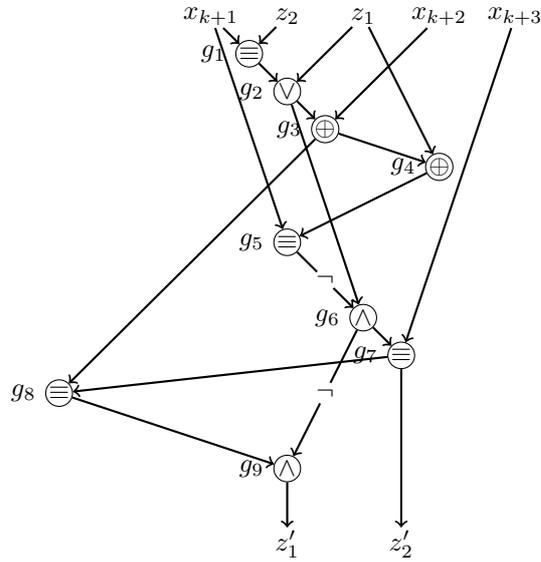
Легко показать, что  $\text{GMOD}_3^n \subseteq T_9^n$ , из чего получаем следующее следствие.

**Следствие 4.2.** Для любой  $f \in \text{GMOD}_3^n$ ,  $C(f) \geq 2.5n - c$ .

## 5 Верхняя оценка $3n$ для $\text{GMOD}_3^n$

В этом разделе мы представляем конструкцию, из которой следует верхняя оценка  $3n + O(1)$  для  $\text{GMOD}_3^n$ . Основной блок (а также его таблица истинности), из которого строится схема размера  $3n + O(1)$ , показан на рис. 4. Блок принимает на вход три новых переменных  $x_{k+1}, x_{k+2}, x_{k+3}$  и значение  $\sum_{i=1}^k x_i \pmod{3}$ , закодированное двумя битами  $(z_1, z_2)$  следующим образом:

$$\sum_{i=1}^k x_i \pmod{3} = \begin{cases} 0, & \text{если } (z_1, z_2) = (0, 0), \\ 1, & \text{если } (z_1, z_2) = (0, 1), \\ 2, & \text{если } z_1 = 1. \end{cases}$$



$x_{k+1}$	0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
$x_{k+2}$	0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
$x_{k+3}$	0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1
$z_1$	0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1
$z_2$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
$g_1$	1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
$g_2$	1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 1 1
$g_3$	1 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 1 1 0 0 1 1 0 1 1 0 0 1 1 0 0 1 1 0 0
$g_4$	1 0 0 1 1 0 0 1 0 0 1 1 1 0 0 1 1 0 1 1 0 0 1 1 0 0 0 1 1 0 0 1 1 0 0 1 1
$g_5$	0 0 1 1 0 0 1 1 1 0 0 1 1 0 0 1 1 1 0 0 1 1 0 0 1 1 0 0 1 0 0 1 1 0 0 1 1
$g_6$	1 0 0 0 1 0 0 0 0 1 1 0 0 1 1 0 0 0 0 1 0 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0
$g_7$	0 1 1 1 1 0 0 0 1 0 0 1 0 1 1 1 0 1 1 1 0 0 0 0 1 1 0 0 1 0 1 1 1 0 1 1 0
$g_8$	0 0 0 1 1 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 1 1 1 0 0 0 1 0 1 0 0 1 0 1 0 1 0 1
$g_9$	0 0 0 1 0 1 1 1 0 1 0 0 0 0 0 0 1 0 1 1 1 0 1 0 0 0 1 0 0 0 0 0 0 0 1 0 0 1
$z'_1$	0 0 0 1 0 1 1 1 0 1 0 0 0 0 0 0 1 0 1 1 1 0 1 0 0 0 1 0 0 0 0 0 0 0 1 0 0 1
$z'_2$	0 1 1 1 1 0 0 0 1 0 0 1 0 1 1 1 0 1 1 1 0 0 0 0 1 1 0 0 1 0 1 1 1 0 1 1 0

Рис. 4: Индуктивный блок для MOD<sub>3</sub> и его таблица истинности.

Выходом блока является пара битов  $(z'_1, z'_2)$ , кодирующая значение  $\sum_{i=1}^{k+3} x_i \pmod{3}$ . Очевидно, что схема размера  $3n + O(1)$  для  $\text{MOD}_3^n$  может быть построена из таких блоков. Более того, так же получается схема размера  $3n + O(1)$  для  $\text{GMOD}_3^n$ . Для любой функции  $f \in \text{GMOD}_3^n$  существует разбиение множества индексов  $\{1, 2, \dots, n\}$  на два непересекающихся подмножества индексов  $I_1, I_2$  такое, что

$$f(x_1, \dots, x_n) = 1 \Leftrightarrow \sum_{i \in I_1} x_i + 2 \sum_{i \in I_2} x_i \equiv r \pmod{3}.$$

Легко видеть, что для такой функции можно построить схему размера  $3|I_1| + 3|I_2| + O(1)$ . Поскольку любой гейт типа- $\oplus$  может быть заменён тремя гейтами типа- $\wedge$ , то эта конструкция также даёт нам верхнюю оценку  $7n$  в базисе  $U_2$ . Интересное свойство показанной схемы для  $\text{GMOD}_3^n$  состоит в том, что она содержит  $n$  гейтов типа- $\wedge$ . Таким образом, нижняя оценка на число гейтов типа- $\wedge$ , приведённая в разд. 2, точна. Другое интересное свойство заключается в том, что примерно  $2n/3$  всех переменных, входящих в схему, имеют исходящую степень 1.

Для нахождения приведённого на рис. 4 блока были использованы SAT-солверы. Утверждение о существовании схемы, вычисляющей некоторую функцию и имеющей фиксированное число гейтов, было записано в виде формулы в КНФ. Для нахождения выполняющего набора для полученной формулы использовались SAT-солверы. Задача поиска схемы оказалась сложной для SAT-солверов даже при небольшом числе гейтов. Это связано с тем, что число различных схем как функция числа гейтов растёт очень быстро. Представленный блок был найден в результате долгих экспериментов с различными ограничениями на рассматриваемые схемы. В частности, накладывались следующие ограничения: а) существует путь, проходящий через все гейты блока; б) исходящая степень каждого гейта не превосходит 2.

## 6 Заключение и дальнейшие направления исследований

Самым естественным вопросом является нахождение точной схемной сложности  $\text{MOD}_3^n$ . Для этого необходимо улучшить либо верхнюю, либо нижнюю оценку. Один из способов улучшения нижней оценки  $2.5n$ , например, состоит в том, чтобы доказать, что  $5X(C) + 4A(C) \geq 12n$ . Из этого следует нижняя оценка  $2.6n$ . Заметим, что удаление пяти гейтов типа- $\oplus$  присваиванием значений двум переменным уменьшает такую меру на 25, удаляя при этом только 2.5 гейтов для каждой из удалённых переменных. Другими словами, эта мера учитывает тот факт, что случаи, в которых удаляются только гейты типа- $\oplus$ , оказываются хорошими, так как нам известно, что схема должна содержать примерно  $n$  гейтов типа- $\wedge$ . Одним из случаев, для которого мы в данный момент не можем гарантировать необходимое уменьшение меры сложности, является случай, когда хог большого числа переменных вычисляется в верхней части схемы. Конечно, можно использовать другие коэффициенты для  $X(C)$  и  $A(C)$ . Также можно пробовать использовать предложенную Цвиком [13] идею: ввести зависимость меры также от числа переменных в схеме с исходящей степенью 1 (однако необходимо заметить, что такая мера была использована Цвиком для базиса  $U_2$ ).

Несмотря на многочисленные эксперименты, нам не удалось найти индуктивный блок, дающий верхнюю оценку лучше, чем  $3n$  для  $\text{MOD}_3^n$ . Однако оптимальная схема вовсе не обязательно должна состоять из индуктивных блоков. Заметим также, что наш метод нахождения индуктивных блоков не работает для больших значений  $p$ , поскольку для того чтобы закодировать остаток в таком случае требуется большое число битов. Во многих случаях SAT-солверы не могли решить построенную нами формулу просто из-за её большого размера. Возможно, что наш метод сведения может быть существенно улучшен. Также было бы интересно реализовать эффективную программу для нахождения оптимальных схем без использования сведения к SAT. Как было сказано во введении, нам до сих пор неизвестно, как соотносятся между собой  $C(\text{MOD}_p^n)$  и  $C(\text{MOD}_q^n)$  для простых  $p < q$ . Интуитивно кажется, что  $\text{MOD}_p^n$  не сложнее чем  $\text{MOD}_q^n$ . Напомним также, что все симметрические функции могут быть вычислены схемами размера не более  $5n + o(n)$ . Аналогичный вопрос о глубине таких схем для таких функций был поставлен в [4]. Более простой вопрос может быть сформулирован так: правда ли, что все функции из  $\text{GMOD}_p^n$  имеют примерно одинаковую схемную сложность? То есть существует ли константа  $c = c(p)$  такая, что для любых двух функций  $f_1, f_2 \in \text{GMOD}_p^n$ ,  $|C(f_1) - C(f_2)| \leq c$ ?

## Благодарности

Мы хотели бы поблагодарить Эдуарда Алексеевича Гирша за ценные замечания.

## Список литературы

- [1] Валерий Михайлович Храпченко. О сложности реализации линейной функции в классе  $\Pi$ -схем. *Математические заметки*, 9(1):35–40, 1971.
- [2] Рошаль Габдулхаевич Нигматуллин. *Сложность булевых функций*. М., Наука, 1991.
- [3] Norbert Blum. A Boolean function requiring  $3n$  network size. *Theoretical Computer Science*, (28):337–345, 1984.
- [4] Andrew Chin. One the depth complexity of the counting functions. *Information Processing Letters*, 35:325–328, 1990.
- [5] Michael J. Fischer, Albert R. Meyer, and Michael S. Paterson.  $\Omega(n \log n)$  lower bounds on length of Boolean formulas. *SIAM Journal on Computing*, 11:416–427, 1982.
- [6] Kazuo. Iwama, Oded Lachish, Hiroki Morizumi, and Ran Raz. An explicit lower bound of  $5n - o(n)$  for boolean circuits. In *Proceedings of 33rd STOC*, pages 399–408, 2001.
- [7] Valerii M. Khrapchenko. Complexity of the realization of a linear function in the case of  $\Pi$ -circuits. *Math. Notes Acad. Sciences*, 9(1):35–40, 1971.
- [8] Michael S. Paterson and Uri Zwick. Shallow circuits and concise formulae for multiple addition and multiplication. *Computational Complexity*, 3:262–291, 1993.
- [9] Wolfgang J. Paul. A  $2.5n$ -lower bound on the combinational complexity of Boolean functions. *SIAM Journal of Computing*, 6(3):427–433, 1977.
- [10] Claus-Peter Schnorr. Zwei lineare untere Schranken für die Komplexität Boolescher Funktionen. *Computing*, 13:155–171, 1974.
- [11] Larry J. Stockmeyer. On the combinational complexity of certain symmetric Boolean functions. *Mathematical Systems Theory*, 10:323–336, 1977.
- [12] Dirk Cornelis van Leijenhorst. A note on the formula size of the “mod  $k$ ” functions. *Information Processing Letters*, 24:223–224, 1987.
- [13] Uri Zwick. A  $4n$  lower bound on the combinational complexity of certain symmetric boolean functions over the basis of unate dyadic Boolean functions. *SIAM Journal on Computing*, 20:499–505, 1991.