Московский Государственный Университет
им. М.В. Ломоносова
Российская Академия Наук
Академия Технологических Наук России
Российская Академия Естественных Наук

Интеллектуальные Системы.

Теория и приложения

ТОМ **21** ВЫПУСК **1** * **2017**

МОСКВА

ISSN 2411–4448

УДК 519.95; 007:159.955
ББК 32.81

Издается с 1996 г.*

В журнале «Интеллектуальные системы. Теория и приложения» публикуются научные достижения в области теории и приложений интеллектуальных систем, новых информационных технологий и компьютерных наук.

Издание журнала осуществляется под эгидой МГУ им. М. В. Ломоносова, Научного Совета по комплексной проблеме «Кибернетика» РАН, Отделения «Математическое моделирование технологических процессов» АТН РФ, Секции «Информатики и кибернетики» РАЕН.

В издании журнала участвуют: механико-математический факультет МГУ, кафедра МаТИС МГУ, МИРЭА, МНЦ КИТ.

Учредитель журнала: ООО «Интеллектуальные системы».

Журнал входит в список изданий, включенных ВАК РФ в реестр публикаций материалов по кандидатским и докторским диссертациям по математике и механике.

Спонсором издания является:

ООО «Два Облака»

Разработка корпоративных информационных систем
http://www.dvaoblaka.ru

Индекс подписки на журнал: 64559 в каталоге НТИ «Роспечать».

Адрес редакции: 119899, Россия, Москва, Воробьевы Горы, МГУ, ГЗ, механико-математический факультет, комн. 12-01.
Адрес издателя: 115230, Россия, Москва, Хлебозаводский проезд, д. 7, стр. 9, офис 9. Тел. +7 (495) 939-46-37, e-mail: mail@intsysjournal.org

*) Прежнее название журнала: «Интеллектуальные системы».

ОГЛАВЛЕНИЕ

Порядковое представление распределения меры возможности

Д. А. Балакин

В статье исследуется представление упорядоченности возможностей [1] элементарных событий, с точностью до изоморфизма задающее меру возможности, матрицами и функциями попарных сравнений значений возможностей, его свойства и операции над такими представлениями, в частности маргинализация совместного распределения, расчет условного распределения по совместному, экспертное восстановление распределения и принятие оптимальных решений.

Ключевые слова: частичный порядок, конечное множество, восстановление порядка, сортировка, сравнение.

Введение

В первом варианте теории возможностей [1] мера возможности принимает значения в шкале $\mathcal{L} = ([0,1], \leqslant, +, \times)$, определенной как отрезок $[0,1]$ с естественной упорядоченностью $\leqslant$ и операциями $+ : [0,1]^2 \to [0,1] : a + b \stackrel{\text{def}}{=} \max\{a,b\}$ и $\times : [0,1]^2 \to [0,1] : a \times b \stackrel{\text{def}}{=} \min\{a,b\}$. Группа автоморфизмов $\mathcal{L}$ порождается группой Γ строго монотонных непрерывных функций $\gamma(\cdot) : [0,1] \to [0,1]$, $\gamma(0) = 0$, $\gamma(1) = 1$, сохраняющих упорядоченность $\leqslant$, с композицией «$\circ$» в качестве групповой операции. Это означает, что $\forall \gamma \in \Gamma\ \gamma[0,1] = [0,1]$, $\forall\, a, b \in [0,1]\ \gamma(a * b) = \gamma(a) * \gamma(b)$, где $*$ — символ любой из бинарных операций: сложения $+$ и умножения $\times$, и для бинарных отношений $a \leqslant b \Leftrightarrow \gamma(a) \leqslant \gamma(b)$. [1] Каждый автоморфизм $\gamma : \mathcal{L} \to \mathcal{L}$ определяет изоморфизм $\gamma : \mathcal{L} \to \gamma\mathcal{L}$ следующим образом: $\forall a \in \mathcal{L}\ \forall \gamma \in \Gamma\ a \mapsto \gamma(a) \in \gamma\mathcal{L}$, $a + b \mapsto \gamma(a + b) = \gamma(a) + \gamma(b)$, $a \times b \mapsto \gamma(a \times b) = \gamma(a) \times \gamma(b)$, $a \leqslant b \Leftrightarrow \gamma(a) \leqslant \gamma(b)$, $a, b \in \mathcal{L}$. Обозначим

[1] Из этого и требований непрерывности операций $* : [0,1]^2 \to [0,1]$, коммутативности $*$ и свойств 0 и 1: $a + 0 = a \times 1 = a$, $a \in [0,1]$ следуют равенства $a + b = \max\{a,b\}$, $a \times b = \min\{a,b\}$, $a, b \in [0,1]$ [1].

$\gamma\mathcal{L}$, $\gamma \in \overline{\Gamma}$, где $\overline{\Gamma}$ — группа изоморфизмов, отвечающая группе Γ, шкалу, изоморфную шкале $\mathcal{L}$ и назовём её «координатным представлением» шкалы $\mathcal{L}$. Будучи сформулированными в некоторых шкалах (координатных представлениях) $\mathcal{L}'$ и $\mathcal{L}''$, модели считаются эквивалентными, если существует шкала $\mathcal{L} = \gamma'\mathcal{L}' = \gamma''\mathcal{L}''$, $\gamma', \gamma'' \in \overline{\Gamma}$, в которой их формулировки совпадают, а содержательно истолкованы могут быть только те модели, формулировки которых не зависят от выбора (координатного представления) шкалы $\mathcal{L}$ и, следовательно, их содержание одинаково для любых исследователей, для которых координатные представления играют роль «систем отсчета».

Таким образом, с точки зрения содержательной интерпретации существенна только упорядоченность различных значений возможности, сохраняющаяся при любом непрерывном изотонном отображении шкалы значений возможности на себя, а не сами эти значения. Поэтому представляет интерес инвариантное относительно выбора шкалы значений возможности представление возможности $\mathrm{P} : \mathcal{X} \to \mathcal{L}$. Такое представление особенно полезно при построении совокупной оценки возможности по распределениям возможностей, полученным из различных источников и потому, возможно, принимающим значения в различным шкалах.

Порядковые представления меры

Идея представления неопределенности с помощью отношения над множеством событий восходит к работам [2, 3], авторы которых искали порядковый вариант вероятности (успешно — в том смысле, что существует необходимое условие того, что некоторая упорядоченность есть упорядоченность по вероятности, безуспешно — в том смысле, что это условие не является достаточным, см. далее).

Рассматриваемое в [4] порядковое представление неопределенности есть (частичный, если некоторые события несравнимы) предпорядок $\leqslant_\mu$ на множестве $\mathcal{X}$ событий — подмножеств множества элементарных событий X, обладающий следующими свойствами:

1. Рефлексивность: $\forall A \in \mathcal{X}\ A \leqslant_\mu A$,
2. Нетривиальность: $\varnothing \leqslant_\mu X$,
3. Соответствие логическому выводу:

$$\forall A, B \in \mathcal{X}\ A \subset B \Rightarrow A \leqslant_\mu B \tag{1}$$

и $\forall A, B, C, D \in \mathcal{X}\ D \subset A \Rightarrow C \leqslant_\mu B$,

4. Транзитивность: $\forall A, B, C \in \mathcal{X}$ если $A \leqslant_\mu B$ и $B \leqslant_\mu C$, то $A \leqslant_\mu C$.

Такой предпорядок определяется некоторой нечеткой (в смысле Сугэно) мерой μ, если $\forall A, B \in \mathcal{X}\ A \leqslant_\mu B \iff \mu(A) \leqslant \mu(B)$. Многие меры, используемые для моделирования неопределенности, удовлетворяют условиям 1.–4. В частности, сравнительные вероятности, введенные в [2] и подробно изученные в контексте принятия решений в [5] являются также линейными упорядоченностями и обладают свойством $\forall A, B, C \in \mathcal{X} : A \cap (B \cup C) = \varnothing\ B \leqslant_\mu C \iff A \cup B \leqslant_\mu A \cup C$, но не любое такое соотношение соответствует хотя бы одной вероятности, и оно не описывается своим сужением на одноточечные множества.

Последним свойством (упорядоченность по мере описывает меру с точностью до изоморфизма), как показано в [4], обладают упорядоченности по возможности $\leqslant_{\mathrm{P}}$ и по необходимости $\leqslant_{\mathrm{N}}$. Они также являются линейными и имеют характерные свойства

$$\forall A, B, C \in \mathcal{X}\ (A \leqslant_{\mathrm{P}} B \& A \leqslant_{\mathrm{P}} C) \Rightarrow A \cup C \leqslant_{\mathrm{P}} B \cup C \tag{2}$$

для упорядоченности по возможности,

$$\forall A, B, C \in \mathcal{X}\ (A \leqslant_{\mathrm{N}} B \& A \leqslant_{\mathrm{N}} C) \Rightarrow A \cap C \leqslant_{\mathrm{N}} B \cap C$$

для упорядоченности по необходимости.

Как показано в [6], свойств 1, 2 и линейности упорядоченности на шкале значений возможности достаточно для того, чтобы однозначно определить упорядоченность возможностей любых множеств $A, B \in \mathcal{X}$, пользуясь только упорядоченностью возможностей элементарных событий: $\mathrm{P}(A) \leqslant \mathrm{P}(B) \iff \forall x_1 \in A\ \exists x_2 \in B : \mathrm{P}(\{x_1\}) \leqslant \mathrm{P}(\{x_2\})$. Поэтому в данной статье рассматриваются упорядоченности по распределениям мер возможности.

В [4] также рассмотрено соответствие между различными модификациями условия 2 и свойствами соответствующих им мер. В [7], ее расширенном варианте [8] и в [9] рассмотрен более общий случай упорядоченности при выполнении только условия 1.

Способы представления бинарных отношений (в частности, матрицами) и соответствие свойств отношений свойствам представляющих их матриц описаны в [10] и применительно к отношениям, описывающим предпочтения, в [11].

Случай конечного множества элементарных событий

Определение 1 ([1]). *Пусть* $(\Omega, \mathcal{B}, \mathrm{P}_\Omega)$ *— пространство с возможностью,* $(X, \mathcal{A})$ *— измеримое пространство,* $\mathcal{A}$ *— σ-алгебра подмножеств* X *и задана функция* $q : Y \to X$*, такая, что* $\forall A \in \mathcal{A}\ q^{-1}(A) \stackrel{def}{=} \{y \in Y, q(y) \in A\} \in \mathcal{B}$*. Функция* q *называется* $(\mathcal{B}, \mathcal{A})$*-измеримой и* задает нечеткий элемент ξ*, определенный на* $(\Omega, \mathcal{B}, \mathrm{P}_\Omega)$ *и принимающий значения в* $(X, \mathcal{A})$*. Нечеткий элемент* ξ определяет *на* $(X, \mathcal{A})$ возможность P^ξ*:* $\mathrm{P}^\xi(\xi \in A) = \mathrm{P}_\Omega(q^{-1}(A))$*,* $A \in \mathcal{A}$*, и поэтому называется* каноническим *для пространства с возможностью* $(X, \mathcal{A}, \mathrm{P}^\xi)$*.*

Определим функцию g^ξ*:* $X \to \mathcal{L}$*:* $g^\xi(x) = \mathrm{P}^\xi(\xi = x) = \mathrm{P}_\Omega(q^{-1}(\{x\}))$*,* $x \in X$*, называемую* распределением возможностей значений нечеткого элемента ξ, или короче — распределением нечеткого элемента ξ.

Как известно [1, §2.5.1, 3.9], [12], для нечеткого элемента ξ, принимающего конечное число значений $\{x_1, x_2, \ldots, x_n\}$, упорядоченность возможностей элементарных событий $p_j = \mathrm{P}(\{x_j\})$, $j = 1, \ldots, n$, и возможности пустого множества, по определению равной 0, может быть задана матрицей G^ξ размера $(n+1) \times (n+1)$, где

$$G^\xi_{ij} = \begin{cases} 1, \text{ если } p_i \leqslant p_j, \\ 0, \text{ если } p_i > p_j, \end{cases} \quad p_{n+1} = 0, i, j = 1, \ldots, n+1.$$

Пусть значения матричных элементов рассматриваются как принадлежащие шкале значений возможности, $\mathcal{L}$, и определены операции сложения $+$ для матриц одинакового размера как поэлементного max: $(A + B)_{ij} \stackrel{\text{def}}{=} \max\{A_{ij}, B_{ij}\}$, умножения $\times$, аналогичному обычному матричному умножению: если A — матрица $m \times n$, B — матрица $n \times q$, то $(A \times B)_{ij} = \max\limits_{k=1,\ldots,n} \min\{A_{ik}, B_{kj}\}$, $A \times B$ — матрица размера $m \times q$, отрицания $\overline{\ }$ как поэлементной замены 0 на 1 и наоборот: $\overline{A}_{ij} = \begin{cases} 1, A_{ij} = 0, \\ 0, A_{ij} = 1. \end{cases}$

В этих обозначениях матрица G, все элементы которой 0 или 1, описывает нечеткий элемент тогда и только тогда, когда:

$$G + G^T = E, \tag{3.1}$$

$$G + \overline{G \times G} = E, \tag{3.2}$$

$$\min_{i=1,\ldots,n} G_{i,n+1} = 0, \tag{3.3}$$

$$\min_{j=1,\dots,n} G_{n+1,j} = 1 \tag{3.4}$$

(требования полноты, транзитивности, существования хотя бы одного элементарного события с ненулевой возможностью и неотрицательности всех значений возможности, соответственно), где E — матрица, все элементы которой равны 1, G^T — транспонированная матрица G.

Доказательство.
Необходимость

1. Полнота (3.1): для любых $i, j = 1, \dots, n+1$ $p_i \leqslant p_j$ и/или $p_j \leqslant p_i$, поэтому $G_{ij} = 1$ и/или $G_{ji} = G_{ij}^T = 1$, т. е. $G_{ij} + G_{ij}^T = 1$.

2. Транзитивность (3.2): для любых $i, j = 1, \dots, n+1$ в силу линейности упорядоченности значений возможности $p_i \leqslant p_j$ или $p_j \leqslant p_i$, то есть $\max\{G_{ij}, G_{ji}\} = 1$ и по определению транзитивности если существует такое $k = 1, \dots, n+1$, что $p_i \leqslant p_k$ и $p_k \leqslant p_j$, то $p_i \leqslant p_j$, то есть $(\exists k = 1, \dots, n+1 : \min\{G_{ik}, G_{kj}\} = 1) \to G_{ij} = 1$, что эквивалентно $\max\{\overline{\max\{\min\{G_{ik}, G_{kj}\} | k = 1, \dots, n+1\}}, G_{ij}\} = 1$.

3. Существование хотя бы одного ненулевого значения (3.3): существует хотя бы одно $i = 1, \dots, n$, для которого $p_i > 0 = p_{n+1}$ (поскольку $\sup\limits_{i=1,\dots,n} p_i = 1$ по условию нормировки). Следовательно, для всех таких i $G_{i,n+1} = 0$, и поэтому $\min\limits_{i=1,\dots,n} G_{i,n+1} = 0$.

4. Неотрицательность (3.4): для всех $j = 1, \dots, n$ $p_j \geqslant 0 = p_{n+1}$, что эквивалентно $G_{n+1,j} = 1$ и, следовательно, $\min\limits_{j=1,\dots,n} G_{n+1,j} = 1$.

Достаточность

1. Полнота: если существуют такие $i, j = 1, \dots, n+1$, что $G_{ij} + G_{ij}^T = 0$, то $G_{ij} = G_{ji} = 0$ и, следовательно, одновременно $p_i < p_j$ и $p_j < p_i$, что невозможно при полноте упорядоченности.

2. Транзитивность: если существуют такие $i, j = 1, \dots, n+1$, что $\max\{\overline{\max\{\min\{G_{ik}, G_{kj}\} | k = 1, \dots, n+1\}}, G_{ij}\} = 0$, то $G_{ij} = 0$ и $\max\{\min\{G_{ik}, G_{kj}\} | k = 1, \dots, n+1\} = 1$, т. е. $G_{ij} = 0$ и $\exists k = 1, \dots, n+1$: $\min\{G_{ik}, G_{kj}\} = 1$, что эквивалентно одновременной истинности при некотором $k = 1, \dots, n+1$ $G_{ij} = 0$, $G_{ik} = G_{kj} = 1$, т. е. $p_i > p_j$, $p_i \leqslant p_k \leqslant p_j$, что невозможно при транзитивности упорядоченности.

3. Существование хотя бы одного ненулевого значения: если $\min\limits_{i=1,\dots,n} G_{i,n+1} = 0$, то для всех $i = 1, \dots, n$, для которых $G_{i,n+1} =$, $p_i > 0$.

4. Неотрицательность: если $\min\limits_{j=1,\dots,n} G_{n+1,j} = 1$, то $\forall i = 1, \dots, n\ p_i \geqslant p_{n+1} = 0$.

■

В частности, из условий (3.1) и (3.2) следует отсутствие циклов (исключая, разумеется, циклы из элементарных событий с одинаковой возможностью), поскольку из (3.1) и (3.2) следует то, что упорядоченность множества $\{1, \dots, n+1\}$, факторизованного по отношению эквивалентности $i \sim j \iff p_i = p_j$, определённая матрицей G, является линейной.

Замечание. Поскольку $\forall x, y \geqslant 1\ x+y \geqslant 1$, $x+0 \geqslant 1$, $x \cdot y \geqslant 1$, $x \cdot 0 = 0$, где $+$ и $\cdot$ — символы обычного сложения и умножения, то при доопределении $\overline{x} = \begin{cases} 1, x = 0, \\ 0, x \geqslant 1, \end{cases}$ $x \in [0, +\infty)$, и замены равенства «$x = 1$» на неравенство «$x \geqslant 1$» и т.п. вместо описанных выше операций (реализованных, например, в пакете NumPy для булевых матриц) могут использоваться обычные матричные сложение и умножение. Однако вычисление $A \times B$ может, вообще говоря, быть быстрее вычисления результата обычного матричного умножения AB, поскольку, в частности, если для некоторого k $\min\{A_{ik}, B_{kj}\} = 1$, максимум по k уже достигнут. Алгоритм умножения для квадратных бинарных матриц $n \times n$, имеющий среднюю сложность $O(n^2)$, описан в статье [13].

Теорема 1. *Если $\eta = f(\xi)$ — нечеткий элемент — функция ξ, принимающий значения из $Y = \{y_1, \dots, y_m\}$, то матрица G^η, задающая с точностью до изоморфизма распределение возможностей его значений, может быть вычислена по формуле*

$$G^\eta = \overline{\Phi^T \times \overline{G^\xi \times \Phi}}, \tag{4}$$

где матрица Φ определена равенствами $\Phi_{ij} = \begin{cases} 1, f(x_i) = y_j, \\ 0, f(x_i) \neq y_j, \end{cases}$ $i = 1, \dots, n$, $j = 1, \dots, m$, $\Phi_{n+1,j} = 1$, $j = 1, \dots, m+1$, $\Phi_{i,m+1} = 0$, $i = 1, \dots, n$.

Доказательство. Пусть $g^\xi : X \to \mathcal{L}$ и $g^\eta : X \to \mathcal{L}$ — распределения нечетких элементов ξ и η, соответственно. При $i, j \leqslant m$ $g^\eta(y_i) \leqslant$

$g^\eta(y_j) \iff \max\{g^\xi(x_k)|k = 1,\dots,n, f(x_k) = y_i\} \leqslant \max\{g^\xi(x_l)|l = 1,\dots,n, f(x_l) = y_j\}$, что эквивалентно тому, что для любого $k \in \{1,\dots,n\}$ такого, что $f(x_k) = y_i$ существует такое $l \in \{1,\dots,n\}$, что $f(x_l) \leqslant y_j$ и $g^\xi(x_k) \leqslant g^\xi(x_l))$, то есть $G^\eta_{ij} = 1$ тогда и только тогда, когда $\forall k \in \{1,\dots,n+1\}(\Phi_{ki} = 1) \to (\exists l \in \{1,\dots,n+1\} : \Phi_{lj} = 1, G^\xi_{kl} = 1)$, где $\to$ — импликация. Но $\exists l \in \{1,\dots,n+1\} : \Phi_{lj} = 1, G^\xi_{kl} = 1$ тогда и только тогда, когда $\max\limits_{l=1,\dots,n+1} \min\{\Phi_{lj}, G^\xi_{kl}\} = (G^\xi \times \Phi)_{kj} = 1$. Аналогично, $\forall k \in \{1,\dots,n\}(\Phi_{ki} = 1) \to ((G^\xi \times \Phi)_{kj} = 1)$ тогда и только тогда, когда $\min\limits_{k=1,\dots,n} \max\{\overline{\Phi_{ki}}, (G^\xi \times \Phi)_{kj}\} = 1$. С учетом двойственности max и min это может быть записано в виде $\max\limits_{k=1,\dots,n} \min\{\Phi_{ki}, \overline{(G^\xi \times \Phi)_{kj}}\} = 0$, то есть $G^\eta_{ij} = (\overline{\Phi^T \times \overline{G^\xi \times \Phi}})_{ij}$, $i, j = 1,\dots,m$.

При $i \leqslant m$ $G^\eta_{i,m+1} = 1 \iff g^\eta(y_i) = 0 \iff \forall k \in \{1,\dots,n+1\}(\Phi_{ki} = 1) \to (G^\xi_{k,n+1} = 1)$, то есть $G^\eta_{i,m+1} = \overline{\max\limits_{k=1,\dots,n+1} \min\{\Phi^T_{ik}, \overline{G^\xi_{k,n+1}}\}}$. В силу определения Φ $G^\xi_{k,n+1} = = \max\limits_{k=1,\dots,n+1} \min\{G^\xi_{kl}, \Phi_{l,m+1}\}$ и потому $G^\eta_{i,m+1} = (\overline{\Phi^T \times \overline{G^\xi \times \Phi}})_{i,m+1}$, $i = 1,\dots,m$.

При $j \leqslant m+1$ $G^\eta_{m+1,j} = 1$ в силу неотрицательности возможности. С другой стороны, $\max\limits_{k=1,\dots,n+1} \min\{G^\xi_{n+1,k}, \Phi_{kj}\} = 1$ и потому $G^\eta_{m+1,j} = (\overline{\Phi^T \times \overline{G^\xi \times \Phi}})_{m+1,j}$, $j = 1,\dots,m+1$. ■

Для инвариантного описания совместного распределения может быть использована аналогичная конструкция, но с двойным индексированием по каждому нечеткому элементу. Например, пусть $G^{\xi,\eta}$ описывает совместное распределение нечетких элементов ξ и η, принимающих значения $\{x_1, x_2, \dots, x_n\}$ и $\{y_1,\dots,y_m\}$, соответственно, то есть $G^{\xi,\eta}_{ijkl} = \begin{cases} 1, p_{ij} \leqslant p_{kl}, \\ 0, p_{ij} > p_{kl}, \end{cases}$ $p_{n+1,j} = p_{i,m+1} = 0, i, k = 1,\dots,n+1, j, l = 1,\dots,m+1$, тогда матрица G^ξ, описывающая маргинальное распределение нечеткого элемента ξ, определяется равенствами

$$G^\xi_{pq} = \overline{\max_{\substack{i=1,\dots,n+1,\\ j=1,\dots,m+1}} \min\{\Phi_{pi}, \overline{\max_{\substack{k=1,\dots,n+1,\\ l=1,\dots,m+1}} \min\{G^{\xi,\eta}_{ijkl}, \Phi_{kq}\}}\}},$$

где $\Phi_{ij} = \begin{cases} \delta_{ij}, & \text{если } \max\{i,j\} \leqslant n, \\ 0, & \text{если } \max\{i,j\} = n+1, \end{cases}$ и не зависит от индексов по η, что соответствует функции $f(x,y) = x$.

Матрица $G^{\xi|\eta=y_j}$, описывающая условное распределение нечеткого элемента ξ при условии $\eta = y_j$, определяется равенствами

$$G_{ik}^{\xi|\eta=y_j} = G_{ijkj}^{\xi,\eta}, i,k = 1,\ldots,n+1.$$

Замечание 1. Матриц $G^{\xi|\eta}$ и G^{η} недостаточно для восстановления $G^{\xi,\eta}$, поскольку ни соответствующая условному распределению $g^{\xi|\eta}$ матрица $G^{\xi|\eta}$, ни матрица G^{η} не содержат информации об том, как упорядочены различные значения $g^{\xi|\eta}$ по отношению к g^{η}.

Экспертное восстановление возможности

Примером ситуации, в которой необходимо рассматривать распределения возможностей, выраженные в различных шкалах, является построение коллективной экспертной оценки распределения возможностей значений нечеткого элемента, рассмотренное в [1, §3.9]. Эксперты оценивают возможности равенств нечеткого элемента ξ его значениям $\xi = x_1$, …, $\xi = x_n$ в своих шкалах, но, поскольку коллективное решение, представляющее мнения всех экспертов, должно быть инвариантным относительно выбора их шкал, для построения коллективной экспертизы каждому эксперту следует оценить максимальный инвариант распределения возможностей — упорядоченность значений возможностей элементарных событий по отношению друг к другу и к 0, причем предполагается, что оценка распределения, предложенная каждым экспертом, не зависит от мнения других экспертов.

Эта задача поиска коллективной оценки решается в [1, §3.9] с помощью поиска такой матрицы парных сравнений, для которой сумма расстояний от нее до матриц парных сравнений, предложенных экспертами, минимальна (медиана Кемени). В [12], где решается похожая задача, анализируются свойства метрик на матрицах отношений и показано, что при выполнении ряда естественных условий (аксиомы метрики, инвариантность к переобозначению элементарных событий, инвариантность к добавлению или отбрасыванию элементарных событий, об упорядоченности возможности которых по отношению к остальным эксперты согласны) и условию, по которому для любых двух матриц сравнений $G^{(1)}$ и $G^{(2)}$ $\rho(G^{(1)},G^{(2)}) = \rho(G^{(1)},G^{(3)}) + \rho(G^{(2)},G^{(3)})$, где $G^{(3)}$ — такая матрица сравнений, согласно которой $p_i < p_j$, $i,j = 1,\ldots,n+1$, если это

имеет место согласно $G^{(1)}$ или $G^{(2)}$, и $p_i = p_j$, если либо это имеет место согласно и $G^{(1)}$, и $G^{(2)}$, или согласно $G^{(1)}$ и $G^{(2)}$ p_i и p_j упорядочены противоположным образом (т.е. $\min\{G^{(1)}_{ij}, G^{(2)}_{ij}\} \leqslant G^{(3)} \leqslant \max\{G^{(1)}_{ij}, G^{(2)}_{ij}\}$, $i, j = 1, \ldots, n+1$), то удовлетворяющая этим условиям метрика ρ существует и с точностью до произвольного множителя, соответствующего масштабу, определяется равенством

$$\rho(G^{(1)}, G^{(2)}) = \sum_{i,j=1}^{n+1} |G^{(1)}_{ij} - G^{(2)}_{ij}|. \tag{5}$$

В (5) и далее в этом разделе сложение и вычитание понимаются в обычном смысле. Таким образом, матрица G для матриц сравнений $G^{(1)}, \ldots, G^{(K)}$, предложенных K экспертами, определяется как решение задачи

$$\sum_{k=1}^{K} \sum_{i,j=1}^{n+1} |G_{ij} - G^{(k)}_{ij}| \sim \min_{G}, \tag{6}$$

где матрица G должна удовлетворять условиям (3). Поскольку число булевых матриц размера $n+1 \times n+1$, $n \geqslant 1$, удовлетворяющих условиям (3), конечно и отлично от 0, то её решение всегда существует.

Задача (6) с ограничениями (3) может быть сведена к задаче булевского программирования с линейной целевой функцией и квадратичными и линейными ограничениями: пусть $U_{ij} = \sum\limits_{k=1}^{K} G^{(k)}_{ij}$, тогда $\sum\limits_{k=1}^{K} \rho(G, G^{(k)}) = \sum\limits_{i,j=1}^{n+1} (G_{ij}(K - U_{ij}) + (1 - G_{ij})U_{ij}) = \sum\limits_{i,j=1}^{n+1} G_{ij}(K - 2U_{ij}) + \sum\limits_{i,j=1}^{n+1} U_{ij}$. Ограничение на полноту соответствующей G упорядоченности (3.1) дает ограничения — линейные неравенства $\forall i, j = \overline{1, n+1}$ $G_{ij} + G_{ji} \geqslant 1$. Ограничение на транзитивность соответствующей G упорядоченности (3.2) дает ограничения — квадратичные неравенства $\forall i, j = \overline{1, n+1}$ $G^2_{ij} - G_{ij} \geqslant 0$. Условие существования хотя бы одного элементарного события с ненулевой возможностью (3.3) дает ограничение — линейное неравенство $\sum\limits_{i=1}^{n+1} G_{i,n+1} \leqslant n$. Условия неотрицательности возможностей (3.4) дают ограничения — линейные равенства $\forall j = \overline{1, n+1}$ $G_{n+1,j} = 1$. Таким образом, задача целочисленного программирования

имеет вид

$$\sum_{i,j=1}^{n+1} G_{ij}(K - 2U_{ij}) \sim \min_{\{G_{ij}\},i,j=\overline{1,n+1}},$$

при условиях

$$\begin{aligned}
\forall i,j = \overline{1,n+1} \qquad & G_{ij} \in \{0,1\},\\
\forall i,j = \overline{1,n+1} \qquad & G_{ij} + G_{ji} \geqslant 1,\\
\forall i,j = \overline{1,n+1} \quad & -G_{ij} + \sum_{k=1}^{n+1} G_{ik}G_{kj} \geqslant 0,\\
& \sum_{i=1}^{n+1} G_{i,n+1} \leqslant n,\\
\forall j = \overline{1,n+1} \qquad & G_{n+1,j} = 1.
\end{aligned}$$

В качестве характеристики качества результата может использоваться расстояние (5) от решения задачи (6) с условиями (3), до решения задачи (6) с частью условий (3), например, без условия транзитивности (3.2), приводящего к запрету циклов. (В этом случае задача может быть сведена к задаче булевского программирования с линейными ограничениями, см. [14].) Если это расстояние велико, т. е. добавление условия транзитивности (3.2) существенно изменяет решение, то экспертиза вызывает недоверие.

Другие способы проверки качества полученной таким образом коллективной экспертизы рассмотрены в [1, §3.9]. В частности, актуален вопрос об обнаружении некомпетентности или «сговора» экспертов. Для обнаружения подобных «дефектов» коллективной экспертизы можно воспользоваться *матрицей корреляции частных экспертных решений*, элементы которой определяются равенствами

$$< G^{(k)}, G^{(k')} >= \frac{(G^{(k)}, G^{(k')})_2}{\|G^{(k)}\|_2 \|G^{(k')}\|_2}, k, k' = 1, \ldots, K, \tag{7}$$

где $G^{(k)}$ — матрица, предложенная k-м (из K) экспертов, $(G^{(k)}, G^{(k')})_2 = \sum\limits_{i,j=1}^{n+1} (G_{ji}^{(k)} - G_{ij}^{(k)})(G_{ji}^{(k')} - G_{ij}^{(k')})$, $\|G^{(k)}\|_2 = \sqrt{(G^{(k)}, G^{(k)})_2}$. Очевидно, для любых $G^{(k)}$, $G^{(k')}$ $< G^{(k)}, G^{(k')} > \in [-1, 1]$, причем

1. $< G^{(k)}, G^{(k')} >= 1$, если $G^{(k)} = G^{(k')} = G$ (одинаковое упорядочение значений по возможности),

2. $< G^{(k)}, G^{(k')} >= -1$, если $G^{(k)} = G^{(k')T}$ (противоположное упорядочение значений по возможности),

причем в обоих случаях результаты экспертизы $G^{(k)}$ и $G^{(k')}$ экспертов «k» и «k'» вызывают подозрение. В случае, когда один эксперт оценивает, например, качество объекта на основе результатов анализа K его характеристик, и каждая матрица $G^{(k)}$ соответствует k-й характеристике, $k = 1, \ldots, K$, значения матрицы корреляции не могут быть интерпретированы подобным образом, но могут быть полезными для выявления взаимозависимости этих характеристик.

Случай произвольного множества элементарных событий

Пусть теперь нечеткий элемент ξ принимает значения, принадлежащие произвольному множеству X. В этом случае аналогом матрицы G^ξ будет функция $G^\xi : \overset{\circ}{X} \times \overset{\circ}{X} \to \{0, 1\}$, определяемая равенствами

$$G^\xi(x_1, x_2) = \begin{cases} 1, \text{ если } g^\xi(x_1) \leqslant g^\xi(x_2), \\ 0, \text{ если } g^\xi(x_1) > g^\xi(x_2), \end{cases} \quad x_1, x_2 \in \overset{\circ}{X},$$

где $\overset{\circ}{X} \overset{\text{def}}{=} X \cup \{\varnothing\}$, g^ξ — распределение возможностей нечеткого элемента ξ, доопределенное значением возможности пустого множества $g^\xi(\varnothing) = 0$. Эта функция является характеристической для графика бинарного отношения «иметь не большую возможность, чем» на $\overset{\circ}{X} \times \overset{\circ}{X}$.

Пусть операции $+$, $\times$, ^{T}, $\overline{\ }$ заданы равенствами: $(A + B)(x, z) = \max\{A(x, z), B(x, z)\}$, $(A \times B)(x, z) = \sup\limits_{y \in \overset{\circ}{Y}} \min\{A(x, y), B(y, z)\}$[2],

$A^T(z, x) = A(x, z)$, $\overline{A}(x, z) = \begin{cases} 1, A(x, z) = 0, \\ 0, A(x, z) \neq 0, \end{cases}$ $A : \overset{\circ}{X} \times \overset{\circ}{Y} \to \{0, 1\}$, $B : \overset{\circ}{Y} \times \overset{\circ}{Z} \to \{0, 1\}$, $x \in \overset{\circ}{X}$, $z \in \overset{\circ}{Z}$.

Как и в случае конечного множества элементарных событий, для того, чтобы функция G описывала некоторый нечеткий элемент, необходимо и достаточно выполнения условий

$$G + G^T = E, G + \overline{G \times G} = E, \inf_{x \in X} G(x, \varnothing) = 0, \inf_{x \in X} G(\varnothing, x) = 1, \qquad (8)$$

[2]Как и в случае конечного множества элементарных событий, с теми же оговорками может использоваться и операция $\cdot : (A \cdot B)(x, z) = \int\limits_{\overset{\circ}{Y}} A(x, y)B(y, z)dy$.

где E — функция $\overset{\circ}{X} \times \overset{\circ}{X} \to \{0,1\}$, тождественно равная 1, поскольку, аналогично конечному случаю, для любых $x, y \in \overset{\circ}{X}$ в силу линейности упорядоченности значений возможности $g^\xi(x) \leqslant g^\xi(y)$ или $g^\xi(y) \leqslant g^\xi(x)$, то есть $\max\{G^\xi(x,y), G^\xi(y,x)\} = 1$ и по определению транзитивности если существует такое $z \in \overset{\circ}{X}$, что $g^\xi(x) \leqslant g^\xi(z)$ и $g^\xi(z) \leqslant g^\xi(y)$, то $g^\xi(x) \leqslant g^\xi(y)$, то есть $(\exists z \in \overset{\circ}{X} : \min\{G^\xi(x,z), G^\xi(y,z)\} = 1) \to G^\xi(x,z) = 1$, что эквивалентно $\max\{\sup\{\min\{G^\xi(x,z), G^\xi(z,y)\} | z \in \overset{\circ}{X}\}, G^\xi(x,y)\} = 1$.

Теорема 2. *Если $\eta = f(\xi)$ — нечеткий элемент — функция ξ, принимающая значения в Y, то описывающая его распределение функция G^η может быть вычислена по формуле*

$$G^\eta = \overline{\Phi^T \times \overline{G^\xi \times \Phi}}, \tag{9}$$

где $\Phi(x,y) = \begin{cases} 1, & \text{если } f(x) = y, \\ 0, & \text{если } f(x) \neq y, \end{cases} \quad x \in X,\ y \in Y$[3], $\Phi(\varnothing, y) = 1,\ y \in \overset{\circ}{Y}$, $\Phi(x, \varnothing) = 0,\ x \in X$.

Доказательство. Для любых $y_1, y_2 \in \overset{\circ}{Y}$ $g^\eta(y_1) \leqslant g^\eta(y_2) \iff \forall x_1 \in X : f(x_1) = y_1\ \exists x_2 \in X : f(x_2) = y_2, g^\xi(x_1) \leqslant g^\xi(x_2)$, то есть $G^\eta(y_1, y_2) = 1 \iff \forall x_1 \in X (\Phi(x_1, y_1) = 1) \to (\exists x_2 \in X : G^\xi(x_1, x_2) = 1, \Phi(x_2, y_2) = 1)$ что эквивалентно $\forall x_1 \in X (\Phi(x_1, y_1) = 1) \to \left(\sup\limits_{x_2 \in X} \min\{G^\xi(x_1, x_2), \Phi(x_2, y_2)\} = 1 \right)$. Это условие выполняется тогда и только тогда, когда $\inf\limits_{x_1 \in X} \max\{\overline{\Phi(x_1, y_1)}, \sup\limits_{x_2 \in X} \min\{G^\xi(x_1, x_2), \Phi(x_2, y_2)\}\} = 1$ или, с учетом двойственности, $\overline{(\Phi^T \times \overline{G^\xi \times \Phi})}(y_1, y_2) = 1$. ■

Замечание. Как и в случае конечного числа элементарных событий, для пары нечетких элементов ξ и η, функций, соответствующих переходному распределению $g^{\xi|\eta}$ и маргинальному распределению g^η, недостаточно для восстановления $G^{\xi,\eta}$, поскольку они не содержат информации об том, как упорядочены различные значения $g^{\xi|\eta}$ по отношению к g^η. Тем не менее, поиск оптимального (минимизирующего некоторый функционал)

[3]Сужение функции Φ на $X \times Y$ — характеристическая функция графика отображения f.

переходного распределения возможен, если оптимальность распределения не зависит от выбора шкалы, но при этом приходится ставить задачу оптимизации для совместного распределения, и поэтому она может быть более сложной по сравнению с «функциональным» представлением распределений. Пример постановки такой задачи см. в теореме 5.

Постановка задачи построения коллективной оценки

В случае произвольного множества элементарных событий задача построения коллективной оценки, комбинирующей распределения, которым соответствуют функции $G^{(1)}, \dots, G^{(K)}$, аналогично § ставится как задача

$$\sum_{k=1}^{K} \rho(G, G^{(k)}) \stackrel{\text{def}}{=} \sum_{k=1}^{K} \int\limits_{\overset{\circ}{X}} \int\limits_{\overset{\circ}{X}} |G(x,y) - G^{(k)}(x,y)| \mu(dx)\mu(dy) \sim \min_{G}, \quad (10)$$

поиска функции G, соответствующей некоторому классу эквивалентности распределений возможности, то есть удовлетворяющей условиям (8). Здесь сумма и умножение понимаются в обычном смысле, μ — фиксированная мера, определенная на σ-алгебре подмножеств $\overset{\circ}{X}$, по которой производится интегрирование в смысле Лебега (например, мера Лебега), относительно $\mu \times \mu$ все функции $G^{(k)}$ являются измеримыми[4]. В случае, если $\mu(\overset{\circ}{X}) < \infty$, интеграл в (10) существует для всех измеримых G.

Теорема 3. *Пусть μ — конечная мера, определенная на σ-алгебре подмножеств $\overset{\circ}{X}$, относительно которой в* (10) *производится интегрирование в смысле Лебега, и относительно $\mu \times \mu$ все функции $G^{(k)}$ являются измеримыми. Тогда решение задачи* (10) *при условиях* (8)*, существует.*

Доказательство. Множество измеримых G, очевидно, вложено в $L^1(\overset{\circ}{X} \times \overset{\circ}{X}, \mu \times \mu)$ и является в нём слабо замкнутым. Функционал $\sum\limits_{k=1}^{K} \rho(G, G^{(k)})$, как и в конечном случае, на допустимых функциях G равен сумме линейного функционала и константы: $\sum\limits_{k=1}^{K} \rho(G, G^{(k)}) = \int\limits_{\overset{\circ}{X}} \int\limits_{\overset{\circ}{X}} G(x,y)(1 -$

[4]Достаточным, но не необходимым условием $\mu \times \mu$-измеримости функции G является μ-измеримость соответствующего ей распределения g.

$2U(x,y))\mu(dx)\mu(dy) + \int\limits_{\overset{\circ}{X}}\int\limits_{\overset{\circ}{X}} U(x,y)\mu(dx)\mu(dy)$, где U — функция, определенная равенствами $U(x,y) = \sum\limits_{k=1}^{K} G^{(k)}(x,y)$, $x,y \in \overset{\circ}{X}$, а следовательно, является слабо непрерывным. Для произвольной функции G, удовлетворяющей условиям (8), и любого $\epsilon > 0$ если $(\mu \times \mu)(E) \leqslant \epsilon$, то $\int\limits_{\overset{\circ}{X}}\int\limits_{\overset{\circ}{X}} G(x,y)\mu(dx)\mu(dy) \leqslant \int\limits_{\overset{\circ}{X}}\int\limits_{\overset{\circ}{X}} \mu(dx)\mu(dy) \leqslant \epsilon$, т. е. множество функций G, удовлетворяющих условиям (8), является равномерно интегрируемым. Согласно [15] (поскольку пространство $\mathbb{R}^1$ с обычной нормой является рефлексивным) равномерная интегрируемость — необходимое и достаточное условие относительной слабой компактности множества функций G, удовлетворяющих условиям (8). Поскольку это множество также является замкнутым, то выполняются условия слабого варианта теоремы Вейерштрасса, и множество решений задачи (10) непусто. ■

Для численного решения задачи (10) с условиями (8) может использоваться, например, метод штрафных функций [16].

Результаты этого и предшествующих разделов опирались только на математические свойства меры возможности, а не на её содержательную интерпретацию. Поэтому эти результаты применимы и к любой другой мере с теми же математическими свойствами, в частности — к мере правдоподобия, описанной в [1, 17].

Пример. *Пусть исследователя интересует неопределенная величина $\widetilde{x}$, о которой у него есть некоторые априорные знания и от значения которой зависит контролирующая (случайный) результат наблюдений $\omega \in \Omega$ вероятность $\Pr(\cdot; x)$. Для комбинирования априорной информации и информации, полученной посредством наблюдений, исследователь:*

1. *предложил распределение правдоподобий $t^{\widetilde{x}}$ значений неопределенного элемента (н.э.) $\widetilde{x}$, показанное на рис. 1а,*

2. *затем получил по случайным данным наблюдений ω, распределение вероятностей $\Pr(\cdot; x)$ которых контролировалось некоторым значением $x \in X$ этого н.э., распределение правдоподобий $t_0^{\widetilde{x}}(\cdot, \omega)$, показанное на рис. 1б как эмпирическую оценку распределения согласно описанному в [17] методу,*

3. *счёл, что эти распределения достаточно хорошо согласуются друг с другом, чтобы скорректировать предложенное им распределение*

правдоподобий с помощью эмпирически восстановленного (например, в том случае, когда значение $\sup\limits_{x'\in X}\Pr(\{\omega'\in\Omega:\Pr(\omega';x')\geqslant\Pr(\omega;x')\};x')$ *максимальной вероятности получить те же результаты наблюдений, что и в действительности, или — любые не более вероятные, если истинное значение* $\widetilde{x}$ *— одно из имеющих единичное правдоподобие согласно предложенному им распределению (на рис. 1а), было близко к* 1*).*

Результат коррекции, полученный как решение задачи (10)*, в которой* μ *— мера Лебега,* $X=[-1,1]$*,* $K=2$*,* $G^{(1)}$ *— функция, соответствующая распределению* $t^{\widetilde{x}}$*,* $G^{(2)}$ *— функция, соответствующая распределению* $t_0^{\widetilde{x}}(\cdot,\omega)$*, показан на рис. 1е, на рис. 1в показано одно из соответствующих ему изоморфных между собой распределений правдоподобий. В случае, если исследователь придает большее или меньшее значение своим априорным знаниям, он может учесть это, заменив в* (10) *внешнюю сумму на выпуклую комбинацию её слагаемых, в которой коэффициент при функции, соответствующей предложенному им распределению, соответственно больше или меньше.*

Эмпирическое восстановление возможности

Эмпирическое восстановление Pr-измеримой ([1, гл. 2]) возможности в случае конечного множества элементарных событий основано на описанных в [18] и [1, §3.3, 3.4] алгоритмах. Пусть X — конечное множество элементарных событий мощности s, $\nu^{(n)}(x)$ — частота события $\{x\}$ после n испытаний, $\delta^{(n,s)}=\left(\frac{2}{n}\ln\frac{1}{\alpha^{(s)}}\right)^{1/2}$, $2s\alpha^{(s)}$ — оценка сверху вероятности ошибочных решений. Тогда алгоритм эмпирического восстановления функции $G:\overset{\circ}{X}\times\overset{\circ}{X}\to\{0,1\}$, описывающей контролировавшее наблюдения распределение возможностей, имеет следующий вид:

1. Для любых $x_1,x_2\in X, x_2\neq x_1$ и каждого $n=1,2,\ldots$ $G(x_1,x_1)=1$, $G(\varnothing,x_1)=1$, $G(x_1,\varnothing)=\begin{cases}0,\ \nu^{(n)}(x_1)>0,\\ 1,\ \nu^{(n)}(x_1)=0,\end{cases}$ а также
   - если $\nu^{(n)}(x_2)-\nu^{(n)}(x_1)>\delta^{(n,s)}$, то $G(x_1,x_2)=1$;
   - если $\nu^{(n)}(x_1)-\nu^{(n)}(x_2)>\delta^{(n,s)}$, то $G(x_2,x_1)=1$;
   - иначе продолжать испытания.

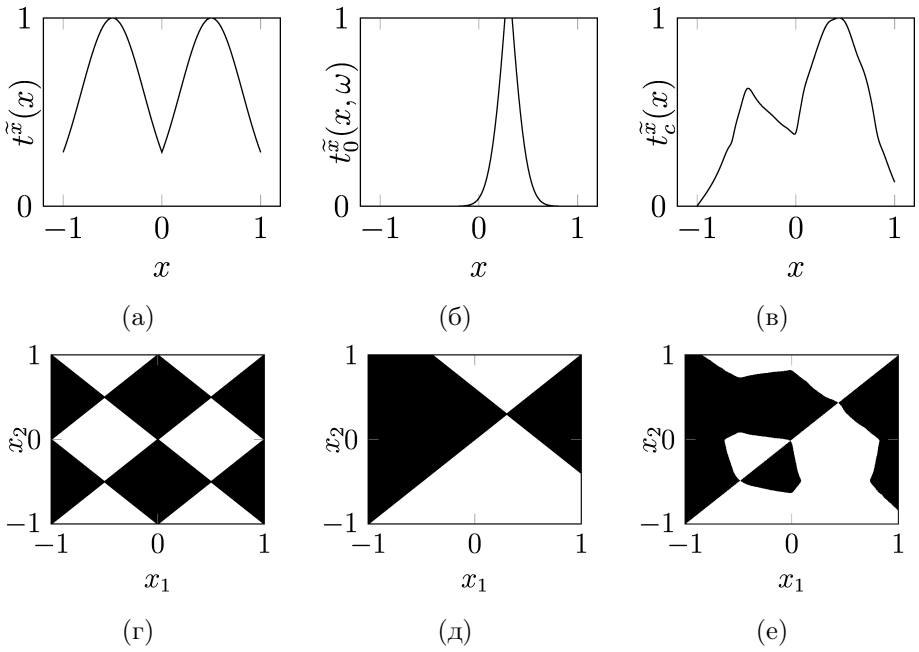


Рис. 1: (а) Распределение $t^{\widetilde{x}}$ правдоподобий н.э. $\widetilde{x}$, предложенное исследователем; (б) Распределение $t_0^{\widetilde{x}}(\cdot,\omega)$ правдоподобий н.э. $\widetilde{x}$, эмпирически восстановленное по данным наблюдений ω; (в) Скорректированное по данным наблюдений распределение $t_c^{\widetilde{x}}$ правдоподобий н.э. $\widetilde{x}$, предложенное исследователем; (г)–(д) Соответствующие (а)–(б) графики бинарных отношений «иметь не большее правдоподобие, чем» (черный цвет — единичные значения, белый — нулевые); (е) График бинарного отношения «иметь не большее правдоподобие, чем», соответствующий скорректированному по данным наблюдений распределению правдоподобий.

2. Для каждого $x \in X$ $X_x^+ \stackrel{\text{def}}{=} \{x' \in X : G(x,x') = 1\}$, $\widehat{f(x)}^{(n)} \stackrel{\text{def}}{=} = \nu^{(n)}(x) + \sum\limits_{x' \in X_x^+} \nu^{(n)}(x')$

   - если $\widehat{f(x)}^{(n)} > 1 + \delta^{(n,s)}$, то $\forall x_1 \in X_x^+, \forall x_2 \in X \setminus X_x^+$ $G(x_1,x_2) = 0$;
   - если $\widehat{f(x)}^{(n)} < 1 - \delta^{(n,s)}$, то для всех таких $x_1 \in X \setminus X_x^+$, что для любого $x_2 \in X \setminus X_x^+$ $G(x_2,x_1) = 1$, $G(x,x_1) = 1$;
   - иначе продолжать испытания.

3. Транзитивно замкнуть G: $\forall x_1, x_2, x_3 \in X$ если $G(x_1, x_2) = G(x_2, x_3)$, то $G(x_1, x_3) = G(x_1, x_2)$. (Этот шаг может также быть выполнен отображением $G \mapsto G \times (I + G)^k$ для любого $k \geqslant s$, где B^k — k-я степень B в смысле умножения $\times$, I — функция, соответствующая бинарному отношению «=» [13].)

В случае, если упорядоченность вероятностей элементарных событий известна заранее, шаг 1 пропускается и используется описывающая эту упорядоченность функция G. Условия остановки с вероятностью 1 за конечное число испытаний те же, что и в [1]: $\forall x_1, x_2 \in X\ \mathrm{pr}(x_1) \neq \mathrm{pr}(x_2)$ в случае постоянных вероятностей элементарных событий $\mathrm{pr}(x)$, $x \in X$, и $\forall n > n_0\ \forall x_1, x_2 \in X\ |\mathrm{pr}^{(n)}(x_1) - \mathrm{pr}^{(n)}(x_2)| \geqslant (1 + \epsilon_{n,s})\delta^{(n,s)}$, где $\mathrm{pr}^{(n)}(x) = \frac{1}{n}\sum\limits_{j=1}^{n} \mathrm{Pr}_j(\{x\})$, Pr_j — контролировавшая j-е испытание вероятность, $\epsilon_{n,s} > 0$ и $\sum\limits_{n=1}^{\infty} (\alpha^{(s)})^{\epsilon_{n,s}^2} < \infty$ для первого шага, $\forall x_1\ f(x) \neq 1$, где $f(x) = \mathrm{pr}(x) + \sum\limits_{x' \in X : \mathrm{pr}(x') \geqslant \mathrm{pr}(x)} \mathrm{pr}(x')$ в случае постоянных вероятностей элементарных событий и $\forall n > n_0\ \forall x \in X\ |f(x)^{(n)} - 1| \geqslant (1 + \epsilon_{n,s})\delta^{(n,s)}$, где $f(x)^{(n)} = \mathrm{pr}^{(n)}(x) + \sum\limits_{x' \in X : \mathrm{pr}^{(n)}(x') \geqslant \mathrm{pr}^{(n)}(x)} \mathrm{pr}^{(n)}(x')$, в случае изменяющихся от испытания к испытанию вероятностей элементарных событий.

Оптимальные решения в задаче идентификации

Пусть субъект, принимающий решения, определяет семейство $\mathcal{L}^{\lambda} = (L, \mathcal{P}(L), \mathrm{P}^{\lambda,(k,d)}, \mathrm{N}^{\lambda,(k,d)})$, $(k, d) \in K \times D$ нечетких пространств потерь [1, §6.4], где λ — нечеткий элемент со значениями в множестве элементарных потерь L, отображения $\mathrm{P}^{\lambda,(\cdot,\cdot)} : (K \times D) \times \mathcal{P}(L) \to [0, 1]$ и $\mathrm{N}^{\lambda,(\cdot,\cdot)} : (K \times D) \times \mathcal{P}(L) \to [0, 1]$ — переходные возможность и необходимость для пространств $(K \times D, \mathcal{P}(K \times D))$, $(L, \mathcal{P}(L))$, $\mathrm{pl}^{\lambda}_{k,d} \stackrel{\mathrm{def}}{=} \mathrm{P}^{\lambda,(k,d)}(V)$, $\mathrm{nl}^{\lambda}_{k,d} \stackrel{\mathrm{def}}{=} \mathrm{N}^{\lambda,(k,d)}(V)$ — соответственно возможность и необходимость множества V потерь, существенных для субъекта, принимающего решения, отвечающих паре $(k, d) \in K \times D$. Тогда модель идентификации — тройка $(g^{\xi,\varkappa}, \widetilde{h}^{\xi,\varkappa}, \mathcal{L}^{\lambda})$, в которой $g^{\xi,\varkappa}, \widetilde{h}^{\xi,\varkappa}$ характеризуют свойства системы, а семейство $\mathcal{L}^{\lambda}$ нечетких пространств и множество V определены субъектом, принимающим решения, в соответствии с условиями ее функционирования при, возможно, неверной интерпретации ее состояний. Достаточная для выбора оптимального четкого решения информация описы-

вается функцией

$$G(k_1,x_1,d_1,k_2,x_2,d_2)=\begin{cases}1, \mathrm{pl}^{\lambda}_{k_1,d_1}\times g^{\xi,\varkappa}(x_1,k_1)\leqslant \mathrm{pl}^{\lambda}_{k_2,d_2}\times g^{\xi,\varkappa}(x_2,k_2),\\ 0, \mathrm{pl}^{\lambda}_{k_1,d_1}\times g^{\xi,\varkappa}(x_1,k_1)> \mathrm{pl}^{\lambda}_{k_2,d_2}\times g^{\xi,\varkappa}(x_2,k_2),\end{cases}$$

$k_1,k_2\in\overset{\circ}{K}$, $x_1,x_2\in\overset{\circ}{X}$, $d_1,d_2\in\overset{\circ}{D}$, причём доопределяется $\mathrm{pl}^{\lambda}_{k,\varnothing}=1$, $k\in\overset{\circ}{K}$. Чёткое решающее правило $d_*:X\to D$ является оптимальным, если оно минимизирует возможность потерь

$$\mathrm{PL}^{\lambda}(d)=\sup_{x\in X,k\in K}\mathrm{pl}^{\lambda}_{k,d(x)}\times g^{\xi,\varkappa}(x,k),$$

причем для нахождения оптимального чёткого решающего правила достаточно [1, §6.4] при каждом $x\in X$ минимизировать

$$\mathrm{PL}^{\lambda}(d(x);x)=\sup_{k\in K}\mathrm{pl}^{\lambda}_{k,d(x)}\times g^{\xi,\varkappa}(x,k).$$

Теорема 4. *Любое чёткое решающее правило $d_*:X\to D$, для которого при любом $d':X\to D$ $G\mathrm{L}^{d}(d_*,d')=1$, где*

$$G\mathrm{L}^{\lambda;d}(d_1,d_2)=\inf_{k_1\in K,x_1\in X}\sup_{k_2\in K,x_2\in X}G(k_1,x_1,d_1(x_1),k_2,x_2,d_2(x_2)),$$

является оптимальным, и для выполнения этого условия достаточно при каждом $x\in X$ потребовать, чтобы

$$\forall d'\in D\; G\mathrm{L}^{\lambda;d}(d_*(x),d';x)=1,$$
$$G\mathrm{L}^{\lambda;d}(d_1,d_2;x)=\inf_{k_1\in K}\sup_{k_2\in K}G(k_1,x,d_1,k_2,x,d_2).$$

Доказательство. $\mathrm{PL}^{\lambda}(d_1)\leqslant\mathrm{PL}^{\lambda}(d_2)$ тогда и только тогда, когда $(\forall k_1\in K,x_1\in X\;\exists k_2\in K,x_2\in X\colon \mathrm{pl}^{\lambda}_{k_1,d_1(x_1)}\times g^{\xi,\varkappa}(x_1,k_1)\leqslant \mathrm{pl}^{\lambda}_{k_2,d_2(x_2)}\times g^{\xi,\varkappa}(x_2,k_2))$, что эквивалентно $(\forall k_1\in K,x_1\in X\;\exists k_2\in K,x_2\in X\colon G(k_1,x_1,d_1(x_1),k_2,x_2,d_2(x_2))=1)$. Это выполняется тогда и только тогда, когда $\inf\limits_{k_1\in K,x_1\in X}\sup\limits_{k_2\in K,x_2\in X}G(k_1,x_1,d_1(x_1),k_2,x_2,\,d_2(x_2))=1$.

Аналогично, $\mathrm{PL}^{\lambda}(d_1;x)\leqslant\mathrm{PL}^{\lambda}(d_2;x)\iff(\forall k_1\in K\;\exists k_2\in K\colon \mathrm{pl}^{\lambda}_{k_1,d_1}\times g^{\xi,\varkappa}(x,k_1)\leqslant\mathrm{pl}^{\lambda}_{k_2,d_2}\times g^{\xi,\varkappa}(x,k_2))$, что эквивалентно $(\forall k_1\in K\;\exists k_2\in K\colon G(k_1,x,d_1,k_2,x,d_2=1)$. Это выполняется тогда и только тогда, когда $\inf\limits_{k_1\in K}\sup\limits_{k_2\in K}G(k_1,x,d_1,k_2,x,d_2)=1$. ■

Рассмотрение нечетких оптимальных решений осложнено проблемой с восстановлением совместного распределения по условному и маргинальному (см. замечание 1). Нечёткое решающее правило $g^{\delta|\xi}$ (распределение возможностей значений принимаемого решения, если получен заданный результат наблюдения) является оптимальным, если оно минимизирует возможность потерь

$$\mathrm{PL}^{\lambda}(g^{\delta|\xi}) = \sup_{x\in X, k\in K, d\in D} \mathrm{pl}^{\lambda}_{k,d} \times g^{\delta|\xi}(d|x) \times g^{\xi,\varkappa}(x,k), \tag{11}$$

причём для нахождения оптимального нечёткого решающего правила достаточно [1, §6.4] при каждом $x \in X$ минимизировать

$$\mathrm{PL}^{\lambda}(g^{\delta|\xi}(\cdot|x)) = \sup_{k\in K, d\in D} \mathrm{pl}^{\lambda}_{k,d} \times g^{\delta|\xi}(d|x) \times g^{\xi,\varkappa}(x,k). \tag{12}$$

Теорема 5. *Любое оптимальное нечёткое решающее правило, описываемое такой функцией $G^{\delta|\xi}$, задаётся для любых $k \in \overset{\circ}{K}, x \in \overset{\circ}{X}, d_1, d_2 \in \overset{\circ}{D}$ равенствами $G^{\delta|\xi}(d_1, d_2; x) = G\mathrm{L}(k, x, d_1, d_1, k, x, d_2, d_2)$, где $G\mathrm{L}$ — такая удовлетворяющая условиям* (8)*, за исключением требования существования хотя бы одного события с ненулевой возможностью, функция, что:*

1. *для функции*
$$G\mathrm{L}(\cdot, \cdot, \varnothing, \cdot, \cdot, \cdot, \varnothing, \cdot) \tag{13}$$
выполняются условия (8) *(фактически, достаточно требования существования хотя бы одного события с ненулевой возможностью, поскольку остальные условия выполняются и для самой функции $G\mathrm{L}$);*

2. *при любых $x \in \overset{\circ}{X}$, $d_1, d_2 \in \overset{\circ}{D}$, $k_1, k_2 \in \overset{\circ}{K}$*
$$G\mathrm{L}(k_1, x, \varnothing, d_1, k_1, x, \varnothing, d_2) = G\mathrm{L}(k_2, x, \varnothing, d_1, k_2, x, \varnothing, d_2); \tag{14}$$

3. *при любых $k_1, k_2 \in \overset{\circ}{K}$, $x_1, x_2 \in \overset{\circ}{X}$, $d_1, d_2 \in \overset{\circ}{D}$*
$$\inf_{d'\in\overset{\circ}{D}} \sup_{d''\in\overset{\circ}{D}} G\mathrm{L}(k_1, x_1, d_1, d', k_2, x_2, d_2, d'') = \\ = G(k_1, x_1, d_1, k_2, x_2, d_2); \tag{15}$$

4. множество

$$\{(k,x,d)\in K\times X\times D|\exists k^*\in K, x^*\in X, d^*\in D:\\ \inf_{d'\in D} G\mathrm{L}(k,x,d,d',k^*,x^*,d^*,d^*)=1\} \quad (16)$$

максимально по включению среди всех функций $G\mathrm{L}$*, удовлетворяющих условиям* (8)*, за исключением требования существования хотя бы одного события с ненулевой возможностью, и условиям* (13)–(15)*.*

Доказательство. Функция $G\mathrm{L}$ определяется равенствами
$G\mathrm{L}(k_1,\,x_1,d_1,d_1',k_2,x_2,d_2,d_2')=$
$\begin{cases}1, \mathrm{pl}^\lambda_{k_1,d_1}\times g^{\xi,\varkappa}(x_1,k_1)\times g^{\delta|\xi}(d_1'|x_1)\leqslant \mathrm{pl}^\lambda_{k_2,d_2}\times g^{\xi,\varkappa}(x_2,k_2)\times g^{\delta|\xi}(d_2'|x_2),\\ 0, \mathrm{pl}^\lambda_{k_1,d_1}\times g^{\xi,\varkappa}(x_1,k_1)\times g^{\delta|\xi}(d_1'|x_1)> \mathrm{pl}^\lambda_{k_2,d_2}\times g^{\xi,\varkappa}(x_2,k_2)\times g^{\delta|\xi}(d_2'|x_2),\end{cases}$
$k_1,k_2\in \overset{\circ}{K};\ x_1,x_2\in \overset{\circ}{X},\ d_1,d_1',d_2,d_2'\in \overset{\circ}{D}$. Выражение $\mathrm{pl}^\lambda_{k,d}\times\ g^{\xi,\varkappa}(x,k)\times g^{\delta|\xi}(d'|x)$, $k\in \overset{\circ}{K}$, $x\in \overset{\circ}{X}$, $d,d'\in \overset{\circ}{D}$, очевидно, принимает значения в шкале возможностей, но не является распределением возможностей. Тем не менее, это выражение может рассматриваться как значения распределения возможностей нечетких элементов λ (взятого при условии d и принимающего два значения, «существенные потери есть» и «существенных потерь нет»), ξ, $\varkappa$ и δ при фиксированном значении λ =«существенные потери есть». Распределением возможностей является и функция $\mathrm{pl}_{k,\varnothing}\times g^{\xi,\varkappa}(x,k)\times g^{\delta|\xi}(d|x)$, что приводит к условию (13). Поэтому функция $G\mathrm{L}$ должна удовлетворять условиям (8), за исключением требования существования хотя бы одного события с ненулевой возможностью (которое может не выполняться, например, если $\mathrm{pl}^\lambda_{\cdot,\cdot}\equiv 0$).

Поскольку $\sup\limits_{d'\in \overset{\circ}{D}} \mathrm{pl}^\lambda_{k,d}\times g^{\xi,\varkappa}(x,k)\times g^{\delta|\xi}(d'|x)=\mathrm{pl}^\lambda_{k,d}\times g^{\xi,\varkappa}(x,k)$, учет информации о задаче, представленной функцией G (соответствие упорядоченности значений согласно распределению, соответствующему G, и согласно распределению, соответствующему $G\mathrm{L}$) приводит к условию (15).

Распределение $g^{\delta|\xi}$ не зависит от $\varkappa$, чему соответствует условие (14), а условное распределение при $\xi=x\in \overset{\circ}{X}$ и $\mathrm{pl}^\lambda_{k,\varnothing}=1$ и фиксированном, но произвольном $\varkappa=k\in \overset{\circ}{K}$ является распределением $g^{\delta|\xi}$.

Если и только если для распределения $g^{\delta|\xi}$ значение $\mathrm{PL}^\lambda(g^{\delta|\xi})$ минимально, то максимально по включению множество таких $(k,x,d)\in K\times X\times D$, что $\mathrm{pl}^\lambda_{k,d}\times g^{\xi,\varkappa}(x,k)\leqslant \mathrm{PL}^\lambda(g^{\delta|\xi})$, т. е., существуют такие $\exists k^*\in$

$K, x^* \in X, d^* \in D$, что для любого $d' \in D$ $\mathrm{pl}^{\lambda}_{k,d} \times g^{\xi,\varkappa}(x,k) \times g^{\delta|\xi}(d'|x) \leqslant \mathrm{pl}^{\lambda}_{k^*,d^*} \times g^{\xi,\varkappa}(x^*,k^*) \times g^{\delta|\xi}(d^*|x^*)$. Очевидно, это множество при фиксированном значении $\mathrm{PL}^{\lambda}(g^{\delta|\xi})$ не зависит от $g^{\delta|\xi}$. ■

Хорошо видно, что задача поиска функции $G\mathrm{L}$ является более сложной, чем минимизация ожидаемой возможности потерь (11). В частности, для поиска оптимальной $G\mathrm{L}$ необходимо осуществить условную минимизацию функционала, а с учетом (12) для нахождения оптимального распределения при фиксированном результате наблюдения достаточно одной безусловной минимизации функции одной переменной [1].

Заключение

В отличие от работ [4, 6], в которых рассматриваются продолжение частичной упорядоченности по распределению нечеткой меры на область определения этой меры, соответствие свойств такого продолжения и свойств исходной меры (аддитивность, max-итивность и т.д.) и свойства основанной на такой упорядоченности логики, и от монографии [12], в которой рассматривается построение комбинированного распределения, в этой статье рассмотрены операции над нечеткими элементами в порядковом представлении, как правило, выполняемые в обычном, функциональном их представлении.

Рассмотренное в этой статье порядковое представление распределений нечетких элементов и мер возможности, для которых эти нечеткие элементы являются каноническими, позволяет выполнять многие из этих операций, в частности, рассчитывать распределение значений функции от нечеткого элемента или от элементов, производить маргинализацию совместного распределения, рассчитывать условное распределение по совместному, эмпирически восстанавливать распределение нечеткого элемента, принимающего конечное множество значений и принимать оптимальные решения.

Однако не все эти действия одинаково удобно выполнять в различных представлениях нечетких элементов: в случае конечного множества элементарных событий вычисление функции от одного неопределенного элемента позволяет использовать хорошо известные алгоритмы линейной алгебры, а вычисление условного распределения сводится к взятию матричного элемента. Формирование распределения возможности, соответствующего объединению информации, содержащейся в нескольких распределениях возможности, принимающих значения в различных

шкалах, более естественно осуществляется в порядковом представлении (если их «взаимная упорядоченность» несущественна, как в случае экспертного восстановления возможности, описанном в [1], где предполагается, что оценка каждого эксперта не зависит от мнения других экспертов).

С другой стороны, формулы, описывающие четкие оптимальные решения, более естественно формулируются в терминах распределений, эмпирическое восстановление нечетких элементов в обычном представлении не требует дополнительного шага для обеспечения транзитивности, а получение совместного распределения по условному и маргинальному в порядковом представлении невозможно. Для варианта теории возможностей, в котором содержательно истолкованы могут быть значения возможности, отличные от 0 и 1, в порядковом представлении необходимо указать также упорядоченности возможностей элементарных событий по отношению этим значениям возможности, что приводит к увеличению размера соответствующих матриц в конечном случае. Вследствие указанной сложности использования условных и переходных распределений (вместо непосредственного поиска условного или переходного распределения приходится искать соответствующее ему совместное) использование нечетких решающих правил (что необходимо для оптимальности принимаемых решений, если объект, от состояния которого зависят последствия принимаемых решений, активен и может конфликтовать с субъектом, принимающим решения, то есть в том случае, когда состояние объекта и принимаемое решение являются зависимыми нечеткими элементами) также существенно сложнее в порядковом представлении.

В заключение — моя искренняя благодарность моему научному руководителю Юрию Петровичу Пытьеву за постановку задачи и её обсуждения.

Работа выполнена при финансовой поддержке РФФИ, проект 14-07-00441.

Список литературы

[1] Пытьев Ю. П. Возможность как альтернатива вероятности. 2 изд., перераб. и дополн. М. : Физматлит, 2015. 596 с.

[2] de Finetti B. Foresight: Its logical laws, its subjective sources // Studies in subjective probability / Ed. by J. Kyburg, H. E. Smokler. Huntingdon, N.Y. : Krieger Pub. Co., 1980. P. 53–118.

[3] Ramsey F. P. Truth and probability // Studies in subjective probability / Ed. by J. Kyburg, H. E. Smokler. Huntingdon, N.Y. : Krieger Pub. Co., 1980. P. 23–52.

[4] Dubois D., Prade H. Formal representations of uncertainty // Decision-making Process: Concepts and Methods / Ed. by D. Bouyssou, D. Dubois, M. Pirlot, H. Prade. London, UK : ISTE, 2009. P. 85–156.

[5] Savage L. J. The foundations of statistics. 2 ed. New York : Dover Publications Inc., 1972. 310 p.

[6] Halpern J. Y. Defining Relative Likelihood in Partially-Ordered Preferential Structures // J. AI Research. 1997. Vol. 7. P. 1–24.

[7] Friedman N., Halpern J. Y. Plausibility measures and default reasoning // Proceedings of the 13th National Conference on Artificial Intelligence. Portland, OR, 1996. P. 1297–1304.

[8] Friedman N., Halpern J. Y. Plausibility measures and default reasoning // Journal of the ACM. 2001. Vol. 48. P. 648–685. URL: http://arxiv.org/abs/cs.AI/9808007.

[9] Halpern J. Y. Plausibility measures: A general approach for representing uncertainty // Proceedings of the 17th International Joint Conference on AI (IJCAI 2001). 2001. P. 1474–1483.

[10] Rosen K. H. Discrete Mathematics and Its Applications. 7 edition. New York, NY : McGraw-Hill, 2012. 1072 p.

[11] Bouyssou D., Vincke P. Binary Relations and Preference Modeling // Decision-making Process: Concepts and Methods / Ed. by D. Bouyssou, D. Dubois, M. Pirlot, H. Prade. London, UK : ISTE, 2009. P. 49–84. doi:10.1002/9780470611876.ch2

[12] Литвак Б. Г. Экспертная информация: Методы получения и анализа. М. : «Радио и связь», 1982. 184 с.

[13] O'Neil P.E., O'Neil E.J. A Fast Expected Time Algorithm for Boolean Matrix Multiplication and Transitive Closure // Information and Control. 1973. Vol. 22. P. 132–138.

[14] Conitzer V., Davenport A., Kalagnanam J. Improved Bounds for Computing Kemeny Rankings // Proceedings of the 21st National

Conference on Artificial Intelligence. Vol. 1 of AAAI'06. Boston, Massachusetts : AAAI Press, 2006. P. 620–626.

[15] Diestel J. Remarks on Weak Compactness in $L_1(\mu, X)$ // Glasgow Mathematical Journal. 1976. December. Vol. 18, № 01. P. 87–91. doi:10.1017/S0017089500003074

[16] Васильев Ф. П. Методы оптимизации. М. : Факториал Пресс, 2002. 824 с.

[17] Пытьев Ю. П. Математическое моделирование субъективных суждений модельера-исследователя о модели объекта исследования // Математическое моделирование. 2013. Т. 25, № 4. С. 102–125.

[18] Пытьев Ю. П. Математические методы и алгоритмы эмпирического восстановления стохастических и нечетких моделей // Интеллектуальные системы. 2007. Т. 11, № 1-4. С. 277–327.

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.

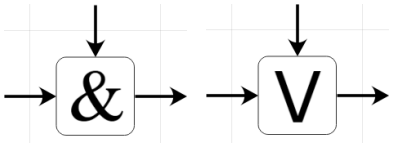
Описывать элемент будем уравнениями, которые задают его оператор, заменяя все переменные в них на сопоставленные им метки (l,r,t или b). Тогда в левой части каждого уравнения будет стоять выходная метка, а в правую будут входить только входные метки.

На рисунке 1 приведены примеры клеточных элементов.

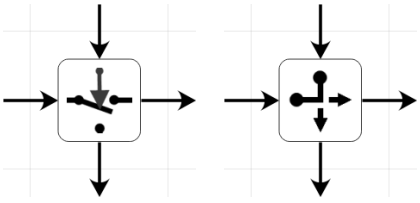
Для удобства введем пустой клеточный элемент — изолирующий (будем обозначать λ).

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

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

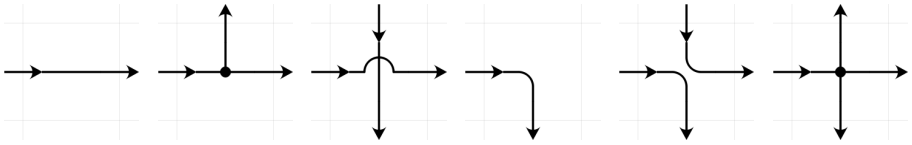


(a) обычные логические элементы



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

(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 $O(\sqrt{|\mathcal{D}|})$.

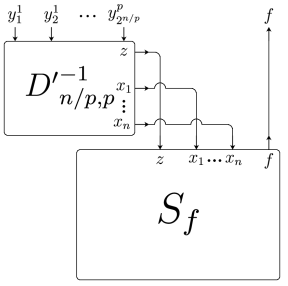


Рис. 2. Реализация схемы $S'_{f,p}$.

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-

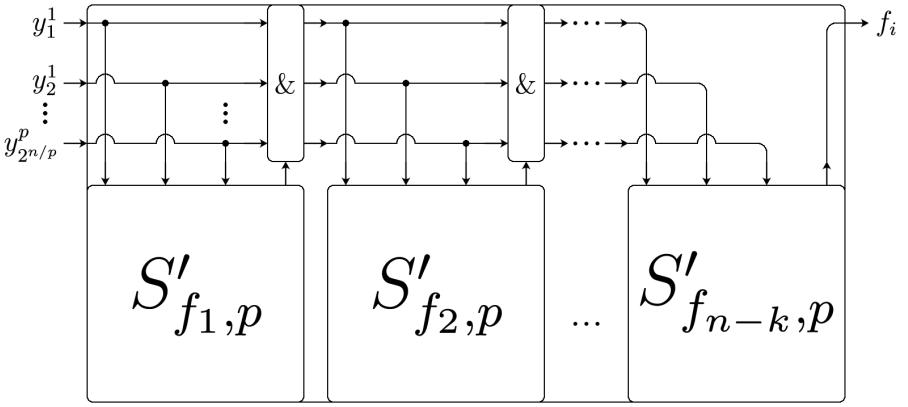


Рис. 3. Схема $G_{f,p}$, реализующая функцию f''.

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].

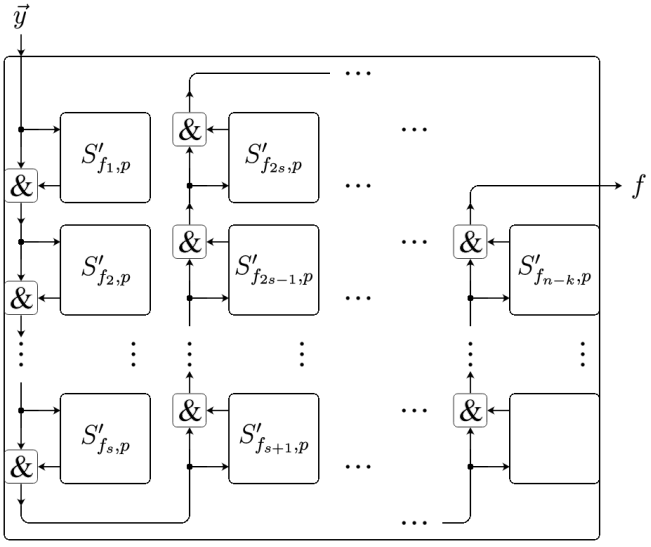


Рис. 4. Квадратная схема $\tilde{G}_{f,p}$, реализующая f''_p.

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.

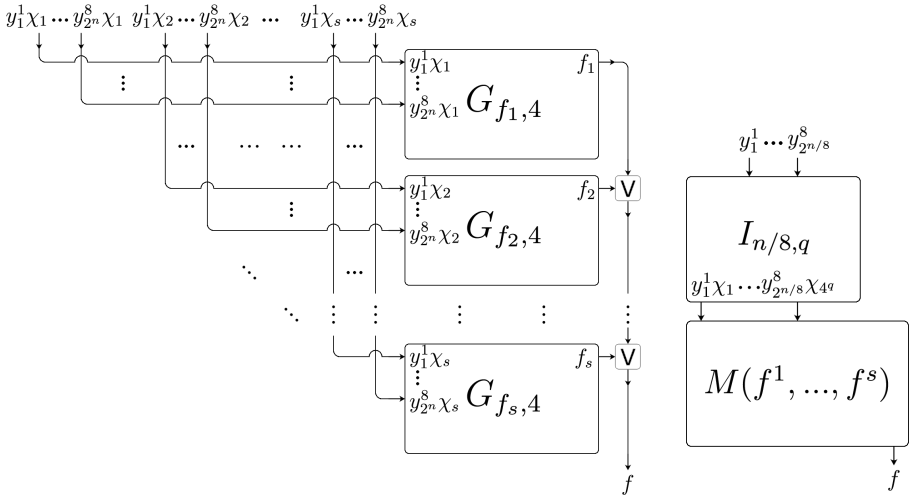
$$\begin{aligned} l(I_{n/8,q}) &= O(2^{n/8} \cdot 4^q) + O(q\sqrt{N}) = \\ &= O((n-k)\sqrt[4]{N} + q\sqrt{N}) = O(\log(n-k)\sqrt{N}), \\ h(I_{n/8,q}) &= O(q2^{n/8}) + O(\sqrt{N}) = O(q\sqrt[4]{N} + \sqrt{N}) = O(\sqrt{N}), \\ \widehat{U}_{\mathcal{G}_{n/8}^8}(I_{n/8,q}) &= O\left(q^2\sqrt{|N_f|}\right)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

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.

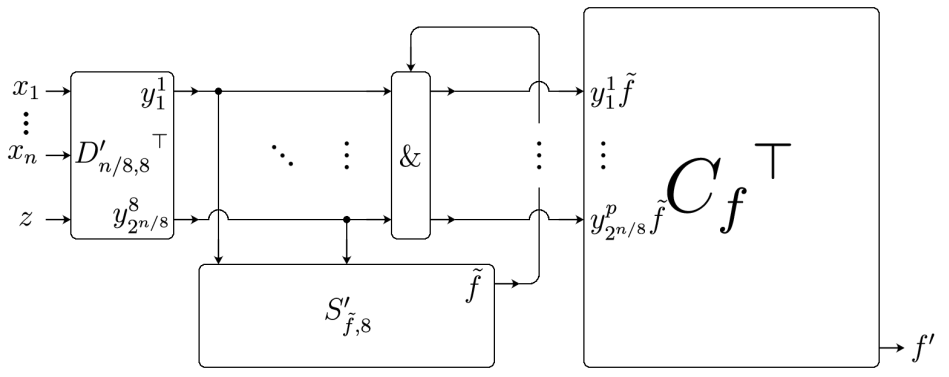


Рис. 6. Блок H_f, реализующий функцию f'.

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.

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

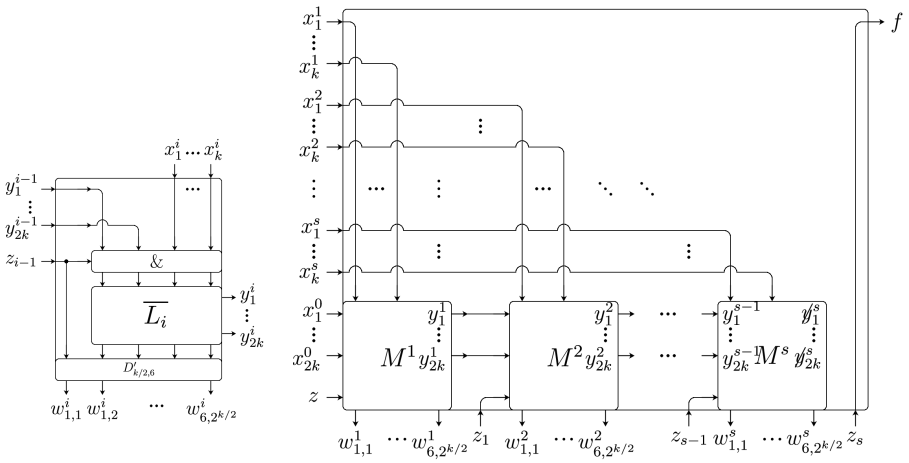
Таким образом, алгоритм, описанный в условии леммы, вычисляет функцию f'. □

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.

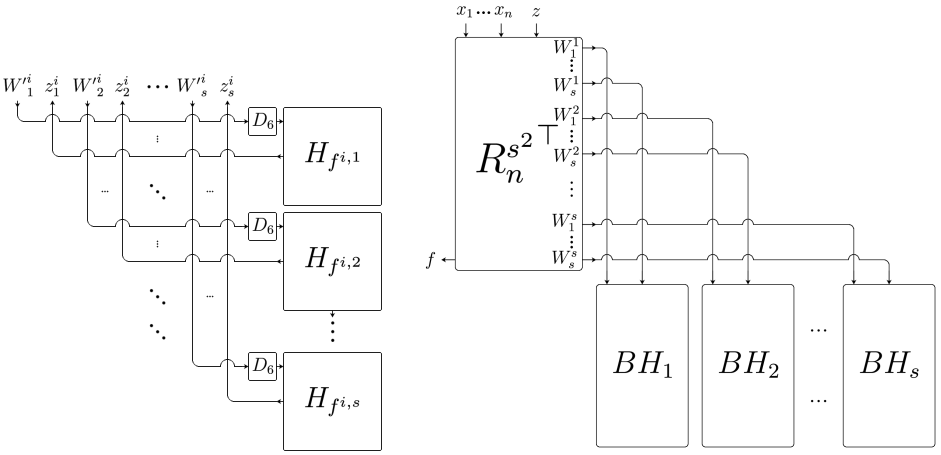
Тогда по лемме 15 при $t = k$ существуют линейные операторы $l_i : \{0,1\}^{3k} \to \{0,1\}^{2k}$ и функции $f^i \in \mathcal{F}_N^{3k}$ такие, что $f' = zf$ может быть вычислена алгоритмом, описанным в условии леммы 15.

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.

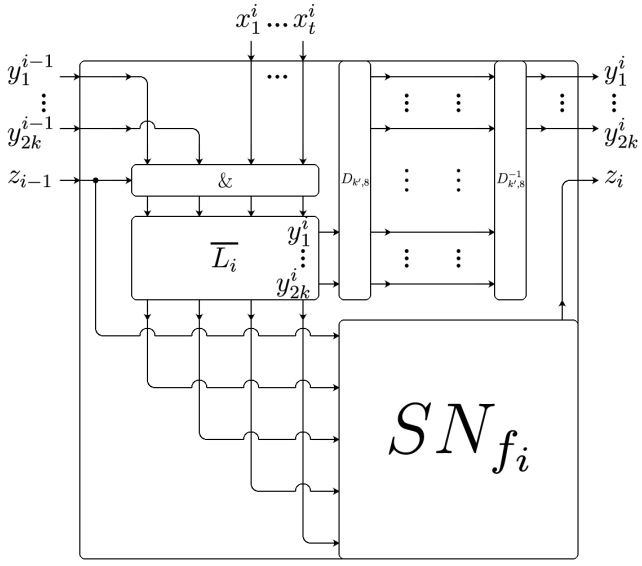


Рис. 9. Блок B_f^i, реализующий функции f^i и l_i.

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}).

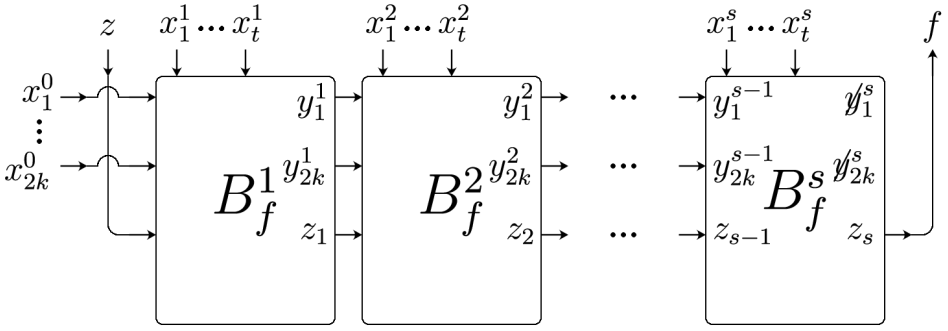


Рис. 10. Схема $SL_{\tilde{f}}^s$, реализующая функцию $\tilde{f}'$.

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

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

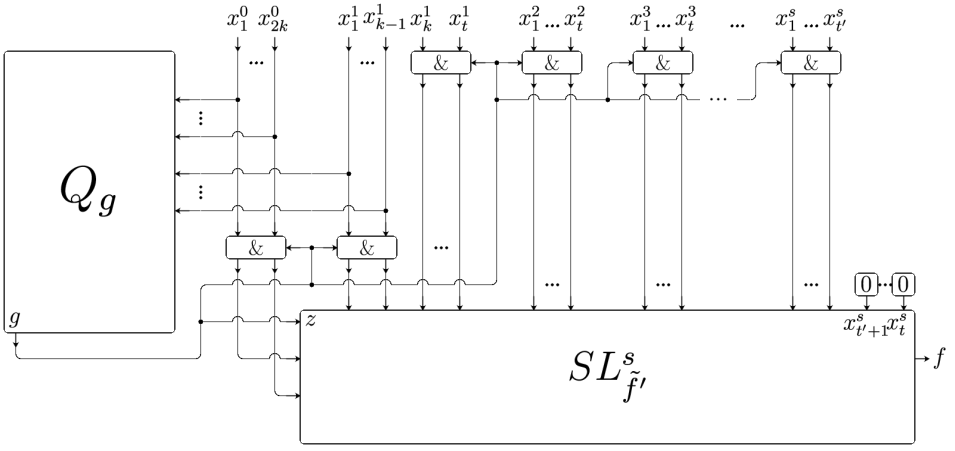


Рис. 11. Схема SF_f^h, реализующая функцию f'.

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

О свойствах кодирований состояний автомата

С. Б. Родин (МГУ имени М. В. Ломоносова, Москва)

Изучается сложность реализации автоматов посредством кодирований его состояний. Рассматриваются всевозможные равномерные кодирования, т.е. кодирования состояний наборами одинаковой длины. На длину кода не накладывается ограничение сверху. Получена верхняя оценка сложности реализации автомата. Получена верхняя оценка длины кода, при котором достигается линейная реализуемость автомата.

Ключевые слова: теория автоматов, переходные системы, подстановка, кодирование, сложность

Введение

На практике часто приходится решать задачу перехода от автоматного описания функционирования на язык схем. Например, при логическом синтезе чипов на первом этапе функционирование чипа описывается как конечный автомат. Переход к описанию на языке схем осуществляется с помощью кодирования алфавита состояний, входного алфавита и выходного алфавита в алфавите $E_2 = \{0, 1\}$.

При этом важно выбрать кодирование, при котором достигается возможно меньшая сложность схемы.

С формальной точки зрения автомат — это пятерка $V = (A, Q, B, \varphi, \psi)$, где A — входной алфавит, Q — алфавит состояний, B — выходной алфавит, φ — функция, которая по текущему входу и состоянию определяет состояние автомата в следующий момент времени, ψ — выходная функция, которая по текущему входу и состоянию определяет выход автомата в текущий момент времени. Кодирование алфавита состояний — это отображение алфавита Q в E_2^k, при котором каждому состоянию из Q ставится в соответствие вектор из E_2^k. Кодирование

входного алфавита — это отображение алфавита A в E_2^p, при котором каждому элементу из A ставится в соответствие вектор из E_2^p. Кодирование выходного алфавита — это отображение алфавита B в E_2^l, при котором каждому элементу из B ставится в соответствие вектор из E_2^l. Кодирования алфавита состояния, входного алфавита и выходного алфавита порождают булев оператор $\phi : E_2^{k+p} \to E_2^{k+l}$, где p — длина кодового набора для символов множества A, k — длина кодового набора для символов множества Q, l — длина кодового набора для символов множества B.

Оператор ϕ можно рассматривать как набор $k+l$ булевых функций от $k+p$ переменных. Сложность такого оператора можно определить как максимальную сложность получающихся булевых функций. Как известно [1], каждой булевой функции единственным образом соответствует полином Жегалкина. Мы будем понимать сложность оператора как максимальную из сложностей полиномов Жегалкина функций, задающих этот оператор, т. е. как максимальную степень полиномов, а сложность автомата — как сложность оператора ϕ. Таким образом, установив связь между автоматом, кодировкой и возникающими полиномами, можно найти минимальную сложность реализации автомата.

Для автомата можно ввести понятие внутренней полугруппы. Внутренняя полугруппа определяется как замыкание отображений множества состояний в себя, определяемых входными символами [5]. Таким образом, на переходную систему автомата можно смотреть как на набор отображений, и сложность реализации автомата определяется сложностью реализации этих отображений.

В работе [9] изучались неизбыточные кодирования и линейная реализуемость автоматов. Неизбыточные кодирования характеризуются тем, что длина кода строго определена мощностью множества состояний автомата. В то же время за счет удлинения кода сложность автомата может уменьшиться. В статье изучается сложность реализации автоматов посредством кодирований, у которых не наложено ограничение на длину кода.

В разделе 2 рассматриваются вопросы сложности реализации отображений множества $E_n = \{0, \ldots, n-1\}$ в себя. В разделе 3 изучается сложность реализации переходной системы автомата.

В статье изучаются переходные с входным алфавитом $A = E_2$. Обозначим через P_n множество всех отображений множества $E_n = \{0, \ldots, n-1\}$ в себя, не обязательно взаимно-однозначных. Данное множество образует полугруппу преобразований множества E_n относитель-

но операции суперпозиции отображений. Взаимно-однозначные преобразования множества E_n образуют группу подстановок на этом множестве [2].

Сложность реализации элементов P_n

Определение 1. Пусть $\phi : E_2^m \to E_2^k$ — булев оператор. Его можно рассматривать как набор k булевых функций, зависящих от m переменных, а именно, если $\phi(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = (\beta_0, \beta_1, \ldots, \beta_{k-1})$, то $f_j(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = \beta_j$, где $0 \le j \le k-1$. Обозначим этот набор через $\mathcal{F}_\phi = \{f_0, f_1, \ldots, f_{k-1}\}$.

Определение 2. Пусть $\mathcal{F} = \{f_0, f_1, \ldots, f_{k-1}\}$ — набор булевых функций, зависящих от k переменных. Данный набор определяет булев оператор $\phi_\mathcal{F} : E_2^m \to E_2^k$ по правилу

$$\begin{aligned}\phi_\mathcal{F}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) =& (f_0(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}), f_1(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}),\\ & \ldots\\ & f_{k-1}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})),\end{aligned}$$

где $\alpha_i \in E_2$.

Определение 3. Пусть $\phi : E_2^m \to E_2^k$ — булев оператор. *Сложностью оператора* назовем максимальную степень полиномов Жегалкина функций $\mathcal{F}_\phi$ или $L_{deg}(\phi) = max\{deg_{f_i \in \mathcal{F}_\phi} f_i\}$

Определение 4. *Кодированием множества* $E_n = \{0, \ldots, n-1\}$ назовем взаимно-однозначное отображение (вложение) $F : \{0, \ldots, n-1\} \to E_2^k$, где $k \ge]\log_2^n[$.

Определение 5. Пусть задано кодирование $F : \{0, \ldots, n-1\} \to E_2^k$, где $k \ge]\log_2 n[$. Кодирование $\hat{F} : \{0, \ldots, 2^k-1\} \to E_2^k$ назовем *доопределением кодирования* F, если для каждого $q \in \{0, \ldots, n-1\}$

$$F(q) = \hat{F}(q).$$

Определение 6. Пусть $s : E_n \to E_n$ — отображение множества $E_n = \{0, \ldots, n-1\}$ в себя. Кодирование $F : Q \to E_2^k$ множества E_n сопоставляет отображению s булев оператор $\phi_s^F : R \to R$, где $R \subseteq E_2^k$, по правилу

$$\phi_s^F(\alpha_1, \ldots, \alpha_{k-1}) = F(s(F^{-1}(\alpha_1, \ldots, \alpha_{k-1}))),$$

где $\alpha_1, \ldots, \alpha_{k-1} \in E_2$.

Определение 7. Оператор $\widehat{\phi} : E_2^m \to E_2^k$, $m, k \in N$ назовем *доопределением оператора* $\phi : R \to {E_2}^k$, где $R \subseteq E_2^m$, если для каждого $(\alpha_1, \ldots, \alpha_m) \in R$ верно

$$\phi(\alpha_1, \ldots, \alpha_m) = \widehat{\phi}(\alpha_1, \ldots, \alpha_m).$$

Определение 8. Отображение $s : E_n \to E_n$ называется *линейно реализуемым посредством кодирования* F, если для оператора ϕ_s^F существует такое доопределение $\hat{\phi}_s^F$, что набор $\mathcal{F}_{\hat{\phi}_s^F}$ состоит из линейных булевых функций.

Определение 9. Кодирование $F : \{0, \ldots, n-1\} \to E_2^n$, определяемое равенством $F(i) = (0 \ldots \underset{i+1}{1} \ldots 0)$, где «1» стоит в i-м разряде, а в остальных разрядах «0», назовем простым позиционным кодированием. Будем обозначать такое кодирование через F_{pos}.

Пример 1. Приведем пример простого позиционного кодирования F_{pos} множества $E_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

q	0	1	2	3	4	5	6	7
$F_{pos}(q)$	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000

Лемма 1. *Отображение $s : E_n \to E_n$ является линейно реализуемым посредством простого позиционного кодирования.*

Доказательство. Обозначим через $s(Q)$ полный образ множества Q отображения s, а через $s^{-1}(q)$ полный прообраз одно-элементного множества $\{q\}$ отображения s. Покажем, что множество

$$\mathcal{F} = \{f_j(\alpha_1, \ldots, \alpha_{k-1}) = \sum_{i \in s^{-1}(j)} \alpha_i, 0 \le j \le k-1\}$$

задает оператор ϕ, являющийся доопределением $\phi_s^{F_{pos}}$.

Рассмотрим значение оператора $\phi_s^{F_{pos}}$ на кодах элементов множества Q. Пусть $s(i) = j$, тогда согласно определению 2

$$\phi_s^F(0, \ldots, \underset{i}{1}, \ldots, 0) = F_{pos}(s(F_{pos}^{-1}(0, \ldots, \underset{i}{1}, \ldots, 0))) =$$

$$= F_{pos}(s(i)) = F_{pos}(j) = (0, \ldots, \underset{j}{1}, \ldots, 0).$$

Заметим, что $f_j(0,\dots,\underset{i}{1},\dots,0) = \sum_{i\in s^{-1}(j)} \alpha_i = 1$, так как $i \in s^{-1}(j)$, и в наборе $(0,\dots,\underset{i}{1},\dots,0)$ ровно одна «1».

С другой стороны $f_l(0,\dots,\underset{i}{1},\dots,0) = \sum_{i\in s^{-1}(j)} \alpha_i = 0$, где $l \neq j$, т.е.

$$\phi(0,\dots,\underset{i}{1},\dots,0) = (0,\dots,\underset{j}{1},\dots,0).$$

□

Пример 2. Булев оператор, сопоставляемый простым позиционным кодированием подстановке

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \end{pmatrix}$$

есть

q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Оператор, задаваемый функциями,

$$f_0(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_1$$
$$f_1(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_2$$
$$f_2(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_3$$
$$f_3(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_4$$
$$f_4(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_5$$
$$f_5(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_6$$
$$f_6(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_7$$
$$f_7(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_0$$

является доопределением построенного частично определенного оператора. Заметим, что p не является линейно реализуемой посредством неизбыточного кодирования.

Сложность реализации переходных систем

В этом разделе будут рассмотрены переходные системы.

Определение 10. Каждое кодирование F множества Q нумерованной переходной системы (A, Q, φ) порождает булев оператор $\phi_V^F : E_2 \times R \to R$, где $R \subseteq E_2^k$, по правилу

$$\phi_V^F(a, \alpha_1, \ldots, \alpha_k) = F(\varphi(a, F^{-1}(\alpha_1, \ldots, \alpha_k))),$$

где $a \in E_2, (\alpha_1, \ldots, \alpha_k) \in R$.

Определение 11. Назовем переходную систему *линейно реализуемой посредством кодирования* F, или просто *линейно реализуемой*, если для заданной нумерованной переходной системы V существует такое кодирование F, что для оператора ϕ_V^F существует доопределение $\widehat{\phi}_V^F$, у которого все элементы $\mathcal{F}_{\widehat{\phi}_V^F}$ являются линейными функциями алгебры логики.

Пример 3. Рассмотрим переходную систему V, изображенную на рисунке 1.

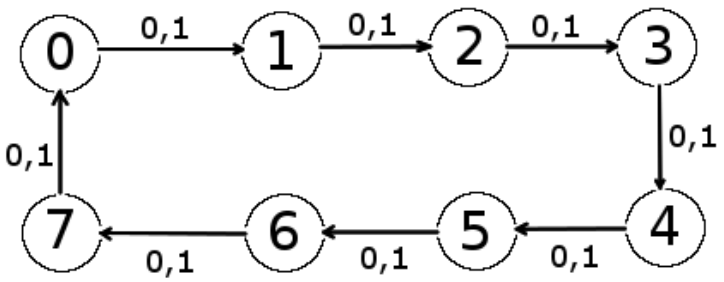


Рис. 1: Линейно реализуемая переходная система

Заметим,что переходная система V не является линейно реализуемой посредством неизбыточных кодирований. Данная переходная система и кодирование F_{pos}

q	0	1	2	3	4	5	6	7
$F_{pos}(q)$	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000

порождают булев оператор

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_3(t)$	$q_4(t)$	$q_5(t)$	$q_6(t)$	$q_7(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$	$q_3(t+1)$	$q_4(t+1)$	$q_5(t+1)$	$q_6(t+1)$	$q_7(t+1)$
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
1	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

Можно видеть, что канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = q_3(0) = q_4(0) = q_5(0) = q_6(0) = q_7(0) = 0 \\ q_0(t+1) = q_1(t) \\ q_1(t+1) = q_2(t) \\ q_2(t+1) = q_3(t) \\ q_3(t+1) = q_4(t) \\ q_4(t+1) = q_5(t) \\ q_5(t+1) = q_6(t) \\ q_6(t+1) = q_7(t) \\ q_7(t+1) = q_0(t) \end{cases}$$

Определение 12. Пусть заданы булев оператор $\phi(a, \alpha_0, \ldots, \alpha_{k-1}) = (\beta_0, \ldots, \beta_{k-1})$, где $a, \alpha_i, \beta_i \in E_2$, $k = \log_2 n$, и кодирование F. Определим переходную систему $V_\phi^F = (E_2, E_n, \varphi)$, в которой функция переходов φ определяется следующим правилом

$$\varphi(a, q) = F^{-1}(\phi(a, F(q)).$$

В работе [9] была доказана лемма

Лемма 2. *Пусть задан булев оператор* $\phi(a, \alpha_0, \ldots, \alpha_{k-1}) = (\beta_0, \ldots, \beta_{k-1})$, *где* $a, \alpha_i, \beta_i \in E_2$, $k = \log_2 n$. *Оператор, порождаемый кодированием* F *и переходной системой* V_ϕ^F, *равен оператору* ϕ .

Определение 13. Пусть задана переходная система $V = (E_2, \{0, \ldots, n-1\}, \varphi)$. Переходную систему $\hat{V} = (E_2, \{0, \ldots, \hat{n}-1\}, \hat{\varphi})$, где $\hat{n} > n$ назовем *доопределением переходной системы* V, если для каждого $a \in E_2$ и $q \in \{0, \ldots, n-1\}$

$$\varphi(a, q) = \hat{\varphi}(a, q).$$

Лемма 3. *Пусть нумерованная переходная система* $V = (E_2, Q = \{0, \ldots, n-1\}, \varphi)$ *линейно реализуема посредством кодирования* $F : \{0, \ldots, n-1\} \to E_2^k$, *где* $k \geq]\log_2 n[$. *Обозначим* $R = F(Q)$. *Тогда существует такое доопределение* $\hat{V} = (E_2, \{0, \ldots, 2^k - 1\}, \hat{\varphi})$ *переходной системы* V, *что переходная система* $\hat{V}$ *является линейно реализуемой.*

Доказательство. Из определения линейной реализуемости следует, что для оператора ϕ_V^F существует такое доопределение $\hat{\phi}_V^F$, что все элементы $\mathcal{F}_{\hat{\phi}_V^F}$ являются линейными функциями. Рассмотрим произвольное доопределение $\hat{F} : \{0, \ldots, 2^k - 1\} \to E_2^k$ кодирования F. По оператору $\hat{\phi}_V^F$ и кодированию $\hat{F}$ построим переходную систему $V_{\hat{\phi}_V^F}^{\hat{F}}$ согласно определению 12. Покажем, что данная переходная система является доопределением V. Множество состояний переходной системы $V_{\hat{\phi}_V^F}^{\hat{F}}$ есть множество $\{0, \ldots, 2^k - 1\}$ и поскольку $k \geq]\log_2 n[$, то $2^k - 1 \geq n - 1$. Согласно определению 12 для функции переходов $V_{\hat{\phi}_V^F}^{\hat{F}}$ верно равенство

$$\varphi_{\hat{\phi}_V^F}^{\hat{F}}(a, q) = \hat{F}^{-1}(\hat{\phi}_V^F(a, \hat{F}(q))).$$

Найдем значение этого оператора на элементах $q \in Q$. Поскольку $\hat{F}$ — доопределение кодирования F, для каждого $q \in Q$ верно равенсво $\hat{F}(q) = F(q)$. Следовательно для всех $q \in Q$

$$\varphi_{\hat{\phi}_V^F}^{\hat{F}}(a, q) = \hat{F}^{-1}(\hat{\phi}_V^F(a, F(q))).$$

Оператор $\hat{\phi}_V^F$ является доопределением оператора ϕ_V^F, значит для всех $q \in Q$ верно

$$\hat{\phi}_V^F(a, F(q)) = \phi_V^F(a, F(q)),$$

так как согласно определению 7 значения этих операторов совпадают на множестве определения оператора ϕ_V^F. Следовательно для всех $q \in Q$

$$\varphi_{\hat{\phi}_V^F}^{\hat{F}}(a, q) = \hat{F}^{-1}(\phi_V^F(a, F(q))).$$

Поскольку согласно определению 6 для любого $q \in Q$ его образ $\phi_V^F(a, F(q))$ принадлежит R, то для каждого $q \in Q$

$$\hat{F}^{-1}(\phi_V^F(a, F(q))) = F^{-1}(\phi_V^F(a, F(q))).$$

Значит для каждого $q \in Q$

$$\varphi^{\hat{F}}_{\hat{\phi}_V^F}(a, q) = F^{-1}(\phi_V^F(a, F(q))).$$

По построению оператора ϕ_V^F для всех $a \in E_2$ и $q \in Q$ верно равенство

$$\varphi^{\hat{F}}_{\hat{\phi}_V^F}(a, q) = F^{-1}(F(\varphi(a, F^{-1}(F(q))))) = \varphi(a, q).$$

Значит, переходная система $V^{\hat{F}}_{\hat{\phi}_V^F}$ является доопределением переходной системы V.

Согласно лемме 2 кодирование $\hat{F}$ по переходной системе $V^{\hat{F}}_{\hat{\phi}_V^F}$ порождает оператор $\hat{\phi}_V^F$. По условию леммы все элементы $\mathcal{F}_{\hat{\phi}_V^F}$ являются линейными функциями, значит переходная система $V^{\hat{F}}_{\hat{\phi}_V^F}$ является линейно реализуемой.

□

Определение 14. Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$, где $Q = \{0, \ldots, n-1\}$. *Сложностью переходной переходной системы* V назовем минимальную сложность среди всех операторов, являющихся доопределениями операторов ϕ_V^F, порождаемых переходной системой V и всевозможными кодированиями F. Обозначим сложность переходной системы через $L_{deg}(V)$.

Теорема 1. *Пусть задана нумерованная переходная система* $V = (E_2, Q, \varphi)$, *где* $Q = \{0, \ldots, n-1\}$. *Тогда* $L_{deg}(V) \leq 2$.

Доказательство. Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$. Обозначим ее порождающие через p_0 и p_1. Согласно лемме 1 они линейно реализуемы посредством простого позиционного кодирования F_{pos}. Рассмотрим линейные доопределения ϕ_{p_0} и ϕ_{p_1} булевых операторов, сопоставляемые отображениям p_0 и p_1 кодированием F_{pos}. Рассмотрим множества функций

$$\mathcal{F}_{\phi_{p_0}} = \{f_0^0(q_0, q_1, \ldots, q_{n-1}), \ldots, f_{n-1}^0(q_0, q_1, \ldots, q_{n-1})\}$$

и

$$\mathcal{F}_{\phi_{p_1}} = \{f_0^1(q_0, q_1, \ldots, q_{n-1}), \ldots, f_{n-1}^1(q_0, q_1, \ldots, q_{n-1})\},$$

определяемых операторами ϕ_{p_0} и ϕ_{p_1}. Покажем, что функции

$$\mathcal{F} = \{x \cdot (f_0^0(q_0, q_1, \ldots, q_{n-1}) \oplus f_0^1(q_0, q_1, \ldots, q_{n-1})) \oplus f_0^0(q_0, q_1, \ldots, q_{n-1}),$$

$$\ldots$$

$$x \cdot (f_{n-1}^0(q_0, q_1, \ldots, q_{n-1}) \oplus f_{n-1}^1(q_0, q_1, \ldots, q_{n-1})) \oplus f_{n-1}^0(q_0, q_1, \ldots, q_{n-1})\}$$

задают оператор ϕ, являющийся доопределением оператора $\phi_V^{F_{pos}}$.

Согласно определению порождающих внутренней полугруппы переходной системы верны равенства $\varphi(0, q) = p_0(q), \varphi(1, q) = p_1(q)$. Пусть $(\alpha_0, \ldots, \alpha_{n-1})$ код некоторого состояния $q \in Q$ при кодировании F_{pos}. Рассмотрим значение оператора $\phi_V^{F_{pos}}$ на наборах $(0, \alpha_0, \ldots, \alpha_{n-1})$.

$$\phi_V^{F_{pos}}(0, \alpha_0, \ldots, \alpha_{n-1}) = F_{pos}(\varphi(0, F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) =$$

$$= F_{pos}(p_0(F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) = \phi_{p_0}(\alpha_0, \ldots, \alpha_{n-1}) =$$

$$= (f_0^0(q_0, q_1, \ldots, q_{n-1}), \ldots, f_{n-1}^0(q_0, q_1, \ldots, q_{n-1})) = \phi(0, \alpha_0, \ldots, \alpha_{n-1}).$$

Рассмотрим значение оператора $\phi_V^{F_{pos}}$ на наборах $(1, \alpha_0, \ldots, \alpha_{n-1})$

$$\phi_V^{F_{pos}}(1, \alpha_0, \ldots, \alpha_{n-1}) = F_{pos}(\varphi(1, F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) =$$

$$= F_{pos}(p_1(F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) = \phi_{p_1}(\alpha_0, \ldots, \alpha_{n-1}) =$$

$$= (f_0^1(q_0, q_1, \ldots, q_{n-1}), \ldots, f_{n-1}^1(q_0, q_1, \ldots, q_{n-1})) = \phi(0, \alpha_0, \ldots, \alpha_{n-1}).$$

Из полученных равенств следует, что оператор ϕ совпадает с $\phi_V^{F_{pos}}$ на области определения оператора $\phi_V^{F_{pos}}$. Поскольку функции из наборов $\mathcal{F}_{\phi_{p_0}}$ и $\mathcal{F}_{\phi_{p_1}}$ линейные, функции из набора $\mathcal{F}$ задаются полиномами Жегалкина степени не выше 2. □

Следствие 1. *Нумерованная переходная система $V = (E_2, Q, \varphi)$, у которой функция переходов фиктивным образом зависит от входа, т.е. переходная система типа часы, является линейно реализуемой.*

Пример 4. Рассмотрим переходную систему V, изображенную на рисунке 2.

Данная переходная система и кодирование

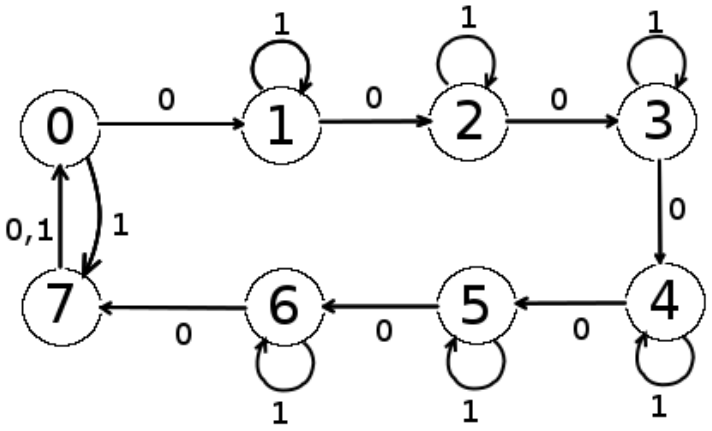


Рис. 2: Переходная система

q	0	1	2	3	4	5	6	7
$F_{pos}(q)$	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000

порождают булев оператор

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_3(t)$	$q_4(t)$	$q_5(t)$	$q_6(t)$	$q_7(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$	$q_3(t+1)$	$q_4(t+1)$	$q_5(t+1)$	$q_6(t+1)$	$q_7(t+1)$
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0
1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
1	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Можно видеть, что канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = q_3(0) = q_4(0) = q_5(0) = q_6(0) = q_7(0) = 0 \\ q_0(t+1) = x(t) \cdot q_1(t) + x(t) \cdot q_7(t) + q_1(t) \\ q_1(t+1) = x(t) \cdot q_2(t) + x(t) \cdot q_1(t) + q_2(t) \\ q_2(t+1) = x(t) \cdot q_3(t) + x(t) \cdot q_2(t) + q_3(t) \\ q_3(t+1) = x(t) \cdot q_4(t) + x(t) \cdot q_3(t) + q_4(t) \\ q_4(t+1) = x(t) \cdot q_5(t) + x(t) \cdot q_4(t) + q_5(t) \\ q_5(t+1) = x(t) \cdot q_6(t) + x(t) \cdot q_5(t) + q_6(t) \\ q_6(t+1) = x(t) \cdot q_7(t) + x(t) \cdot q_6(t) + q_7(t) \\ q_7(t+1) = x(t) \cdot q_0(t) + x(t) \cdot q_0(t) + q_0(t) \end{cases}$$

Теорема 2. *Пусть задана линейно реализуемая нумерованная переходная система $V = (E_2, Q, \varphi)$, где $Q = \{0, \ldots, n-1\}$. Тогда существует такое кодирование $F : Q \to E_2^k$, где $k \leq 2^n$, что переходная система V линейно реализуема посредством F.*

Доказательство. Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$, где $Q = \{0, \ldots, n-1\}$, линейно реализуемая посредством кодирования $F : Q \to E_2^k$, где $k > 2^n$. Рассмотрим матрицу кодов, задаваемых кодированием F,

$$T = \begin{pmatrix} F(0) \\ F(1) \\ \ldots \\ F(n-1) \end{pmatrix}.$$

Столбцы этой матрицы имеют длину n и состоят из 0 и 1. Число различных векторов длины n из 0 и 1 равно 2^n. Число столбцов в матрице равно k. Так как $k > 2^n$, то в данной матрице найдутся два равных столбца. Без ограничения общности считаем, что равны первый и второй столбцы, т.е. для любого $q \in Q$, из условия $(\alpha_0, \alpha_1, \ldots, \alpha_{k-1}) = F(q)$ следует, что $\alpha_0 = \alpha_1$.

Обозначим через ϕ_L линейное доопределение оператора ϕ_V^F. Согласно определению 7 доопределения оператора для всех $a \in E_2$ и $q \in Q$

$$\phi_L(a, F(q)) = \phi_V^F(a, F(q)).$$

Следовательно для функций $f_i \in \mathcal{F}_{\phi_L}, g_i \in \mathcal{F}_{\phi_V^F}$ для всех $a \in E_2$ и $q \in Q$

$$f_i(a, F(q)) = g_i(a, F(q)).$$

Причем f_i - линейные функции, где $0 \le i \le k-1$, т.е.

$$f_i(x, q_0, q_1, \ldots, q_{k-1}) = c \cdot x + \sum_{l=0}^{k-1} c_l \cdot q_l.$$

Согласно определению оператора 6 $\phi_V^F(a, F(q)) \in F(Q)$. Значит, для всех $a \in E_2$ и $q \in Q$

$$g_0(a, F(q)) = g_1(a, F(q)),$$

где $g_0, g_1 \in \mathcal{F}_{\phi_V^F}$. Поскольку для всех $a \in E_2$ и $q \in Q$

$$g_0(a, F(q)) = f_0(a, F(q)),$$

$$g_1(a, F(q)) = f_1(a, F(q)),$$

где $f_0 \in \mathcal{F}_{\phi_L}, g_0 \in \mathcal{F}_{\phi_V^F}, f_1 \in \mathcal{F}_{\phi_L}, g_1 \in \mathcal{F}_{\phi_V^F}$, верно, что для всех $a \in E_2$ и $q \in Q$

$$f_0(a, F(q)) = f_1(a, F(q)).$$

По кодированию $F : Q \to E_2^k$ построим кодирование $F' : Q \to E_2^{k-1}$ по следующему правилу: если $F(q) = (\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$, то $F'(q) = (\alpha_1, \ldots, \alpha_{k-1})$. Заметим, что по определению кодирования, если $q \ne q'$, то $F(q) = (\alpha_0, \alpha_1, \ldots, \alpha_{k-1}) \ne (\alpha'_0, \alpha'_1, \ldots, \alpha'_{k-1}) = F(q')$. Значит существует такое i, что $\alpha_i \ne \alpha'_i$.

Если $i > 0$, то $(\alpha_1, \ldots, \alpha_{k-1}) \ne (\alpha'_1, \ldots, \alpha'_{k-1})$.

Если $i = 0$, то заметим, что $\alpha_0 = \alpha_1$ и $\alpha'_0 = \alpha'_1$, и следовательно, $\alpha_1 \ne \alpha'_1$, что означает $(\alpha_1, \ldots, \alpha_{k-1}) \ne (\alpha'_1, \ldots, \alpha'_{k-1})$. Таким образом показано, что отображение F' взаимно-однозначно на Q.

По построению кодирования F' видно, что если набор $(\alpha_1, \ldots, \alpha_{k-1}) \in F'(Q)$, то набор $(\alpha_1, \alpha_1, \ldots, \alpha_{k-1}) \in F(Q)$ и $F'(\alpha_1, \ldots, \alpha_{k-1}) = F(\alpha_1, \alpha_1, \ldots, \alpha_{k-1})$.

Рассмотрим оператор переходной системы, построенный посредством кодирования F'.

$$\phi_V^{F'}(a, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}) = F'(\varphi(a, F'^{-1}(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}))) =$$

$$= F'(\varphi(a, F^{-1}(\alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}))) =$$

$$= (g_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots, g_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})),$$

где $g_i \in \mathcal{F}_{\phi_V^F}$. Последнее равенство следует из построения кодирования F' и равенства

$$F(\varphi(a, F^{-1}(\alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}))) =$$

$$= (g_0(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), g_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots,$$

$$g_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})).$$

Как было показано раннее, функции f_i и g_i равны для всех $a \in E_2$ и $q \in Q$. Следовательно, верно равенство

$$(g_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots, g_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})) =$$

$$= (f_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots, f_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})),$$

где $f_i \in \mathcal{F}_{\phi_L}$. То есть множество $\mathcal{F}_{\phi_V^{F'}}$ составляют функции, полученные из линейных операцией отождествления первого и второго аргументов. При такой операции функции остаются линейными[1].

Таким образом показано, что если переходная системы линейно реализуема посредством кодирования, которое кодирует состояния кодами длины k больше чем 2^n, то можно построить кодирование, которое кодирует состояния кодами длины $k-1$, посредством которого переходная система линейно реализуема. Повторяя данные построения, придем к кодированию, которое кодирует состояния кодами длины 2^n. □

В заключение автор выражает благодарность Алёшину Станиславу Владимировичу, чьи советы оказали неоценимую помощь в получении результатов, изложенных в данной работе.

Список литературы

[1] Яблонский С.В., *Введение в дискретную математику.* - М.:Наука,1979.

[2] А. Клиффорд, Г. Престон *Алгебраическая теория полугрупп, Том 1* -М.:Мир, 1972.

[3] Р. Лидл, Г. Нидеррайтер *Конечные поля.* - М.:Мир, 1988.

[4] М.И. Карагаполов, Ю.И. Мерзляков *Основы теории групп.* - 3-е издание-М.:Наука, 1982.

[5] М.А. Арбиб *Декомпозиция автоматов и расширение полугрупп* Алгебраическая теория автоматов, языков и полугрупп-М.“Статистика“, 1975, С.46-64

[6] Родин С.Б., *Переходные системы с максимальной вариантностью относительно кодирования состояний.* Интеллектуальные системы. Т.4, вып. 3-4. С.335-352.

[7] Родин С.Б., *О связи линейно реализуемых автоматов и автоматов с максимальной вариативностью относительно кодирования состояний.* Интеллектуальные системы. Т.20, вып. 2. С.337-347.

[8] С.В. Алешин *Алгебраические системы автоматов* -М.:МАКС Пресс, 2016

[9] Родин С.Б., *Линейно реализуемые автоматы* Дискретная математика. Т. 29, вып. 1, С.59–79

Оценка длины периода выхода для автономного автомата с однобуквенным магазином

И. Е. Иванов (МГУ имени М. В. Ломоносова, Москва)

Ранее автор доказал, что автоматные функции с магазинной памятью сохраняют множество периодических последовательностей, и привел экспоненциальную от характеристик автомата оценку удлинения периода. В данной работе для автоматов с однобуквенным магазином эту оценку удалось понизить до квадратичной.

Ключевые слова: автомат с магазинной памятью с однобуквенным магазином, детерминированная функция, периодические последовательности.

Введение

Первые упоминания автоматов с дополнительной памятью в виде стека начали появляться в 50-х годах прошлого века. Они возникали преимущественно в контексте задач обработки естественного языка. Формализовали определение автомата с магазинной памятью Эттингер[1] и Шютценберже [2] уже в 60-х годах. Эквиваленность автоматов с магазинной памятью и контекстно-свободных грамматик была показана Хомским[3] и Эви[4].

Очень скоро стало понятно, что класс контекстно-свободных языков устроен сложнее класса регулярных. В работах [5, 6] появились примеры алгоритмически неразрешаемых проблем, которые были успешно разрешены для регулярных языков. Оказалось, что многие техники работы с конечными автоматами и регулярными языками для автоматов с магазинной памятью не работают. В частности, было показано, что классы языков, разпознаваемых детерминированными автоматами с магазинной

памятью, не равен классу всех контекстно-свободных языков, а является его собственным подмножеством [7, 2].

Полученные отрицательные результаты мотивировали математиков рассматривать более простые подклассы автоматов с магазинной памятью. Хорошим примером такого класса является класс детерминированных автоматов с магазинной памятью с однобуквенным магазином. С одной стороны, этот класс автоматов является естественным расширением класса конечных автоматов, с другой стороны, он является довольно содержательным, так как, например, содержит язык правильных скобочных записей. Лишь в 70-80-х годах для этого класса автоматов была успешно решены проблема эквивалентности, а также проверка языка на регулярность [8, 9]. Исследование этого класса автоматов продолжается до сих пор. Нельзя не отметить работу [10], в которой была получена сложность проверки двух автоматом с однобуквенным магазином на эквивалентность.

Несмотря на довольно большие успехи в изучении автоматов с магазинной памятью в большинстве работ никак не изучается функциональные свойства этих автоматов, как, например, это было сделано для конечных автоматов. Основные результаты можно найти в [11]. Отдельно хотелось бы отметить результат Д.Н. Бабина — решение им аналога 13-ой проблемы Гильберта для автоматных функций [12]. Аналогичных работ, изучающих свойства автоматов с магазинной памятью как преобразователей последовательностей, почти не встречается в литературе. Поэтому автором была предпринята попытка разобраться в данной области.

В работе [13] было доказано, что автоматы с магазинной памятью сохраняют периодические последовательности. Автором приводится экспоненциальная верхняя оценка на максимальную длину периода в зависимости от периода входной последовательности и характеристик автомата и доказывается, что если в алфавите магазина разрешается использовать хотя бы два символа, то существенно понизить экспоненциальную оценку нельзя [14].

В данной работе удалось понизить верхнюю оценку до квадратичной от количества состояний в случае автономного автомата с однобуквенным магазином.

Работа состоит из 7 разделов, включая введение, заключение и списком литературы. Во втором разделе даются основные определения и постановка задачи. В третьем — приводятся основные резлуьтаты. В четверном разделе доказывается нижняя оценка путем построения приме-

ра. В пятом — доказывается асимптотическая верхняя оценка. Далее следует заключение и библиография. В последний раздел (дополнений) вынесены простые, но технически громоздкие утверждения.

Определения

Будем говорить, что $P_0 = \{Q, B, \Gamma, \varphi, \psi, \eta, q_0, \gamma_0\}$ — инициальный автомат с магазинной памятью без входа (автономный), где Q — конечное множество состояний, B — выходной алфавит, Γ — алфавит памяти (алфавит ленты магазина), $\varphi : Q \times (\Gamma \cup \lambda) \to Q$ — функция переходов, $\psi : Q \times (\Gamma \cup \lambda) \to B$ — функция выхода, $\eta : Q \times (\Gamma \cup \lambda) \to \Gamma^*$ — функция памяти, $q_0 \in Q$ — начальное состояние, $\gamma_0 \in \Gamma^*$ — начальная запись в магазине. Функционирование автомата P_0 удовлетворяет системе канонических уравнений:

$$\begin{cases} q(0) = q_0 \\ \gamma(0) = \gamma_0 \\ z(t) = LS(\gamma(t)) \\ q(t+1) = \varphi(q(t), z(t)) \\ \gamma(t+1) = S(\gamma(t))\eta(q(t), z(t)) \\ b(t) = \psi(q(t), z(t)) \end{cases} \tag{1}$$

где $LS : \Gamma^* \to \Gamma \cup \{\lambda\}$ возвращает последний символ при подаче непустого слова и $LS(\lambda) = \lambda$, а $S : \Gamma^* \to \Gamma^*$— стирает последний символ входного слова и $S(\lambda) = \lambda$.

Пусть $n = |Q|$, $m = |\Gamma|$, $k = \max\limits_{(q,z) \in Q \times \Gamma \cup \{\lambda\}} |\eta(q, z)|$. Обозначим множество автоматов с магазинной памятью без входа с заданными n, m, k через $\mathcal{M}_0(n, m, k)$.

В работе [13] было показано, что автоматы с магазинной памятью сохраняют периодические последовательности. Откуда следует, что выходом автономного автомата будет периодическая последовательность. Для автомата с магазинной памятью без входа обозначим $L(P)$ минимальную длину периода периодической последовательности, которую он генерирует. Далее под длиной периода будем понимать именно минимальную, то есть $L(P)$. Нас будет интересовать максимальная длина периода в классе автоматов $\mathcal{M}_0(n, m, k)$, а именно:

$$L(n, m, k) = \max_{P \in \mathcal{M}_0(n,m,k)} L(P).$$

Для получения оценок на $L(n,1,k)$ введем дополнительные ограничения на рассматриваемые автоматы. Пусть P — автономный автомат с магазинной памятью с однобуквенным магазином. Будем считать, что P генерирует периодическую последовательность без предпериода и все состояния достижимые и встречаются бесконечное число раз в последовательности $q(t)$, заданной каноническими уравнениями. Заметим, что если в последовательности $\gamma(t)$ пустое слово встречается лишь конечное число раз, то из-за отсутствия предпериода магазин не бывает пустым. Поэтому в этом случае P функционируют в точности как автомат без магазина, то есть конечный автомат. Разумеется, этот случай нас не интересует. Поэтому будем считать, что пустое слово в последовательности $\gamma(t)$ будет встречаться бесконечное число раз. Для удобства будем считать, что начальная запись в магазине пустая, то есть $\gamma_0 = \lambda$. Будем рассматривать наиболее общую функцию выхода $\psi(q,z) = (q,z)$, то есть $B = Q \times \Gamma \cup \{\lambda\}$. Очевидно, что наложение описанных ограничений на класс автоматов не меняют максимальную длину периода внутри класса автоматов.

Обозначим через $\mathcal{M}'_0(n,1,k)$ множество автоматов P из $\mathcal{M}'_0(n,1,k)$, для которых выполнены описанные выше ограничения, а именно:

- периодическая последовательность, сгенерированная P, не имеет предпериода;
- все состояния достижимы бесконечное число раз;
- $\gamma_0 = \lambda$;
- $B = Q \times \Gamma \cup \{\lambda\}$ и $\psi(q,z) = (q,z)$.

Очевидно, что выполнено

$$L(n,1,k) = \max_{P \in \mathcal{M}'_0(n,1,k)} L(P),$$

поэтому далее будем рассматривать автоматы только из $\mathcal{M}'_0(n,1,k)$.

Введем еще несколько определений, необходимых для дальнейших рассуждений. Для автомата P выделим множество стирающих состояний

$$S = \{q \in Q \mid \eta(q,1) = \lambda\}.$$

Если $q \in W = Q \backslash S$, то будем говорить, что состояние пишущее. В множестве пишущих состояний выделим подмножество нейтральных состояний

$$N = \{q \in Q \mid \eta(q, 1) = 1\},$$

то есть таких, при прохождении через которые непустое слово, записанное в магазине, не изменяет свою длину.

Если в автомате P найдётся множество состояний $C = \{c_1, ..., c_\ell\} \subseteq Q$ такое, что выполнено $\varphi(c_i, 1) = c_{i+1}$ для $i = 1, .., l-1$ и $\varphi(c_\ell, 1) = c_1$, то будем говорить, что C является автоматным циклом. Длиной автоматного цикла C будем называть число состояний в этом цикле.

Для автомата P однозначно определены последовательности состояний и состояний магазина согласно (1). Будем говорить, что автоматный цикл C достижим, если найдется такой номер t_1, что выполнены следующие условия:

1) $\{q(t_1), q(t_1 + 1), ..., q(t_1 + |C| - 1)\} = C$;

2) $z(t_1) = z(t_1 + 1) = ... = z(t_1 + |C| - 1) = 1$.

Каждому автоматному циклу сопоставим индекс — число, на которое изменится длина памяти магазина при одном проходе по нему. Будем называть автоматный цикл стирающим, если индекс отрицательный, то есть количество символов в магазине при одном проходе по циклу уменьшается. Если индекс автоматного цикла неотрицательный, то будем говорить, что автоматный цикл пишущий.

Будем называть конфигурацией автомата пару его состояние и состояние магазина $(t) = (q(t), \gamma(t))$. Будем говорить, что конфигурация c_2 достижима из конфигурации c_1, и писать $c_1 \Rightarrow c_2$, если автомат с магазинной памятью из конфигурации c_1 перейдет в конфигурацию c_2 через конечное число тактов.

В некоторых случаях нас будет интересовать поведение автомата при непустом магазине. В таких случаях будем говорить, что конфигурация c_2 достижима без опустошения магазина из конфигурации с непустым магазином c_1, и писать $c_1 \Rrightarrow c_2$. Заметим, что и c_1, и c_2 могут иметь пустой магазин.

Основные результаты

Основным результатом работы является доказательство следующей теоремы.

Теорема 1. *При* $k > 1$ *и* $n \to \infty$

$$L(n,1,k) = \frac{k(k-1)}{4k-2} n^2 (1 + o(1)).$$

Доказательство нижней оценки L(n,1,k)

Пример 1.

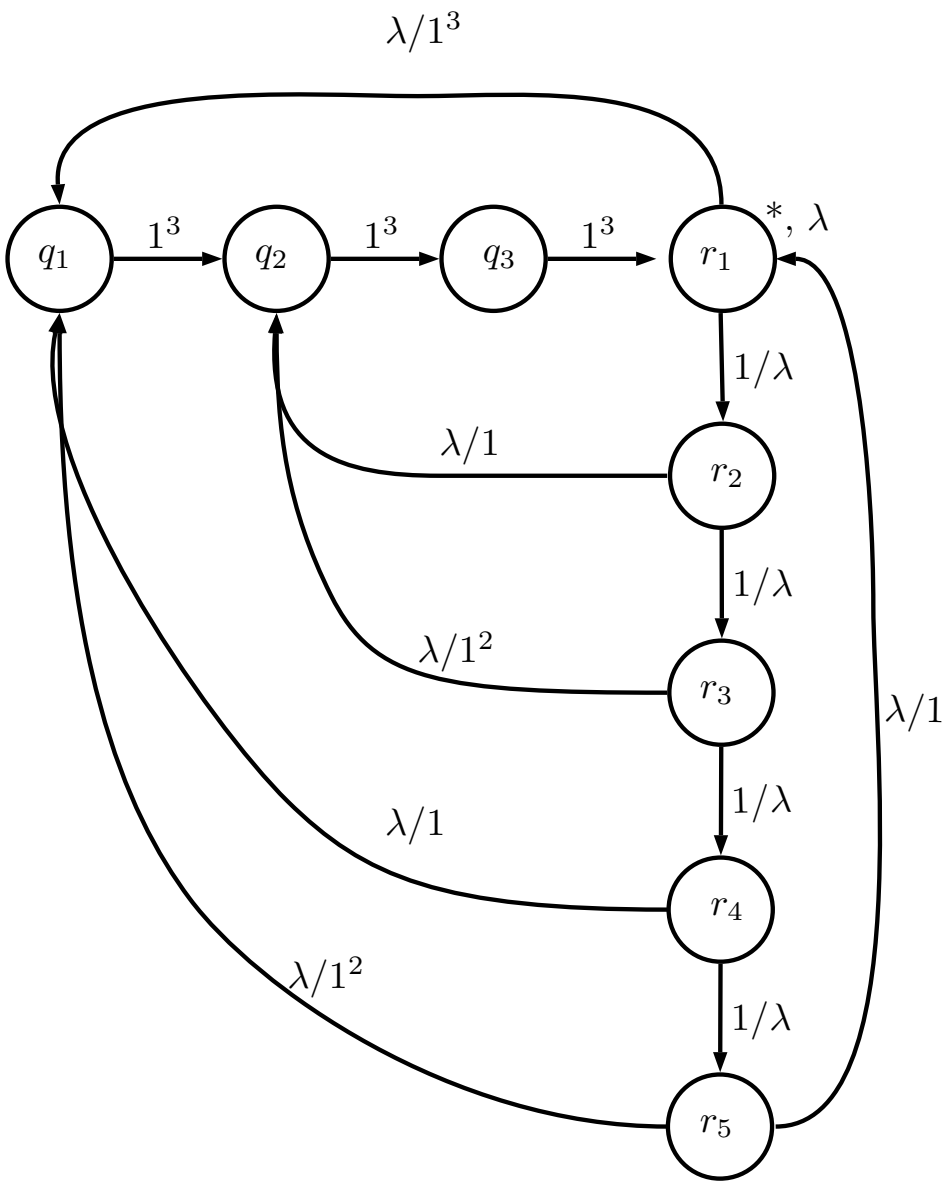
Пусть автономный автомат с магазинной памятью $P(s) = \{Q, B, \Gamma, \varphi, \psi, \eta, r_h, \lambda\} \in \mathcal{M}_0(n,1,k)$, где $0 < s < n$, $B = \{0,1\}$, $Q = \{q_1, ..., q_{n-s}, r_1, ..., r_s\}$, $\Gamma = \{1\}$, $h = (((k-1)(n-s+1)+2) \mod s) + 1$

$$\psi(q,z) = \begin{cases} 1, & q = q_h,\ z = \lambda, \\ 0, \end{cases}$$

$$\varphi(q,z) = \begin{cases} q_{i+1}, & q = q_i,\ i \neq n-s, \\ r_1, & q = q_{n-s}, \\ r_{i+1}, & q = r_i,\ z = 1, \\ q_1, & q = r_h,\ z = \lambda, \\ q_{1+[\frac{(h-1-i) \mod s}{k-1}]}, & q = r_i,\ i \neq h,\ z = \lambda, \\ q, \end{cases}$$

$$\eta(q,z) = \begin{cases} 1^k, & q = q_i, \\ 1^k, & q = r_h,\ z = \lambda, \\ 1^{k-1-((h-1-i) \mod s) \mod (k-1)}, & q = r_i,\ i \neq h,\ z = \lambda, \\ \lambda, \end{cases}$$

Ниже приведем диаграмму этого автомата для $n = 8$, $k = 3$ и $s = 5$. Переходы автомата описываются следующим шаблоном z/η, то есть из данного состояния, при значении верхнего символа магазина z, автомат записывает на выходную ленту пару (q, z), а в магазине стирает последний символ и дописывает слово η. Следующее состояние указывает стрелка.



Опишем функционирование описанного выше автомата $P(s)$ и поясним его канонические уравнения. Автомат начинает работу из состояния r_h и с пустым магазином. Далее автомат максимально заполняет магазин, проходя по состояниям $q_1, ..., q_{n-s}$ до тех пор, пока не попадает в стирающий цикл $r_1, ..., r_s$. В состоянии r_1 в магазине записано

$(k-1)(n-s+1)+1$ символов. Так как дальше при каждом заполнении магазина мы будем уменьшать на единицу количество записываемых символов, то состояния, в которых, магазин становится пустым, будут меняться последовательно. То есть если мы стартовали из состоянии r_{i+1} при пустом магазине, то, заполнив и опустошив магазин, автомат окажется в состоянии r_i. Исходя из этого, мы и получаем формулу для номера начального состояния. Мы подберем r_h таким, чтобы, заполняя магазин максимально возможным количеством символов, после стирания их попасть в состояние r_{h-1}. Отсюда получаем, что

$$h = (((k-1)(n-s+1)+2) \mod s)+1.$$

Следующим требующем объяснения моментом в описании уравнений автомата является его поведение при опустошении магазина, то есть в состоянии r_i и $z=\lambda$. По сказанному выше в состоянии r_h автомат пишет максимально возможное количество символов в магазин. Значит, из этого состояния при пустом магазине автомат должен перейти в состояние q_1 и записать при этом слово длины k в магазин. При следующем опустошении магазина мы окажемся в состоянии r_{h-1}. Из этого состояния начинается заполнение магазина. Причем автомат должен записать на единицу меньше символов в магазин. Следовательно, из состояния r_{h-1} автомат перейдет в состояние q_1, и в магазин будет записано слово длины $k-1$. Продолжая опустошать магазин, автомат будет писать на 1 символ меньше и переходить в состояние q_1 до тех пор, пока не придётся записать один символ. После этого мы уже не сможем перейти в состояние q_1, так как зациклимся. Следовательно, мы должны будем перейти в состояние q_2 и записать в магазин $k-1$ символ по той же причине. И далее при переходе из стирающего цикла мы будем писать от $k-1$ до 1 символа в магазин, после чего будем менять состояние перехода.

Подсчитаем длину периода $L(P(s))$. Удобно считать стирающие такты и записывающие по отдельности:

$$L(P(s)) = \tau + \tau,$$

где

$$\tau = \sum_{i=0}^{s-1}((n-s)(k-1)+1-i) = s(k-1)(n-s+1)+s-\frac{s(s-1)}{2},$$

$$\tau = s(n-s+1) - \sum_{i=0}^{s-2}[\frac{i}{k-1}].$$

Таким образом, длина периода сгенерированной им последовательности равна

$$L(P(s)) = sk(n-s+1) + s - \frac{s(s-1)}{2} - \sum_{i=0}^{s-2}[\frac{i}{k-1}]$$

Лемма 1. *Для натуральных s, $k > 1$ выполнено*

$$\frac{s^2}{2(k-1)} - s \le \sum_{i=0}^{s-2}[\frac{i}{k-1}] \le \frac{s^2}{2(k-1)} + \frac{3s}{2}$$

Доказательство. Пусть $f(s) = \sum\limits_{i=0}^{s-2}[\frac{i}{k-1}]$. Тогда

$$f(s) = (k-1)\sum_{i=0}^{[\frac{s}{k-1}]-1} i + [\frac{s}{k-1}](s \mod (k-1)) =$$

$$= (k-1)\frac{[\frac{s}{k-1}]([\frac{s}{k-1}]-1)}{2} + [\frac{s}{k-1}](s \mod (k-1))$$

Отсюда получаем, что

$$f(s) \le (k-1)\frac{\frac{s}{k-1}(\frac{s}{k-1}-1)}{2} = \frac{s^2}{2(k-1)} - \frac{s}{2}$$

и

$$f(s) \ge (k-1)\frac{(\frac{s}{k-1}+1)\frac{s}{k-1}}{2} + s = \frac{s^2}{2(k-1)} + \frac{3s}{2}.$$

Так как

$$\sum_{i=0}^{s-2}[\frac{i}{k-1}] = f(s) - [\frac{s-1}{k-1}],$$

то

$$\frac{s^2}{2(k-1)} - s \le \sum_{i=0}^{s-2}[\frac{i}{k-1}] \le \frac{s^2}{2(k-1)} + \frac{3s}{2},$$

что и требовалось доказать.

□

Применяя лемму, получаем, что

$$L(P(s)) \geq sk(n-s+1)+s-\frac{s(s-1)}{2}-\frac{s^2}{2(k-1)}-\frac{3s}{2} = sk(n-s+1)-\frac{ks^2}{2(k-1)}$$

Полагая $P = P(s)$ при $s = [\frac{k-1}{2k-1}n]$, получаем, что

$$L(P) \geq [\frac{k-1}{2k-1}n]k(n-[\frac{k-1}{2k-1}n]+1) - \frac{k([\frac{k-1}{2k-1}n])^2}{2(k-1)} \geq$$

$$\geq (\frac{k-1}{2k-1}n-1)k(n-\frac{k-1}{2k-1}n+1) - \frac{k(\frac{k-1}{2k-1}n)^2}{2(k-1)} =$$

$$= \frac{k(k-1)}{4k-2}n^2 - \frac{1}{2k-1}n - 1.$$

Данный пример доказывает нижнии оценки на $L(n,1,k)$.

Теорема 2. *При $k > 1$ и $n \to \infty$*

$$L(n,1,k) \geq \frac{k(k-1)}{4k-2}n^2(1+o(1)).$$

Теорема 3. *При $n > 1$ и $k \to \infty$*

$$L(n,1,k) \geq \frac{n^2}{4}k(1+o(1)).$$

Доказательство верхней оценки L(n,1,k)

Сформулируем и докажем несколько вспомогательных утверждений.

Лемма 2. *Пусть P — автомат с магазинной памятью из $\mathcal{M}'_0(n,1,k)$. Тогда существует автомат с магазинной памятью P' из $\mathcal{M}'_0(n,1,k)$, который в процессе функционирования не бывает с пустым магазином два такта подряд, и периоды выходных последовательностей автоматов P и P' отличаются не более чем на n.*

Доказательство. Пусть автомат P при очередном такте стирает последний символ из магазина, оказываясь в некотором состоянии q, и далее проходит еще несколько состояний, не делая записей в магазин. После чего попадает в состояние q_1, в котором пишет непустое слово 1^ℓ и переходит в состояние q_2. Тогда можно трансформировать автомат P так,

чтобы из состояния q автомат сразу переходил в q_2 и писал при этом в магазин 1^ℓ. Делая такую трансформацию для всех аналогичных состояний, получаем автомат P', который удовлетворяет условием леммы, так как внутри одного периода автомат может быть с пустым магазином не более n раз. □

Простая верхняя оценка

Теперь непосредственно приступим к доказательству верхней оценки на $L(n, 1, k)$.

Лемма 3. *Пусть P — автомат с магазинной памятью из класса $\mathcal{M}'_0(n, 1, k)$. Тогда*

$$L(P) \leq n(h_{max} + 1),$$

где $h_{max} = \max\limits_t |\gamma(t)|$ — максимальное количество символов, которое может быть записано в магазине.

Доказательство. Заметим, что из определения класса автоматов $\mathcal{M}'_0(n, 1, k)$ следует, что h_{max} всегда существует, то есть $h_{max} < \infty$. Внутри одного периода автомат может находиться в состоянии q только с разными состояниями магазина от пустого до содержащего h_{max} символов. Суммируя по всем состояния, получаем требуемую оценку. □

Утверждение 1. *При $k > 1$*

$$L(n, 1, k) \leq (k - 1)n^2 + 2n.$$

Доказательство. Так как среди n состояний должно быть хотя бы одно стирающее, то $n-1$ пишущее состояние не может записать больше $n(k-1)+1$, то есть $h_{max} \leq n(k-1)+1$. Подставляя эту оценку в предыдущую лемму, получаем требуемое. □

Случай пишущего автоматного цикла

Лемма 4. *Пусть P — автомат с магазинной памятью из $\mathcal{M}'_0(n, 1, k)$. Если в P есть достижимый пишущий автоматный цикл, то период сгенерированной P последовательности равен длине этого цикла.*

Доказательство. Если в P есть достижимый пишущий цикл, то автомат не может его покинуть, так как магазин уже никогда не будет пустым в силу неотрицательности индекса. Значит, период будет равен длине цикла. □

Замечание. В силу доказанной леммы далее не имеет смысл рассматривать автоматы с достижимыми пишущими циклами. Будем считать, что если в автомате есть достижимый цикл, то он стирающий.

Случай без автоматных циклов

В этом разделе будет дана оценка на максимальную длину периода выходной последовательсти для автомата без стирающих циклов.

Лемма 5. *Пусть P — автомат с магазинной памятью из класса $\mathcal{M}'_0(n,1,k)$. Если P не имеет автоматных циклов, то период сгенерированной P последовательности не превосходит $\frac{k-1}{k}n^2+2n$.*

Доказательство. Оценим h_{max}. Так как в P нет автоматных циклов, то h_{max} не может быть большим. Максимально возможное значение h_{max} можно получить следующем образом. Необходимо в автомате иметь максимально возможное число w пишущих по k символов состояний, так чтобы оставшихся $s=n-w$ состояний хватило, чтобы стереть то, что было записано. Все стирания должы быть сделаны в разных состояниях, так как стирающих циклов нет. Отсюда получаем следующее условие:

$$h_{max} \le (w+1)(k-1)+1 = s.$$

Решая, получаем, что

$$h_{max} \le s = \frac{k-1}{k}n+1.$$

Подставляя h_{max} в полученную выше оценку, получаем требуемое. □

Обозначим $L_0(n,k)=\frac{k-1}{2k}n^2+5n$

Утверждение 2. *Пусть P — автомат с магазинной памятью из класса $\mathcal{M}'_0(n,1,k)$. Если P не имеет автоматных циклов или имеет только недостижимые пищущие автоматные циклы, то период сгенерированной P последовательности не превосходит $L_0(n,k)$.*

Доказательство. При функционировании автомата P найдется последовательность тактов от t_1 до t_2, когда из пустого магазина автомат заполняет магазин до уровня в h_{max} символов, то есть $\gamma(t_1)=\lambda$, $\gamma(t_2)=1^{h_{max}}$ и $\gamma(t)\neq\lambda$ при $t_1<t\le t_2$. Очевидно, что каждое состояние $q(t)$ при $t_1<t\le t_2$ не может встречаться в одном периоде больше, чем

$|\gamma(t)|+1$ раз в силу определения h_{max}. Пусть $h_{max} = 1 + h_0 + h_1(k-1)$, где $0 \le h_0 < k-1$. Нетрудно видеть, что в отрезке от t_1+1 до t_2 найдутся такие t_i, что будет выполнено $|\gamma(t_i)| \le (k-1)i+1$ при $i = 1, ..., h_1$ и $q(t_i) \in W$. Учитывая это, получаем, что

$$L(P) \le (h_{max}+1)(n-h_1) + \sum_{i=1}^{h_1}(2+i(k-1)) =$$

$$= (h_{max}+1)n - \sum_{i=1}^{h_1}(h_{max} - 2 - i(k-1)) =$$

$$= (h_{max}+1)n - \sum_{i=1}^{h_1}(h_0 + (h_1 - i)(k-1) - 1) =$$

$$= (h_{max}+1)n + h_1 - h_0 h_1 - \frac{(k-1)h_1(h_1-1)}{2} =$$

$$= (h_{max}+1)n + \frac{h_1(k+2-h_0-h_{max})}{2} \le (h_{max}+1)n + \frac{h_{max}(k+2-h_{max})}{2(k-1)}.$$

Каждому состоянию q сопоставим число $h(q)$, равное максимальному числу символов в магазине, которое может быть при достижении этого состояния. Заметим, что оценку удалось улучшить за счет уточнения функции $h(q)$ для некоторых пишущих состоятий q пользуясь тем, что автомат за один такт может писать ограниченное количество символов. Теперь сделаем аналогичное уточнение при стирании магазина, то есть для стирающих состояний.

Покажем, что в P для любого натурального d такого, что $1 \le d < h_{max}$, найдется такое стирающее q, что $h(q) = d$. Рассмотрим последовательность тактов от t_2 до t_3, когда автомат стирает магазин от h_{max} до пустого, то есть $\gamma(t_2) = 1^{h_{max}}$, $\gamma(t_3) = \lambda$ и $\gamma(t) \ne \lambda$ при $t_2 < t < t_3$. В этом отрезке найдется такой номер t', что $q(t') = q_0 \in S$ и $|\gamma(t')| = d$. Если $h(q_0) = d$, то заканчиваем процедуру поиска. Если $h(q_0) > d$, то это означает, что найдется момент времени t_4 такой, что $q(t_4) = q_0$ и $|\gamma(t_4)| > d$. Тогда пусть t_5 таково, что $\gamma(t_5) = \lambda$ и при $t_4 < t < t_5$ $\gamma(t_5) \ne \lambda$. На этом новом отрезке выберем аналогичным образом t'' такое, что $q(t'') = q_1 \in S$ и $|\gamma(t')| = d$ и так далее. Возможны два результата работы этой процедуры: мы найдем такое q_i, что $h(q_i) = d$ или последовательность $q_0, q_1, ..., q_\ell$ зациклится. Если последовательность зациклилась, то это означает, что

в автомате есть стирающий автоматный цикл, что противоречит условию. Значит, данная процедура всегда приводит к нахождению требуемого состояния.

Таким образом, мы можем понизить верхнюю оценку еще на $\frac{h_{max}(h_{max}-1)}{2}$, то есть получаем, что выполнено:

$$L(P) \leq (h_{max}+1)n + \frac{h_{max}(k+2-h_{max})}{2(k-1)} - \frac{h_{max}(h_{max}-1)}{2}.$$

Максимизируя выражение по h_{max} при условии, что $0 \leq h_{max} \leq \frac{(k-1)n}{k} + 1$, получаем, что $L(P) \leq \frac{k-1}{2k}n^2 + 5n$, что и требовалось доказать.

□

Пример 2.

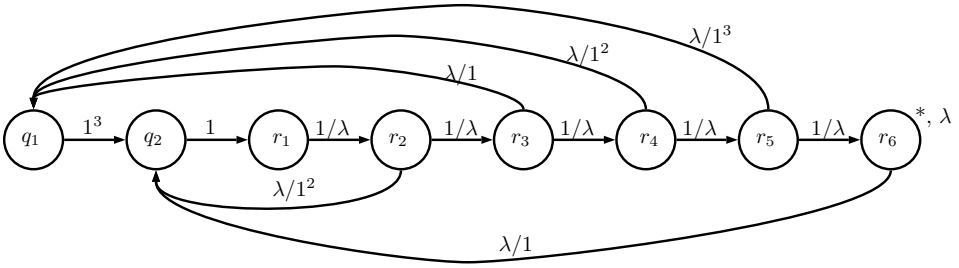
Для $n \geq 3$ и $k \geq 2$ рассмотрим автономный автомат с магазинной памятью $P_0 = \{Q, B, \Gamma, \varphi, \psi, \eta, r_s, \lambda\} \in \mathcal{M}_0(n, 1, k)$, где $s = n - 1 - [\frac{n-3}{k}]$, $x = s - 1 - (k-1)(n-s-1)$, $B = \{0, 1\}$, $Q = \{q_1, ..., q_{n-s}, r_1, r_2..., r_s\}$, $\Gamma = \{1\}$,

$$\psi(q,z) = \begin{cases} 1, & q = r_2,\ z = \lambda, \\ 0, & \end{cases}$$

$$\varphi(q,z) = \begin{cases} q_{i+1}, & q = q_i,\ i \neq n-s, \\ r_1, & q = q_{n-s}, \\ r_{i+1}, & q = r_i,\ i \neq s,\ z = 1, \\ q_{n-s}, & q = r_s,\ z = \lambda, \\ q_1, & q = r_{s-1},\ z = \lambda, \\ q_{n-s-[\frac{i-1}{k-1}]}, & q = r_i,\ 1 < i < s-1,\ z = \lambda, \\ q, & \end{cases}$$

$$\eta(q,z)=\begin{cases}1^k, & q=q_i,\ i\neq n-s,\\ 1, & q=q_{n-s},\\ \lambda, & q=r_i,\ z=1,\\ 1, & q=r_s,\ z=\lambda,\\ 1^x, & q=r_{s-1},\ z=\lambda,\\ 1^{k-1}, & q=r_i,\ z=\lambda,\ i \mod (k-1)=0,\\ 1^{i \mod (k-1)}, & q=r_i,\ z=\lambda,\ i \mod (k-1)\neq 0,\\ \lambda,\end{cases}$$

Ниже приведем диаграмму этого автомата для $n=8$ и $k=3$. Переходы автомата описываются следующим шаблоном z/η, то есть из данного состояния, при значении верхнего символа магазина z, автомат записывает на выходную ленту пару (q,z), а в магазине стирает последний символ и дописывает слово η. Следующее состояние указывает стрелка.



Опишем функционирование описанного выше автомата P_0 и поясним его канонические уравнения. Состояния автомата поделены на две группы: $\{q_1,...,q_{n-s}\}$ — состояния в которых происходит наполнение магазина, и состояния $\{r_1,...,r_s\}$ — в которых происходит опустошение магазина. Автомат начинает свою работу из состояния r_s с пустым магазином. Далее автомат переходит в первую группу состояний, где происходит запись в магазин, после заполнения автомат переходит во вторую группу состояний, а именно: в состояние q_1 с одном записанным символом в магазине. Далее происходит опустошение. После чего подобные итерации повторяется с той лишь разницей, что каждую последующую итерацию количество записанных в магазин символов увеличивается на 1 вплоть до значения $s-1$. После стирания $s-1$ символа автомат опять попадает в состояние r_s.

Аналогично предыдущему примеру получаем, что

$$L(P_0) = \frac{(s-1)s}{2} + (s-1)(n-s) + x - \sum_{i=0}^{s-2-x} [\frac{i}{k-1}]$$

Оценим $L(P_0)$, пользуясь леммой из предыдущего примера, и упростим выражение:

$$L(P_0) \geq \frac{(s-1)s}{2} + (s-1)(n-s) + x - \frac{(s-x)^2}{2(k-1)} - \frac{3(s-x)}{2} \geq sn - \frac{s^2 k}{2(k-1)} - s.$$

Далее подставим оценки на s:

$$L(P_0) \geq n(n-2-\frac{n-3}{k}) - \frac{(n-1-\frac{n-3}{k})^2 k}{2(k-1)} + (n-1-\frac{n-3}{k}) \geq \frac{k-1}{2k} n^2 - 3n - 2.$$

Замечание. Нижняя оценка, полученная в примере, асимптотически совпадает с доказанной верхней оценкой при $n \to \infty$.

Дополнительные определения

Перейдем к рассмотрению основного случая, когда в автомате с магазинной памятью есть стирающие автоматные циклы.

Пусть в автомате P из $\mathcal{M}'_0(n, 1, k)$ есть хотя бы один автоматный цикл. Выберем любой и обозначим C. Тогда для $q \in C$ определим множество состояний $W(q) \subseteq Q \backslash C$, из которых можно попасть в стирающий цикл через q:

$$W(q) = \{q' \in Q \backslash C \mid \exists t_1, t_2 : \ q(t_1) = q', \ q(t_2) = q, \ \forall t : \ t_1 \leq t < t_2,$$

$$\gamma(t) \neq \lambda, \ q(t) \notin C\}.$$

Заметим, что для различных $q_1 \in C$ и $q_2 \in C$ выполнено $W(q_1) \cap W(q_2) = \emptyset$. Для всех состояний из $W(q)$ будем говорить, что q является точкой входа в автоматный цикл.

Для стирающего цикла C определим множество состояний $W(C)$, которые попадают в автоматный цикл C:

$$W(C) = \bigcup_{q \in C} W(q).$$

Заметим, что для двух стирающих циклов C_1 и C_2 выполнено $W(C_1) \cap W(C_2) = \emptyset$.

Назовем окресностью стирающего цикла множество состояний $U(C) = C \cup W(C)$. Обозначим U_0 — множество состояний, которые не лежат ни в какой окресности стирающего цикла. Для автомата только со стирающими автоматными циклами $C_1, ..., C_d$ имеем следующее разложение:

$$Q = \bigsqcup_{i=1}^{d} U(C_i) \sqcup U_0.$$

Пусть P — автомат из $\mathcal{M}'_0(n, 1, k)$ с периодом выхода τ. Пусть $q(t)$ — последовательность состояний автомата и $\gamma(t)$ — последовательность слов, записанных в магазине, заданы каноническими уравнениями. Так как эти последовательности периодические, рассмотрим их лишь на номерах от 0 до τ. Пусть $t_1, ..., t_{d+1}$ — множество номеров на этом отрезке, когда магазин пуст. Не ограничивая общности, будем считать, что $0 = t_1 < t_2 < ... < t_d < t_{d+1} = \tau$. Рассмотрим полуинтервал $(t_i, t_{i+1}]$, на котором функционирует автомат P. На этой последовательности тактов автомат порождает подпоследовательности состояний $\{q(t)\}_{t_i+1}^{t_{i+1}}$ и слов $\{\gamma(t)\}_{t_i+1}^{t_{i+1}}$, записанных в магазин. Эту пару подпоследовательностей назовём этапом функционирования автомата и будем обозначать I_i. Обозначим длину этапа $|I_i|$ — количество тактов работы автомата в этапе. Для P однозначно определено представление периода в виде упорядоченного множества этапов $(I_1, I_2, ..., I_d)$. Обозначим это отображение $I(P)$. Описание функционирование автомата как последовательности этапов важно, так как имеет довольно интересные свойства, описываемые в следующей лемме.

Лемма 6. *Пусть P — автомат из $\mathcal{M}'_0(n, 1, k)$ и для него выполнено $I(P) = (I_1, ..., I_d)$. Тогда выполнены следующие утверждения:*

1) *Для любой перестановки σ на d элементах найдется автомат P_σ из $\mathcal{M}'_0(n, 1, k)$ такой, что его период будет описываться последовательностью этапов $I(P_\sigma) = (I_{\sigma(1)}, ..., I_{\sigma(d)})$.*

2) *Для любого подмножества этапов $I_{j_1}, ..., I_{j_h}$ найдется автомат P' из $\mathcal{M}'_0(n, 1, k)$ такой, что $I(P') = (I_{j_1}, ..., I_{j_h})$.*

Доказательство. Нетрудно видеть, что оба автомата P_σ и P' получаются из автомата P изменением его поведения на пустом магазине. □

Случай одного стирающего цикла

Пусть в автомате P из $\mathcal{M}'_0(n,1,k)$ есть ровно один стирающий цикл C длины ℓ со стирающим индексом $-s$. Обозначим $C_W = C \cap W$ — все пишущие состояния автоматного цикла, а $C_S = C \cap S$ — все его стирающие состояния. Пусть $C_{S_0} = \{q \in C_S |\ \exists h > \ell : (q, 1^h) \Rrightarrow (q, \lambda)\}$, а $C_{S_1} = C_S \backslash C_{S_0}$. Нетрудно видеть, что $|C_{S_0}| = s$.

Для каждого состояния q из стирающего цикла C определим функцию стирания $f_C(q,h) : \times \to$ — минимальное количество тактов необходимое для достижение пустого магазина из состояния q с записанном в магазине словом длины h. Нетрудно видеть, что если ℓ — длина стирающего цикла, а s — абсолютное значение стирающего индекса C, то

$$h + \lfloor \frac{h}{s} \rfloor (\ell - s) \le f_C(q,h) \le h + \lceil \frac{h}{s} \rceil (\ell - s) = f_C^{max}(h).$$

Лемма 7. *В текущих обозначениях*

$$\sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) = \begin{cases} h_{max} l - \frac{s(s-1)}{2}, & s \le h_{max} - (k-1), \\ \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + h_{max}(\ell - s), s > h_{max} - (k-1),\ \ell \ne n, \end{cases}$$

где $s' = \min(s, h_{max} - (k-1))$.

Доказательство. Если $s \le h_{max} - (k-1)$, то

$$\sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) = \sum_{i=0}^{s-1} f_C^{max}(h_{max} - i) =$$

$$= \sum_{i=0}^{s-1} \left(h_{max} - i + \lceil \frac{h_{max} - i}{s} \rceil (\ell - s) \right) =$$

$$= h_{max} s - \frac{s(s-1)}{2} + (\ell - s) \sum_{i=0}^{s-1} \lceil \frac{h_{max} - i}{s} \rceil =$$

$$= h_{max} s - \frac{s(s-1)}{2} + (\ell - s) \sum_{i=0}^{s-1} \frac{h_{max} - i}{s} + \frac{(l-s)(s-1)}{2} =$$

$$= h_{max} s - \frac{s(s-1)}{2} + h_{max}(\ell - s) = h_{max} \ell - \frac{s(s-1)}{2}.$$

Если $s > h_{max} - (k-1)$, то

$$\sum_{i=0}^{s'-1} f_C^{max}(h_{max}-i) = \sum_{i=0}^{h_{max}-k} f_C^{max}(h_{max}-i) = \sum_{i=k}^{h_{max}} f_C^{max}(i) =$$

$$= \sum_{i=k}^{h_{max}} \left(i + \lceil \frac{i}{s} \rceil (\ell - s) \right) =$$

$$= \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + (\ell - s) \sum_{i=k}^{h_{max}} \lceil \frac{i}{s} \rceil =$$

$$= \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + (\ell - s) \left(\sum_{i=k}^{h_{max}-k+1} \lceil \frac{i}{s} \rceil + \sum_{i=h_{max}-k+2}^{h_{max}} \lceil \frac{i}{s} \rceil \right) =$$

$$= \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + (\ell - s) \left(\sum_{i=k}^{h_{max}-k+1} 1 + \sum_{i=h_{max}-k+2}^{h_{max}} 2 \right) =$$

$$= \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + (\ell - s) h_{max},$$

что и требовалось доказать.

□

Лемма 8. *Пусть P — автомат из $\mathcal{M}'_0(n,1,k)$ и пусть P удовлетворяет следующим условиям:*

1) *в P есть единственный автоматный цикл C с отрицательным стирающем индексом;*

2) *вне этого цикла стирающих состояний нет, то есть $S \subseteq C$.*

Тогда найдется такой автомат из P' из $\mathcal{M}'_0(n,1,k)$, удовлетворяющий тем же условиям, такой, что все состояния вне стирающего цикла при непустом магазине пишут ровно k символов в магазин, при этом выполнено

$$L(P) \leq L(P') + n.$$

Доказательство. Рассмотрим непустое $W(q_*)$ для некоторого $q_* \in C$. Рассмотрим все этапы, которые начинаются с состояния из $W(q_*)$. Любой такой этап можно разделить на две части: это заполнение магазина, когда текущее состояние не из стирающего цикла, и стирание магазина, когда автомат вошел в стирающий цикл. Заметим, что длина второй части зависит только от количества символов записанных в магазин. Проведем следующую трансформацию автомата. Во всех состояниях q из $W(q_*)$ сделаем $\eta(q,1) = 1^k$, а также изменим переходы и запись в магазин по пустым состояниям стирающего цикла так, чтобы изменения коснулись только рассматирваемых этапов и для каждого рассматриваемого этапа количество символов, записанное в магазин, при первом попадании в стирающий цикл (то есть в q_*) не изменилось. Заметим, что при данной трансформации стирающая часть этапа будем иметь такую же длину, как и раньше. Может так оказаться, что количество тактов, которое автомат заполнял магазин уменьшилось. Если после трансформации среди состояний из $W(q_*)$ возникли недостижимые, то все такие состояния добавим в стирающий цикл как нейтральные сразу после q_*. Таким образом, каждый рассматриваемый этап может уменьшиться не более чем на 1.

Проводя подобные трансформации для всех непустых $W(q)$, построим требуемый автомат P'. Так как количество этапов не превосходит n, то будет верна оценка

$$L(P) \leq L(P') + n,$$

что и требовалось доказать.

□

Обозначим $L_1(n,k) = \frac{k(k-1)}{4k-2}n^2 + (8k+32)n$.

Утверждение 3. *Пусть P — автомат из $\mathcal{M}'_0(n,1,k)$ и пусть P удовлетворяет следующим условиям:*

1) *в P есть единственный автоматный цикл C с отрицательным стирающем индексом;*

2) *вне этого цикла стирающих состояний нет, то есть $S \subseteq C$.*

Тогда

$$L(P) \leq L_1(n,k).$$

Доказательство. Последовательно применяя леммы 2 и 8, далее можно рассматривать автомат P' такой, что при пустом магазине автомат P'

должен писать в магазин и для которого при $q \notin C$ выполнено $\eta(q,1) = 1^k$, при этом будет верно, что

$$L(P) \leq L(P') + 2n.$$

Так как начальное слово, записанное в магазине, пустое, то всё функционировние автомата устроено следующем образом. Из стирающего цикла при пустом магазине автомат заполняет магазин одним из двух способов: либо он выходит из стирающего цикла и заполняет магазин до тех пор, пока не попадает в стирающий цикл снова, либо, не выходя, переходит в другое состояние стирающего цилка. В стирающем цикле автомат опустошает магазин и так далее повторяется до зацикливания, то есть пока автомат не окажется опять в начальном состоянии с пустым магазином.

Пусть ℓ — длина стирающего цикла C. Пусть $s = |C_{S_0}|$ и $r = |C_{S_1}|$.

Пусть $I(P') = (I_1, I_2, ..., I_{r+s})$ — упорядоченное множество этапов автомата P' таково, что последнее состояние первых s этапов из C_{S_0}. Оценим отдельно $\sum\limits_{i=1}^{s} |I_i|$ и $\sum\limits_{i=s+1}^{s+r} |I_i|$.

Начнем с $\sum\limits_{i=s+1}^{s+r} |I_i|$. Эти этапы характерны тем, что в них автомат не проходит по всем состояним стирающего цикла. И максимальное количество символов в магазине не более чем r. С другой стороны, можно считать, что автомат сразу находится в стирающем цикле на протяжении всего этапа. Отсюда получаем оценку

$$\sum_{i=s+1}^{s+r} |I_i| \leq L_0(\ell - s, k) \leq \frac{k-1}{2k}(\ell - s)^2 + 5(\ell - s).$$

Теперь оценим $\sum\limits_{i=1}^{s} |I_i|$. Заметим, для всех этапов из рассматриваемого подмножества, в которых автомат не покидает стирающий цикл, можно оценить сверху сумму их длин как $(k+1)n$. Рассмотрим остальные этапы. Для них отдельно оценим "такты записи"и "такты стирания". Пусть τ — количество тактов, которые начинаются либо вне стирающего цикла, либо из стирающего цикла, но с пустым магазином, а τ — все остальные такты работы автомата.

Рассмотрим случай, когда найдется $q_* \in C$ такое, что $W(q_*) = Q \backslash C$. Заметим, что автомат P' не сможет записать больше, чем $h_{max} = (n - \ell + 1)(k-1) + 1$ символ в магазин. Учитывая, что внутри одного периода

автомат не может оказаться в одном и том же состоянии с одинаковым содержимом магазина, получаем:

$$\tau \leq \sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i),$$

где $s' = \min(s, h_{max} - (k-1))$ — количество оставшихся этапов.

Теперь оценим τ. При максимальном заполнении магазина автомат пройдет по всем пишушим состояним. Из стирающего цикла автомат не может перейти в одно и то же состояние более не более $k-1$ раза, кроме, тех состояний, в которые можно попасть только из стирающего цикла. В такие состояния автомат можем попасть не более k раз. Отсюда получаем, что

$$\tau \leq (n - \ell + 1)s' - \sum_{i=0}^{s'-2} [\frac{i}{k-1}]$$

Откуда получаем, что

$$\sum_{i=1}^{s} |I_i| \leq \sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) + (n - \ell + 1)s - \sum_{i=0}^{s'-2} [\frac{i}{k-1}] + (k+1)n.$$

Пусть теперь $W(q) \neq Q \backslash C$ для всех $q \in C$. Заметим, что если $s \leq (n-k)(k-1)+1$, то полученные оценки остаются в силе, так как, собирая состояния $Q \backslash C$ в одном $W(q)$ достигается большая длина этапов. Если же $s > (n-k)(k-1)+1$, то можно считать, что все непустые $W(q)$ для $q \in C$ содержат по одному состоянию, кроме одного, в котором лежат все остальные состояния. Этапы, которые начинаются с состояния из $W(q)$, где $|W(q)| = 1$ можно суммарно оценить сверху $2kn$, так как до входа в стирающий цикл не будет записано более $2k-1$ символов в магазин. Таким образом можно считать, что в случае, когда $W(q) \neq Q \backslash C$ для всех $q \in C$ оценка увеличится не более чем на $2kn$

Суммируя обе оценки, получаем, что

$$L(P') \leq \sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) + (n - \ell + 1)s' - \sum_{i=0}^{s'-2} [\frac{i}{k-1}] +$$

$$+ \frac{k-1}{2k}(\ell - s)^2 + 5(\ell - s) + 2kn.$$

Следовательно,

$$L(P) \le \sum_{i=0}^{s'-1} f_C^{max}(h_{max}-i) + (n-\ell+1)s' - \sum_{i=0}^{s'-2}[\frac{i}{k-1}] + \frac{k-1}{2k}(\ell-s)^2 +$$

$$+5(\ell-s) + 2kn + (k+1)n + 2n \le$$

$$\le \sum_{i=0}^{s'-1} f_C^{max}(h_{max}-i) + (n-\ell+2)s' - \frac{s'^2}{2(k-1)} + \frac{k-1}{2k}(\ell-s)^2 + 5(\ell-s) + (3k+3)n,$$

где $h_{max} = (n-\ell+1)(k-1)+1$ и $s' = \min(s, h_{max}-(k-1))$.

При $s \le (n-\ell)(k-1)+1$, получаем:

$$L(P) \le ((n-\ell+1)(k-1)+1)\ell - \frac{s(s-1)}{2} + s(n-\ell+2) -$$

$$-\frac{s^2}{2(k-1)} + \frac{k-1}{2k}(\ell-s)^2 + 5(\ell-s) + (3k+3)n \le$$

$$\le \max_{\substack{1 \le s \le \ell \le n,\\ s \le (n-\ell)(k-1)+1}} \left(((n-\ell+1)(k-1)+1)\ell - \frac{s(s-1)}{2} + s(n-\ell+2) - \right.$$

$$\left. -\frac{s^2}{2(k-1)} + \frac{k-1}{2k}(\ell-s)^2 + 5(\ell-s) \right) + (3k+3)n.$$

Максимизируя квадратичную функцию по s и ℓ получаем, что

$$L(P) \le \frac{k(k-1)}{4k-2}n^2 + 5kn + (3k+3)n = \frac{k(k-1)}{4k-2}n^2 + (8k+3)n.$$

Значит, $L(P) \le L_1(n,k)$ в этом случае.

При $s > (n-\ell)(k-1)+1$ и $\ell \ne n$ получаем:

$$L(P) \le \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + h_{max}(l-s) + s'(n-\ell+2) -$$

$$-\frac{s'^2}{2(k-1)} + \frac{k-1}{2k}(\ell-s)^2 + 5(\ell-s) + (3k+3)n =$$

$$= \frac{k-2}{2(k-1)}h_{max} + h_{max}(n-s) + \frac{k-1}{2k}(\ell-s)^2 + kh_{max} +$$

$$+\frac{7}{2}h_{max} + (k-1)(n-\ell) + 5(\ell-s) + \frac{k^2}{2} + \frac{1}{2} - 2(k-1) + (3k+3)n \leq$$

$$\leq nh_{max} - \frac{k-1}{k}\ell h_{max} + \frac{k-1}{2k}\ell^2 - \frac{2k-1}{2k(k-1)}h_{max}^2 +$$

$$+k(2h_{max}+2\ell-n)+4\ell-\frac{5}{2}h_{max}+n+3(k-1)+\frac{k^2}{2}+\frac{1}{2}+\frac{(k-1)^3}{2k}+(3k+3)n \leq$$

$$\leq nh_{max}-\frac{k-1}{k}\ell h_{max}+\frac{k-1}{2k}\ell^2-\frac{2k-1}{2k(k-1)}h_{max}^2+6kn+8n+5(k-1)+k^2+\frac{1}{2}$$

Подставляя $h_{max} = (n-\ell+1)(k-1)+1$, получаем

$$L(P) \leq \frac{n^2}{2} - \frac{n^2}{2(k-1)} + \frac{n^2}{2k(k-1)} - \frac{1}{2(k-1)} + n -$$

$$-k(n-\ell+1) - \frac{1}{2} + 6kn + 8n + 5(k-1) + k^2 + \frac{1}{2} \leq$$

$$\leq \frac{k-1}{2k}n^2 + 6kn + 9n + 5(k-1) + k^2 \leq \frac{k-1}{2k}n^2 + 7kn + 14n \leq L_1(n,k)$$

Остаётся лишь заметить, что в случае $\ell = n$, будет верна оценка

$$L(P) \leq L_0(n,k) + 2n + 2kn \leq L_1(n,k),$$

что и завершает доказательство.

□

Утверждение 4. *Пусть P — автомат из $\mathcal{M}'_0(n,1,k)$ и пусть в P есть единственный автоматный цикл C с отрицательным стирающем индексом. Тогда*

$$L(P) \leq L_1(n,k).$$

Доказательство. Применяя лемму 2, далее можно рассматривать автомат P' такой, что при пустом магазине автомат P' должен писать в магазин при этом будет выполнено:

$$L(P) \leq L(P') + n.$$

Рассмотрим $I(P') = (I_1, I_2, ..., I_d)$ — упорядоченное множество этапов автомата P'. Разобьём этапы на две группы. В первую включим все этапы, предпоследнее состояние которых не лежит в стирающем цикле C, в во вторую все остальные. По лемме 6 найдутся такие автоматы P'_1 и P'_2 из $\mathcal{M}'_0(n, 1, k)$, что $I(P'_1)$ будет состоять из первой группы этапов, а $I(P'_2)$ — из второй, причем будет выполнено, что

$$L(P') = L(P'_1) + L(P'_2).$$

Пусть n_0 — количество состояний в $L(P'_1)$. Тогда можно имеет место оценка

$$L(P'_1) \leq L_0(n_0, k) \leq \frac{k-1}{2k} n_0^2 + 5n_0.$$

Теперь оценим $L(P'_2)$. В P'_2 после стирающих состояний вне стирающего цикла магазин не становится пустым. Это означает, что можно трансформировать запись в магазин, не изменив при этом длину периода. Следовательно, можно считать, что автомат удовлетворяет предыдущей лемме, то есть для него верна оценка

$$L(P'_2) \leq \sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) + (n - \ell + 2)s' - \frac{s'^2}{2(k-1)} + \frac{k-1}{2k}(\ell - s)^2 +$$

$$+5(\ell - s) + (3k + 2)n,$$

$\mathrm{h}_{max} \leq (n - \ell - n_0 + 1)(k-1) + 1$ и $s' = \min(s, h_{max} - (k-1))$.

Суммируя обе оценки, имеем

$$L(P) \leq L(P'_1) + L(P'_2) + n \leq \frac{k-1}{2k} n_0^2 + 5n_0 + \sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) +$$

$$+(n - \ell + 2)s' - \frac{s'^2}{2(k-1)} + \frac{k-1}{2k}(\ell - s)^2 + 5(\ell - s) + (3k + 3)n,$$

где $h_{max} \leq (n - \ell - n_0 + 1)(k-1) + 1$ и $s' = \min(s, h_{max} - (k-1))$.

При $s \leq (n - \ell - n_0)(k-1) + 1$, получаем:

$$L(P) \leq \left(\frac{k-1}{2k} n_0^2 + 5n_0 + ((n-\ell-n_0+1)(k-1)+1)\ell - \frac{s(s-1)}{2} + s(n-\ell+2) \right.$$

$$\left. - \frac{s^2}{2(k-1)} + \frac{k-1}{2k}(\ell - s)^2 + 5(\ell - s) \right) + (3k+3)n,$$

Максимизируя по n_0, ℓ и s, получаем,что

$$L(P) \leq L_1(n,k).$$

При $s > (n - \ell - n_0)(k-1) + 1$ и $\ell \neq n$ получаем:

$$L(P) \leq \frac{k-1}{2k} n_0^2 + 5n_0 + nh_{max} - \frac{k-1}{k}\ell h_{max} + \frac{k-1}{2k}\ell^2 - \frac{2k-1}{2k(k-1)} h_{max}^2 +$$

$$+3(k-1) + \frac{k^2}{2} + \frac{1}{2} + \frac{(k-1)^3}{2k} + (3k+3)n \leq$$

$$\leq (\frac{k-1}{2k} n_0^2 + 5n_0 + n - \frac{k-1}{k}\ell)((n-\ell-n_0+1)(k-1)+1) + \frac{k-1}{2k}\ell^2 -$$

$$- \frac{2k-1}{2k(k-1)}(n-\ell-n_0)(k-1) + (4k+3)n + 3k$$

Максимизируя по n_0, ℓ , получаем,что

$$L(P) \leq L_1(n,k).$$

При $\ell = n$ получаем, что $n_0 = 0$, следовательно, будет верна оценка из предыдущего утверждения, что и завершает доказательство.

□

Общий случай

Теперь все готово для доказательства асимптотической верхней оценки для $L(n,1,k)$.

Теорема 4. *При* $k > 1$

$$L(n,1,k) \leq L_1(n,k).$$

Доказательство. Пусть P содержит d автоматных циклов. В случае $d = 0$ и $d = 1$ все доказано. Пусть $d \geq 1$. Заметим, что все циклы являтся стирающими, и обозначим их C_1,..., C_d. Имеет место следующее разбиение множества состояний:

$$Q = \bigsqcup_{i=0}^{d} Q_i,$$

где при $i > 0$ $Q_i = {}_i \cup W(C_i)$ — множество состояний, и, а Q_0 — все оставшиеся состояния, то есть множество состояний, из которых автомат не попадает ни в один стирающий цикл. Заметим, что внутри каждого этапа I все состояния лежат в одном и том же Q_i. Следовательно, для каждого Q_i можно выделить своё подмножество этапов, для которого по лемме 6 будет существовать автомат P_i, реализующий его. Так как каждый этап автомата P воздет в $I(P_i)$, то будет выполнено, что

$$L(P) = \sum_{i=0}^{d} L(P_i).$$

По построению P_0 — автомат без стирающего цикла, а остальные P_i — автоматы с одним стирающим циклов. Сделовательно, для каждого P_i будет выполнено $L(P_i) \leq L_1(|Q_i|, k)$. Значит,

$$L(P) \leq \sum_{i=0}^{d} L_1(|Q_i|, k) \leq L_1(\sum_{i=0}^{d} |Q_i|, k) = L_1(n, k),$$

что и требовалось доказать.

□

Заключение

В работе была получена асимптотическая верхняя оценка на максимальную длину периода выходной последовательности, сгенерированной автоматом с магазинной памятью с однобуквенным магазином. Построен пример автомата, на котором эта оценка достигается. Ранее автором была опубликована работа, в которой была допущена досадная неточность в доказательстве. В данной работе доказательство было полностью исправлено, что повлекло усложнение его конструкции. И хотя принципиально результат не поменялся, автор приносит свои извинения читателю.

Автор выражает благодарность Калачеву Глебу Вячеславовичу и проф. Гасанову Эльяру Эльдаровичу за продуктивные и конструктивные обсуждения, своему научному руководителю проф. Бабину Дмитрию Николаевичу за ценные замечания и внимание к работе.

Список литературы

[1] Oettinger A., Automatic syntatic analysis and the pushdown store, в сб. Structure of Language and its Mathematical Concepts, Proc. 12th Symposium on Applied Mathematics, 1961, 104-129.

[2] Schutzenberger M. P., On contex-free languages and pushdown automata, Inforc and contril, 6:3, 1963, 246-264.

[3] Chomsky N., Context-free gtammars and pushdown storage, Quarlerly Progress Report, № 65, Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambrig, Mass, 1962.

[4] Evey R.J., Applications of pushdown-store machines, Proc. AFIPS Fall Joint Computer Conference, 24, 1963, 215-227.

[5] Bar-Hillel Y., Perles M., Shamir E., On formal properties of simple phrase structure grammars. Z. Phonctik, Sprachwissensch. Kommunikationsforsch. 14, 1961, 143-172

[6] Ginsburg S., Rose G.F., Some recursively unsolvable problems in ALGOL-like languages, J. Assoc. Computing Machinety, 10, 1963, 175-195.

[7] Ginsburg S., Greibach S., Deterministic context free languages, Information and Control, Volume 9, Issue 6, 1966, 620-648.

[8] L.G. Valiant, M.S. Paterson, Deterministic one-counter automata, J. Comput. System Sci. 10 (1975) 340-350.

[9] M. Oyamaguchi, The equivalence problem for real-time d.p.d.a's, J. Assoc. Comput. Mach. 34 (1987) 731-760.

[10] S. Bohm, S. Goller, P. Jancar, Equivalence of deterministic one-counter automata is NL-complete, in: Proc. of STOC, ACM, 2013, pp. 131–140.

[11] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. М.:Наука, 1985.

[12] Бабин Д. Н. О полноте двухместных автоматных функций относительно суперпозиции. Дискретная математика. том 1, 4, 1989, 423-431.

[13] Иванов И.Е. Некоторые классы функций, вычислимые автоматами. Интеллектуальные системы, том 15, вып. 1, 2011, 361-378.

[14] Иванов И. Е. Улучшение нижней оценки на максимальную длину периода выходной последовательности автономного автомата с магазинной памятью. Интеллектуальные системы, том 20, вып. 4, 2016, 174-187.

Дополнения: решение экстремальных задач

Лемма 9. *Пусть*

$$g(n,k) = \max_{\substack{s,\ell \\ 1 \le s \le \ell \le n, \\ s \le (n-\ell)(k-1)+1}} \left(((n-\ell+1)(k-1)+1)\ell - \frac{s(s-1)}{2} + s(n-\ell+2) - \right.$$

$$\left. - \frac{s^2}{2(k-1)} + \frac{k-1}{2k}(\ell-s)^2 + 5(\ell-s) \right).$$

Тогда $g(n,k) \le \frac{k(k-1)}{4k-2}n^2 + 5kn$.

Доказательство. Максимум квадратичной функции достигается либо в критической точке (где все частные производные равны нулю), либо на границе области. Обозначим максимизируемую функцию через f. Найдем критические точки:

$$\begin{cases} \frac{\partial f}{\partial s} = n - 2\ell + \frac{\ell-s}{k} - \frac{s}{k-1} - 5/2 = 0, \\ \frac{\partial f}{\partial \ell} = 3\ell - n - 2s + k(n-2\ell+1) - \frac{(\ell-s)}{k} + 5 = 0 \end{cases}$$

Полученная система линейных уравнений не имеет решений, поэтому продолжим поиск решений на границе заданной области.

1. Пусть $s = 1$. При $s = 1$

$$f = 5\ell + n - \frac{1}{2k-2} + \frac{(k-1)(\ell-1)^2}{2k} + \ell(k-1)(n-\ell+1) - 3.$$

1.1. Найдем критические точки

$$\frac{\partial f}{\partial \ell} = 3\ell - n + k(n-2\ell+1) - \frac{\ell-1}{k} + 3 = 0.$$

Откуда находим:

$$\ell = \frac{3k - kn + k^2n + k^2 + 1}{2k^2 - 3k + 1}.$$

Подставляя в f получаем:

$$\frac{k(k-1)}{4k-2}n^2 + \frac{kn}{2} + \frac{11n}{4(2k-1)} + \frac{11n}{4} + \frac{k}{4} + \frac{12}{k-1} - \frac{121}{8(2k-1)} - \frac{5}{8} \le \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

1.2. Рассмотрим границу $\ell = 1$. Подставляя в f, получаем:

$$kn - \frac{1}{2(k-1} + 2 \leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

1.3. Рассмотрим границу $\ell = n$. Подставляя в f, получаем:

$$5n + kn - \frac{1}{2k-2} + \frac{(k-1)(n-1)^2}{2k} - 3 \leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

2. Пусть $s = (n-\ell)(k-1)+1$. При $s = (n-\ell)(k-1)+1$

$$f = \frac{5\ell}{2} + \frac{3n}{2} - \frac{1}{2(k-1)} + \frac{7k\ell}{2} - \frac{5kn}{2} - \frac{(n-1)^2}{2k} + \frac{n^2}{2} - \frac{5}{2}.$$

2.1. Найдем критические точки

$$\frac{\partial f}{\partial \ell} = \frac{7k}{2} + \frac{5}{2} = 0.$$

Критических точек нет, поэтому будем искать максимум на границе, а именно: $\ell = 1$ и $\ell = n$.

2.2. При $\ell = 1$ получаем

$$\frac{7k}{2} + \frac{3n}{2} - \frac{1}{2(k-1)} - \frac{5kn}{2} - \frac{(n-1)^2}{2k} + \frac{n^2}{2} \leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

2.3. При $\ell = n$ получаем

$$5n + kn - \frac{1}{2k-2} + \frac{(k-1)(n-1)^2}{2k} - 3 \leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

3. Пусть $s = \ell$. При $s = \ell$

$$f = \frac{\ell(2k - \ell - 2k\ell + 2kn + 5)}{2} - \frac{\ell^2}{2(k-1)}.$$

3.1. Найдем критические точки

$$\frac{\partial f}{\partial \ell} = k(n - 2\ell + 1) - \ell - \frac{\ell}{k-1} + 5/2 = 0.$$

Откуда находим:

$$\ell = \frac{(k-1)(2k + 2kn + 5)}{2k(2k-1)}.$$

Подставляя в f, получаем:

$$\frac{(k-1)(2k+2kn+5)^2}{8k(2k-1)} \le \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

Рассмотрим граничные значения ℓ.

3.2. Случай $\ell = 1$ уже был рассмотрен в 1.2.

3.3. При $\ell = n$ получаем

$$\frac{n(2k-n+5)}{2} - \frac{n^2}{2(k-1)} \le \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

4. Теперь s не лежит на границе. Пусть $\ell = n$. При $\ell = n$

$$f = 5n - 3s + kn - \frac{s(s-1)}{2} - \frac{s^2}{2k-2} + \frac{(n-s)^2(k-1)}{2k}.$$

Найдем критические точки

$$\frac{\partial f}{\partial s} = \frac{n-s}{k} - n - \frac{s}{k-1} - \frac{5}{2} = 0.$$

Откуда находим:

$$s = -\frac{(k-1)(5k-2n+2kn)}{2(2k-1)} < 0.$$

Следовательно, подставим граничное значение s, а именно: $s = 1$. Подставляя, получаем:

$$5n + kn - \frac{1}{2k-2} + (\frac{(k-1)(n-1)^2}{2k} - 3 \le \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

Во всех случаях получили верхнюю оценку

$$\frac{k(k-1)}{4k-2}n^2 + 5kn,$$

что и требовалось доказать.

□

Лемма 10. *Пусть*

$$g(n,k) = \max_{\substack{s,\ell,n_0 \\ 1 \le s \le \ell \le n, \\ s \le (n-\ell)(k-1)+1, \\ 0 \le n_0 \le n-\ell}} \left(\frac{k-1}{2k}n_0^2 + 5n_0 + ((n-\ell-n_0+1)(k-1)+1)\ell - \right.$$

$$-\frac{s(s-1)}{2}+s(n-\ell+2)-\frac{s^2}{2(k-1)}+\frac{k-1}{2k}(\ell-s)^2+5(\ell-s)\Big).$$

Тогда $g(n,k)\le\frac{k(k-1)}{4k-2}n^2+5kn$.

Доказательство. Максимум квадратичной функции достигается либо в критической точке (где все частные производные равны нулю), либо на границе области. Обозначим максимизируемую функцию через f. Найдем критические точки:

Найдем критические точки:

$$\begin{cases}\frac{\partial f}{\partial s}=n-2\ell+\frac{\ell-s}{k}-\frac{s}{k-1}-\frac{5}{2}=0,\\ \frac{\partial f}{\partial \ell}=\frac{(k-1)(2\ell-2s)}{2k}-(k-1)(\ell-n+n_0-1)-\ell(k-1)-s+6=0,\\ \frac{\partial f}{\partial n_0}=\frac{n_0(k-1)}{k}-\ell(k-1)+5=0\end{cases}$$

Решая систему, получаем:

$$\begin{cases}\ell=\frac{17k+5}{2k(k-1)},\\ s=k(\frac{n}{2}-\frac{5}{4})-\frac{n}{4}-\frac{k(n/4+35/8)-5/2}{k(2k-1)}-\frac{63}{8},\\ n_0=\frac{6}{k-1}+\frac{7}{2}\end{cases}$$

Решая систему, получаем:

$$\frac{25k}{16}+\frac{5n}{8}+\frac{48}{k-1}-\frac{5kn}{4}-\frac{(2n-5)^2}{32(2k-1)}+\frac{kn^2}{4}-\frac{25}{8k}-\frac{n^2}{8}+\frac{731}{32}\le\frac{k(k-1)}{4k-2}n^2+5kn.$$

Продолжим поиск решений на границе заданной области.

1. Случай, когда $n_0=0$, уже был полностью разобран.

2. Пусть теперь $n_0=n-\ell$. Тогда в этом случае можно оценить

$$L(P)\le(k+1)n+L_0(n-\ell,k)+L_0(\ell-s,k)+n\le L_0(n,k)+(k+2)n\le\frac{k(k-1)}{4k-2}n^2+5kn.$$

3. Пусть теперь n_0 лежит не на границе. 3.1. Пусть $s=1$. При $s=1$

$$f=5\ell+n+5n_0-\frac{1}{2k-2}+\frac{(k-1)(\ell-1)^2}{2k}-\ell(k-1)(\ell-n+n_0-1)+\frac{n_0^2(k-1)}{2k}-3.$$

3.1.1. Найдем критические точки

$$\begin{cases}\frac{\partial f}{\partial \ell}=\frac{(\ell-1)(k-1)}{k}-\ell(k-1)-(k-1)(\ell-n+n_0-1)+5=0,\\ \frac{\partial f}{\partial n_0}=\frac{n_0(k-1)}{k}-\ell(k-1)+5=0\end{cases}$$

Решая систему, получаем:

$$\begin{cases} \ell = \frac{5}{k-1} + \frac{k(n+1)-6}{k^2+2k-1}, \\ n_0 = \frac{k(k+kn-6)}{k^2+2k-1} \end{cases}$$

Подставляя в f, получаем:

$$7n+\frac{12}{k-1}-\frac{(51k)/2-7n+9kn+(3kn^2)/2-n^2/2+23/2}{k^2+2k-1}+\frac{n^2}{2}+3 \le \frac{k(k-1)}{4k-2}n^2+5kn.$$

Продолжим поиск решений на границе заданной области.

3.1.2. Пусть $\ell = 1$. При $\ell = 1$

$$f = n + 5n_0 - \frac{1}{2k-2} + (n-n_0)(k-1) + \frac{n_0^2(k-1)}{2k} + 2$$

Найдем критические точки

$$\frac{\partial f}{\partial n_0} = \frac{n_0(k-1)}{k} - k + 6 = 0$$

Откуда находим:

$$n_0 = \frac{k(k-6)}{k-1}.$$

Подставляя в f, получаем:

$$k(n+11/2) - 13/(k-1) - k^2/2 - 21/2 \le \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

3.1.3. Пусть $\ell = n$. Тогда $n_0 = 0$, случай был разобран.

3.2. Пусть $s = (n-\ell)(k-1)+1$. При $s = (n-\ell)(k-1)+1$

$$f = \frac{5\ell}{2}+\frac{3n}{2}+5n_0-\frac{1}{2(k-1)}+\frac{7k\ell}{2}-\frac{5kn}{2}+\ell n_0-\frac{n^2-2n+n_0^2+1}{2k}+\frac{n^2}{2}+\frac{n_0^2}{2}-kln_0-\frac{5}{2}.$$

3.2.1. Найдем критические точки

$$\begin{cases} \frac{\partial f}{\partial \ell} = \frac{7k}{2} + n_0 - kn_0 + \frac{5}{2} = 0, \\ \frac{\partial f}{\partial n_0} = \frac{n_0(k-1)}{k} - \ell(k-1) + 5 = 0 \end{cases}$$

Решая систему, получаем:

$$\begin{cases} \ell = \frac{17k+5}{2k(k-1)}, \\ n_0 = \frac{7k+5}{2(k-1)} \end{cases}$$

Подставляя в f, получаем:

$$\frac{3n}{2}+\frac{95}{2(k-1)}-\frac{5kn}{2}-\frac{n^2-2n+29/4}{2k}+\frac{n^2}{2}+\frac{169}{8}\le\frac{k(k-1)}{4k-2}n^2+5kn.$$

3.2.2. Пусть $\ell=1$. Тогда и $s=1$, случай был рассмотрен.

3.2.3. Пусть $\ell=n$. Тогда опять $s=1$ и случай был рассмотрен.

3.3. Пусть $s=\ell$. При $s=\ell$

$$f=5n_0-\ell((k-1)(\ell-n+n_0-1)-1)+\ell(n-\ell+2)-\frac{\ell(\ell-1)}{2}-\frac{\ell^2}{2k-2}+\frac{n_0^2(k-1)}{2k}.$$

3.3.1 Найдем критические точки:

$$\begin{cases}\frac{\partial f}{\partial \ell}=n_0-\ell-k(2\ell-n+n_0-1)-\frac{\ell}{k-1}/(k-1)+\frac{5}{2}=0,\\ \frac{\partial f}{\partial n_0}=\frac{n_0(k-1)}{k}-\ell(k-1)+5=0\end{cases}$$

Решая систему, получаем:

$$\begin{cases}\ell=\frac{(k-1)(12k+2kn+5)}{2k^3},\\ n_0=n-\frac{5}{k-1}-\frac{5}{2k^2}-\frac{2n+7}{2k}+1\end{cases}$$

Подставляя в f, получаем:

$$\frac{(7k+2kn-2k^2n-2k^2+5)(7k+2kn-2k^2n-22k^2+5)}{8k^3(k-1)}\le\frac{k(k-1)}{4k-2}n^2+5kn.$$

3.3.2. Пусть $\ell=1$. Тогда и $s=1$, случай был рассмотрен.

3.3.3. Пусть $\ell=n$. Тогда $n_0=0$ и случай уже был разобран.

3.4. Пусть теперь s лежит не на границе.

3.4.1. Пусть $\ell=1$. Тогда $s=1$ и случай уже был разобран.

3.4.2. Пусть $\ell=n$. Тогда $n_0=0$ и случай уже был разобран.

Во всех случаях получили верхнюю оценку

$$\frac{k(k-1)}{4k-2}n^2+5kn.$$

□

Лемма 11. *Пусть*

$$g(n,k)=\max_{\substack{\ell,\,n_0\\ \frac{k-1}{k}n+1\le\ell\le n,\\ 0\le n_0\le n-\ell}}\left(\frac{k-1}{2k}n_0^2+5n_0+(n-\frac{k-1}{k}\ell)\cdot\right.$$

$$\cdot((n-\ell-n_0+1)(k-1)+1)+\frac{k-1}{2k}\ell^2-\frac{2k-1}{2k(k-1)}(n-\ell-n_0)(k-1)\Big).$$

Тогда $g(n,k)\le\frac{k-1}{2k}n^2+kn+3n+23$.

Доказательство. Максимум квадратичной функции достигается либо в критической точке (где все частные производные равны нулю), либо на границе области. Обозначим максимизируемую функцию через f. Найдем критические точки:

$$\begin{cases}\frac{\partial f}{\partial n_0}=\ell-2n+4n_0-k(\ell-n+2n_0-2)+(n-2n_0)/k+4=0,\\ \frac{\partial f}{\partial \ell}=k+n_0-kn_0=0\end{cases}$$

Решая систему получаем, что

$$\begin{cases}\ell=n+\frac{6}{k-1}-\frac{n}{k},\\ n_0=\frac{1}{k-1}+1\end{cases}$$

Подставляя в f и упрощая, получаем:

$$\frac{k-1}{2k}n^2+\frac{11}{(2(k-1))}+\frac{11}{2}\le\frac{k-1}{2k}n^2+11.$$

Продолжим поиск решений на границе заданной области.
1. Случай $n_0=0$ уже был рассмотрен.
2. Пусть теперь $n_0=n-\ell$. При $n_0=n-\ell$

$$f=5n-5\ell+kn-\ell(k-1)-\frac{k(2k-1)}{2(k-1)}+\frac{(k-1)\ell^2}{2k}+\frac{(k-1)(\ell-n)^2}{2k}.$$

Найдем критические точки:

$$\frac{\partial f}{\partial \ell}=2\ell-k-n-\frac{2l-n}{k}-4=0.$$

Решая уравнение, получаем:

$$\ell=k/2+n/2+5/(2(k-1))+5/2.$$

Подставляя в f получаем:

$$3n-(13k)/4-27/(4(k-1))+(kn)/2-k^2/4+n^2/4-n^2/(4k)-27/4\le n^2/4+kn+3n.$$

3. Пусть теперь n_0 не на границе.

3.1. Случай $\ell = n$ уже был рассмотрен, так как в этом случае $n_0 = 0$.
3.2. Пусть теперь $\ell = \frac{k-1}{k}n + 1$. Тогда

$$f = 5n_0 - \frac{1}{2(k-1)} + kn_0 - \frac{n^2}{2k} - \frac{n_0^2}{k} - kn_0^2 + \frac{n^2}{2} + 2n_0^2 - 1/2.$$

Найдем критические точки:

$$\frac{\partial f}{\partial n_0} = 4n_0 - \frac{2n_0}{k} - k(2n_0 - 1) + 5.$$

Решая уравнение, получаем:

$$n_0 = \frac{k^2 + 5k}{2k^2 - 4k + 2}.$$

Подставляя в f получаем:

$$\frac{k}{4} + \frac{23}{2(k-1)} + \frac{9}{(k-1)^2} + \frac{n^2}{2} - \frac{n^2}{2k} + \frac{5}{2} \leq \frac{k-1}{2k}n^2 + 23 + k/4.$$

Во всех случаях получили, что максимум ограничен:

$$\frac{k-1}{2k}n^2 + kn + 3n + 23.$$

□

Биометрическое личностное шифрование

А. В. Поляков

В данной статье представлен протокол шифрования, в котором биометрические данные пользователя используются для генерации открытого ключа посредством нечеткого экстрактора. Это схема устойчива к адаптивной атаке с выбранным открытым текстом и обладает шифртекстом постоянного размера. определена модель безопасности и показано, что безопасность протокола основана на Билинейной задаче принятия решения Диффи-Хеллмана. Сравнительный анализ показывает большую устойчивость и безопасность предложенной схемы перед аналогами.

Введение

Асимметричная криптография стала элегантным решением задачи распределения ключей. Однако этот подход стало причиной возникновения другой проблемы. А именно, открытый ключ, в силу математических свойств асимметричных криптоалгоритмов, является набором случайных бит, не содержащих никакой информации о владельце, поэтому он не может служить средством аутентификации. Этот недостаток стал причиной появления иерархической системы сертификации открытых ключей. В настоящее время аутентификация пользователей происходит следующим образом:

1. Пользователь Алиса проходит процедуру проверки в удостоверяющем центре и получает сертификат;
2. Алиса посылает свой сертификат Бобу;
3. Боб получает сертификат удостоверяющего центра;
4. С помощью полученных сертификатов Боб производит аутентификацию Алисы.

Личностное шифрование впервые было предложено А. Шамиром [2] в 1984 году, которое возникло как идея упрощения этой схемы. Шамир предположил, что если бы появилась возможность использовать в качестве открытого ключа имя или почтовый адрес Алисы, то это лишило бы сложную процедуру аутентификации всякого смысла.

Под личностным шифрованием подразумевается криптосистема с открытым ключом, в которой пользователю разрешено выбрать адрес своей электронной почты либо телефонный номер в качестве открытого ключа вместо генерации случайным образом пары открытого и секретного ключей. Генератор секретного ключа вычисляет секретный ключ пользователя по личным данным пользователя и секретный мастер-ключ, после чего передает пользователю его секретный ключ.

Долгое время идея Шамира оставалась всего лишь красивой криптографической головоломкой, главным недостатком подобной схемы долгое время была невозможность использования биометрии в этой системе в силу ее изменчивости.

Однако в 2005 году в статье [3] была предложена концепция нечеткого личностного шифрования, в которой личностные характеристики были представлены набором атрибутов, а не строкой символов. В 2007 в статье [4] была предложена концепция цифровой подписи, основанной на пользовательской биометрии. В ней была предложена идея использования биометрических данных для создания открытого ключа, но не было предложено конкретной схемы. В 2008 году в статье [5] был впервые предложен протокол биометрического личностного шифрования. В 2010 году в статье [6] были предложены общие схемы биометрического личностного шифрования.

Однако протоколы, описанные в этих статьях, обладают следующими ограничениями: размер шифртекста линеен по пользовательским данным и требует большого количества операций при расшифровании. Целью настоящего исследования является устранение этих ограничений. В этой статье представлен новый протокол биометрического личностного шифрования, удовлетворяющий следующим свойствам:

- Постоянный размер шифртектста;
- Быстрый алгоритм генерации ключей;
- Эффективный алгоритм расшифрования. Представленный алгоритм расшифрования требует всего две операции спаривания, что

лучше, чем количество операций в аналогичных алгоритмах (линейное число от параметра, определяющего допустимое количество ошибок);

- Сводимость к билинейной задаче распознавания Диффи-Хеллмана. Сложность этой задачи считается выше сложности билинейной инверсионной задачи Диффи-Хеллмана, на которой основаны схемы [5], [6];

- Безопасность протокола. Протокол обладает стойкостью к атаке на основе адаптивно подобранных выбранной идентифицирующей информации и шифртекста (в то время как аналогичные схемы обладают устойчивостью только к атаке с выбранным открытым текстом).

Предварительные сведения и определения

Определение 1. *Пусть* $\mathbb{G}$ *и* $\mathbb{G}_1$ *- две мультипликативные циклические группы простого порядка* p*. Пусть* g *— порождающий элемент* $\mathbb{G}$*. Билинейным отображением называется отображение* $f : G \times G \to G_1$ *со следующими свойствами:*

1) билинейность: $f(u^a, v^b) = f(u, v)^{ab}$ $\forall u, v \in G, \forall a, b \in \mathbb{Z}_p$

2) невырожденность: $f(g, g) \neq 1_{\mathbb{G}_1}$

3) эффективная вычислимость: существует эффективный алгоритм, который вычисляет $f(u, v)$ $\forall u, v \in \mathbb{G}$*.*

Примерами таких отображений служат модифицированное спаривание Вейля и спаривание Тейта [7].

Определение 2. *(Билинейная задача распознавания Диффи-Хеллмана) Пусть дана группа* G *простого порядка* p*,* g *— порождающий элемент этой группы,* $g^a, g^b, g^c \in G$ *для некоторых случайным образом выбранных* $a, b, c \in \mathbb{Z}_p$*. Пусть дан* $Z \in \mathbb{G}_1$*, требуется выяснить, равен ли* Z *величине* $f(g, g)^{abc}$ *или нет.*

Определение 3. *Скажем, что алгоритм* $A(\varepsilon)$*, где* ε*— параметр алгоритма* A*, на выходе которого может быть получено значение* $\{0, 1\}$*, имеет преимущество* ε *в решении задачи распознавания Диффи-Хеллмана, если*

$$P(A(f(g, g)^{a,b,c}, g, g^a, g^b, g^c) = 1) - P(A(Z, g, g^a, g^b, g^c) = 1) \geq \varepsilon$$

Здесь $P(B)-$ частота события B. Частота вычисляется при условии, что бит на выходе алгоритма A является случайным.

Определение 4. *Будем говорить, что если не существует алгоритма, который с преимуществом ε за время t может решить билинейную задачу распознавания Диффи-Хеллмана, то выполняется предположение $(t, e)-$ безопасности.*

Определение 5. *Статистическим расстоянием между двумя вероятностными распределениями A и B называется величина*

$$SD(A, B) = \frac{1}{2} \sum_{v} (|P(A = v) - P(B = v)|).$$

Определение 6. *Мин-энтропией случайной величины A называется называется величина*

$$H_{\infty}(A) = -\log(\max_{a}(P(A) = a)).$$

Определение 7. *Функция $f(x) : \mathbb{Z} \to \mathbb{R}$ называется пренебрежимо малой, если для каждого полинома $p(x)$ существует такая константа N_p, что $f(x) \leq \frac{1}{p(x)}$ $\forall x \geq N_p$.*

Схема разделения секрета Шамира

В 1979 г. А. Шамир предложил схему разделения секрета между n сторонами [8] таким образом, что для восстановления секрета достаточно не менее k частей, и никакие (k-1) частей не дают никакой информации о секрете.

Пусть требуется разделить секрет S между n участниками так, чтобы восстановить его смогли $k \leq n$ человек.

Для этого выбирается простое число $p > S$. Оно задает конечное поле порядка GF(p). Над этим полем строится многочлен степени k-1:

$$F(x) = S + \sum_{i=1}^{k-1} a_i x^i \ mod \ p$$

В схеме разделения секрета Шамира ключ секрет делится на несколько частей, которые впоследствии передаются d различным участникам. Для восстановления секрета требуется определенное количество частей.

Здесь $S-$ разделяемый секрет, а коэффициенты $a_1, \ldots, a_{d-1} \in GF(p)$ выбираются случайным образом.

Для всех $i \in \{1, \ldots, n\}$, каждому участнику P_i ставится в соответствие уникальный элемент $\alpha_i \in GF(p)$, после чего ему посылается его доля секрета: $S_i = F(\alpha_i)$.

Любая группа участников M численностью не менее k может восстановить секрет, вычислив

$$F(x) = \sum_{P_i \in M} l_i(x) S_i,$$

где

$$l_i(x) = \prod_{p_j \in S, i \neq j} \frac{x - \alpha_i}{\alpha_i - \alpha_j} \; mod \; p$$

С другой стороны, никакая группа участников численностью меньше k не сможет восстановить секрет S.

Нечеткие экстракторы

Современная криптография базируется на использовании независимых равномерно распределенных случайных строк для создания секретных ключей. Строки, не обладающие свойствами случайности и не являющиеся воспроизводимыми (а именно такими строками являются биометрические шаблоны: действительно, отпечаток пальца, радужка глаза, лицо не является ни случайным, ни точно воспроизводимым при повторных измерениях), кажутся не столь привлекательными для криптографических целей. Тем не менее, в [1] предложен строгий и теоретически обоснованный подход использования таких строк в криптографических приложениях. Он базируется на использовании нового криптографического примитива: нечеткого экстрактора. Нечеткий экстрактор определяется следующим образом.

Пусть $\mathcal{M} = \{0,1\}^n-$ метрическое пространство с метрикой $\rho : \mathcal{M} \times \mathcal{M} \to \mathbb{Z}^+$.

Каждая точка метрического пространства представляет собой биометрический шаблон, метрика - расстояние между шаблонами $T, T' \in \mathcal{M}$.

Определение 8. *Нечетким экстрактором называется пара рандомизированных функций (Gen,Rep) со следующими свойствами:*

1) Функция $Gen : \mathcal{M} \to \{0,1\}^l \times P$ *получает на вход биометрический шаблон* $T \in \mathcal{M}$ *и возвращает строку* $R \in \{0,1\}^l$ *и вспомогательную информацию* $P \in \{0,1\}^*$*;*

2) Функция $Rep : \mathcal{M} \times \{0,1\}^* \to \{0,1\}^l$ *получает на вход элемент* $T' \in \mathcal{M}$ *и битовую строку* $P \in \{0,1\}^*$. *Свойство корректности нечетких экстракторов гарантирует, что если* $\rho(T,T') < t$ *и пара* (R,P) *является образом* $Gen(T)$, *то* $Rep(T',P) = R$. *Если* $\rho(T,T') \geq t$, *то значение Rep(T',P) не определено.*

3) Свойство безопасности гарантирует, что для любого распределения W *на* $\mathcal{M}$ *с мин-энтропией m, выход функции Gen близок к равномерному распределению даже при условии обладания информацией P, а именно, если* $Rep(W) \to (R,P)$, *то* $SD((R,P),(U_l,P)) \leq \varepsilon$.

Будем говорить, что нечеткий экстрактор эффективен, если функции *Rep* и *Gen* вычислимы за полиномиальное время.

Нечеткий экстрактор характеризуется работой с неравномерными распределениями строк и устойчивостью к ошибкам. Он надежно извлекает случайную строку R от входа T устойчивым к ошибкам способом. Если вход незначительно меняется по метрике ρ, то выход экстрактора R остается тем же. Для восстановления R по T' экстрактор использует публичные данные — строку P, однако R остается случайной при известном P.

В [1] приведен конкретный пример нечеткого экстрактора, построенного в пространстве $\mathcal{M} = \{0,1\}^n$ с метрикой Хэмминга и криптографической хэш-функцией $H : \{0,1\}^n \to \{0,1\}^l$.

Функция *Gen* принимает на вход биометрический шаблон T, возвращает $ID = H(T)$ и публичную строку $P = T \oplus C_e(ID)$, где C_e- функция кодирования. Функция *Rep* получает на вход публичную строку P и биометрический шаблон T' и вычисляет $ID' = C_d(T' \oplus P) = C_d(T' \oplus T \oplus C_e(ID)) = e' \oplus C_e(ID)$, где $e' = T' \oplus T$.

Тогда, если $\rho(T,T') < t$, то $ID = ID'$. Здесь C_d- функция декодирования, исправляющая до t ошибок.

Обработка биометрических данных

Обработка биометрических данных производится в четыре этапа:

1) Биометрия пользователя сканируется посредством оптического сенсора. Получается изображение биометрической модальности.

2) С помощью экстрактора из изображения выделяется вектор признаков (атрибутов).Каждый i-й атрибут связан с уникальным $\mu_i \in \mathbb{Z}_p^*$. Тогда личность моделируется набором биометрических атрибутов $(\mu_1, ..., \mu_n)$, где n- количество биометрических модальностей.

3) Каждый признак, формирующий вектор признаков, преобразуется в бинарную строку для генерации биометрического шаблона.

4) Нечеткий экстрактор используется для генерации уникальной строки ID посредством кодов, исправляющих ошибки, из биометрического шаблона b таким образом, что разрешается допустить t ошибок. То есть если $\rho(b, b') < t$, то $ID(b) = ID(b')$.

Определение биометрического личностного шифрования

Система личностного биометрического шифрования состоит из 4-х алгоритмов: установка, экстракция, шифрование, расшифрование.

Установка: дан параметр безопасности k и порог d, алгоритм порождает генерирует секретный мастер-ключ MK и множество публичных параметров PK системы.

Экстракция: дан биометрический шаблон T и секретный мастер-ключ MK, алгоритм возвращает конфиденциальный ключ пользователя K_T.

Шифрование: даны PK, биометрический шаблон T', сообщение M, алгоритм возвращает шифртекст C.

Расшифрование: дан секретный ключ K_T и шифртекст C, зашифрованный посредством биометрического шаблона T'. алгоритм возвращает текст M в случае, если $|T \cap T'| > d$, и останавливает работу в противном случае.

Модель угрозы

Определение 9. *Биометрическое личностное шифрование устойчиво к атаке с выбранным шифртекстом, если не существует алгоритма A, имеющего не пренебрежимо малое преимущество в следующей игре:*

Инициализация. Противник A генерирует биометрический шаблон T'.

Подготовительный этап. Претендент B запускает алгоритм установки и посылает публичные данные PK противнику A.

Первый этап. Противник A посылает запросы экстракции и расшифрования секретным ключом.

1. Запросы экстракции. A посылает запросы для личности γ_j такой, что $|\gamma_j \cap T'| < d$. B ответ на запрос B запускает алгоритм экстракции с целью получить секретный ключ K_{γ_j} и отправляет его A.

2. Запросы дешифрования. A отправляет запросы расшифрования на шифртекст C и биометрию γ_j, где $|\gamma_j - T'| \geq d$. B ответ, B запускает алгоритм экстракции с целью получить секретный ключ γ_j и затем запускает алгоритм расшифрования, чтобы получить открытый текст M, который отправляет A.

Задача: Противник A отправляет 2 сообщения M_0, M_1 B. B случайно выбирает число $\beta \in \{0, 1\}$ и шифрует текст M_β биометрией T'. Шифртекст отправляется к A.

Второй этап. A отправляет запросы экстракции и расшифрования как аналогично первому этапу.

Догадка: противник A случайно угадывает число $\beta' \in \{0, 1\}$ и побеждает, если $\beta' = \beta$. Преимущество противника A в этой игре определяется следующим образом:

$$Adv_A = |P(\beta' = \beta) - \frac{1}{2}|.$$

Определение 10. *Скажем, что биометрическая личностная система шифрования $(t, \varepsilon, q_E, q_D)-$ безопасна, если за время t противник посылает не более q_E запросов экстракции, q_D запросов расшифрования, и получает преимущество в игре не более ε.*

Система биометрического личностного шифрования

В данном разделе приводится список обозначений и описание системы биометрического личностного шифрования. У системы есть три участника: Генератор секретных ключей (Мерлин), Передатчик (Алиса) и Приемник (Боб). На этапе шифрования Алиса получает биометрию от Боба и публичный параметр P. Алиса выделяет из биометрии вектор признаков и вычисляет биометрическую строку с помощью нечеткого экстрактора. На этапе дешифрования предложенная система устойчива к ошибкам, возникающих из-за изменчивости биометрической информации.

Будем считать, что если $|T \cap T'| > d$, то $|b - b'| < t$ и $ID = ID'$. В этом случае Алиса может расшифровать текст, зашифрованный с помощью T', используя секретный ключ, соответствующий T, если b и b' находятся на расстоянии не более t друг от друга.

Список обозначений

$G-$ мультипликативная группа простого порядка p.

G_1- мультипликативная группа простого порядка p.

$g-$ порождающий элемент группы G.

$f : G \times G \to G_1-$ билинейное упорядочение

$M-$ сообщение C_e- функция кодирования кода, исправляющего ошибки

C_d- функция декодирования кода, исправляющего ошибки

$d-$ пороговое значение параметра устойчивости к ошибке, которое представляет собой расстояние между двумя биометрическими шаблонами для успешного расшифрования сообщения.

H_1 - криптографическая хэш-функция, $H_1 : \mathbb{Z}_p^* \times \{0,1\}^* \to \mathbb{Z}_p^*$

Подготовительный этап

Пусть k_0- параметр безопасности, Мерлин генерирует две мультипликативные группы G и G_1 простого порядка $p > 2^{k_0}$ и выбирает порождающий элемент $g \in G$. После этого Мерлин выбирает случайный элемент $g_1 \in G, s \in \mathbb{Z}_p^*$ и вычисляет $g_2 = g^s$ и выбирает порог ошибок $d \in \mathbb{Z}^+$.

После этого Мерлин публикует параметры $\{g, g_1, g_2, d\}$, мастер-ключ s он держит в секрете.

Экстракция

Сначала создается вектор признаков Боба $T = (\mu_1, ..., \mu_n)$ из изображения, полученного со сканера посредством алгоритма выделения признаков, входящего в состав любой биометрической системы. Каждый $\mu_i \in \mathbb{Z}_p^*, i \in \{1, ..., n\}$. Далее вычисляется $ID = H(b)$ от биометрического шаблона b.

Пусть дан вектор признаков T и ID, Мерлин создает секретный ключ следующим образом:

1) выбирается случайный полином степени $(d-1)$:

$$p(x) = a_0 + a_1 x + ... + a_{d-1} x^{d-1}$$

такой, что $p(0) = a_0 = s$.

2) Для $\mu_i \in T$ вычислить $d_{i,1} = (g_1 g^{H_1(T,ID)})^p(\mu_i)$, $d_{i,2} = g^p(\mu_i)$, $P = Gen(b, ID)$

3) Мерлин передает конфиденциальным образом ключ $\{d_{i,1}, d_{i,2}\}_{mu_i \in T}$ пользователю Бобу и публикует P.

Шифрование

Алиса получает биометрические данные Боба и публичные данные P. Алиса по ним извлекает T' и вычисляет $ID' = Rep(b', P)$. При $\rho(b, b') < t$ имеем $ID = ID'$.

При данном ID', T' и сообщении M Алиса делает следующее:

1) Выбирает случайное число $r \in \mathbb{Z}_p^*$ и вычисляет следующие величины:

$$C_1 = g^r$$

$$C_2 = (g^{H_1(T', ID')})^r$$

$$C_3 = f(g_1, g_2)^r M$$

и отправляет шифртекст $C = (T', C_1, C_2, C_3)$ Бобу.

Расшифровка

Дан шифртекст $C = (T', C_1, C_2, C_3)$, Боб расшифровывает C своим закрытым ключом K_T следующим образом:

1) если $|T \cap T'| < d$, то расшифровка прерывается;

2) если $|T \cap T'| \geq d$, то Боб выбирает любое подмножество $S \subseteq T \cap T'$, $|S| = d$ и вычисляет

$$M = C_3 \frac{f(C_2, \prod_{\mu_j \in S} d_{i,2}^{l_i(0)})}{f(C_1, \prod_{\mu_j \in S} d_{i,1}^{l_i(0)})}$$

Лемма 1. *Пусть M-открытый текст, в указанных выше обозначениях величины $C_1 = g^r$, $C_2 = (g^{H_1(T', ID')})^r$, $C_3 = f(g_1, g_2)^r M$,*

$d_{i,1} = (g_1 g^{H_1(T, ID)})^p(\mu_i)$,

$d_{i,2} = g^p(\mu_i)$,

тогда справедливо равенство

$$M = C_3 \frac{f(C_2, \prod_{\mu_j \in S} d_{i,2}^{l_i(0)})}{f(C_1, \prod_{\mu_j \in S} d_{i,1}^{l_i(0)})}$$

Доказательство: *Действительно,*

$$C_3\frac{f(C_2,\prod_{\mu_j\in S}d_{i,2}^{l_i(0)})}{f(C_1,\prod_{\mu_j\in S}d_{i,1}^{l_i(0)})}=f(g_1,g_2)^rM\frac{f((g^{H_1(T',ID')})^r,\prod_{\mu_j\in S}d_{i,2}^{l_i(0)})}{f(g^r,\prod_{\mu_j\in S}d_{i,1}^{l_i(0)})}=$$

$$=\frac{f((g^{H_1(T',ID')})^r,g^s)}{f(g^r,(g_1g^{H_1(T,ID)})^s)}Mf(g_1,g_2)^r=\frac{f((g^{H_1(T',ID')})^r,g^s)}{f((g^{H_1(T,ID)})^s,g^r)f(g_1,g^r)^s}Mf(g_1,g_2)^r=$$

$$=\frac{f((g^{H_1(T',ID')})^r,g^s)}{f((g^{H_1(T,ID)})^s,g^r)f(g_1,g^r)^s}Mf(g_1,g_2)^r=$$

$$\frac{f((g^h)^r,g^s)}{f((g^h)^s,g^r)f(g_1,g^r)^s}Mf(g_1,g_2)^r=M.$$

Здесь $h=H_1(T',ID')=H_1(T,ID)$ *в силу того, что* $ID=ID'$, *т.к.* $T\cap T'>d$ *и* $\rho(b,b')<t$.

Лемма доказана

Анализ безопасности

Теорема 1. *Пусть* $G-$*мультипликативная группа,* $|G|=p$, *где* $p-$ *простое, и для* G *выполняется* (t',ε') $--$*предположение безопасности. Тогда построенная система биометрического личностного шифрования* $(t,\varepsilon,q_E,q_D)-$ *безопасна, где* $\varepsilon=\varepsilon'$, $t=t'-d(t_{MULT}+t_{EXP})q_E$, *где* $t_{MULT}-$*время, требующееся на умножение,* $t_{EXP}-$*время на возведение в степень,* $d-$ *порог устойчивости системы к ошибкам,* q_E- *количество запросов экстракции.*

Доказательство: *Пусть существует* $(t,e,q_E,q_D)-$*противник Ева. Тогда может быть построен алгоритм* C, *решающий билинейную задачу распознавания Диффи-Хеллмана за время* t' *с вероятностью* ε'. *Под алгоритмом будем понимать кортеж* (g,g^a,g^b,g^c,Z) *из формулипровки билинейной задачи распознавания Диффи-Хелммана, где* Z *либо равно* $f(g,g)^{abc}$ *либо случайный элемент из* G_1.

Далее игра развивается следующим образом.

1. Инициализация. Евой выбирается биометрическая личность $T^*=(\mu_1^*,...,\mu_n^*)$.

2. Подготовительный этап. Ева на вход алгоритму C *устанавливает параметры* $g_1=g^a$, $g_2=g^b$ *и параметр ошибки* $d\in\mathbb{Z}^+$.*Алгоритм на выходе возвращает Еве публичные параметры* $P=(g,g_1,g_2,d)$

3.Хэш-запросы: будем считать, что Ева может посылать хэш-запросы на любом этапе игры. При получении запроса T_i, если в хэш-таблице существует (T_i, α_i, g_i^h), возвращается g^{h_i}. Если $T_i = T^*$, выбрать случайно $\alpha^* \in \mathbb{Z}_p$ и положить $g^{h^*} = g^{\alpha^*}$. В противном случае выбрать случайным образом $\alpha_i \in \mathbb{Z}_p$ и вычислить $g^{h_i} = \frac{g^{l_i}}{g_1}$.

Этап 1. на данном этапе Ева посылает запросы экстракции и запросы расшифрования секретного ключа.

1) Запросы экстракции. При получении запроса секретного ключа для $\gamma_j = (\mu_1, ..., \mu_n)$, где $|\gamma_j \cap T^*| < d$, алгоритм C устанавливает $\Gamma = \gamma_j \cap T'$ и пусть $\Gamma'-$ любое множество, удовлетворяющее следующим условиям: $\Gamma \subseteq \Gamma' \subseteq \gamma_j$, $|\Gamma'| = d - 1$.

Пусть $S = \Gamma' \cup \{0\}$. запустить указанный выше запрос для получения $(\gamma_j, \alpha_j, g^{h_j})$ из хэш-таблицы.

а) Для каждого $\mu_i \in \Gamma'$, выберем случайным образом $\lambda_i \in \mathbb{Z}_p$ и вычислим $(d_{i,1}, d_{i,2}) = ((g_1 g^{h_j})^{\lambda_i}, g^{\lambda_i})$. Для случайного полинома $p(x) \in \mathbb{Z}_p[x]$, $deg(p(x)) = d - 1$, $p(0) = b$, определим $\lambda_i = p(\mu_i)$. Таким образом, алгоритм C может успешно построить $(d_{i,1}, d_{i,2})$ для $\mu_i \in \Gamma'$.

б) Для каждого $\mu_i \in \gamma_j \setminus \Gamma'$, $i \in \{1, ..., n\}$, вычислить:

$$d_{i,1} = g_2^{l_0(\mu_i)\alpha_j} \prod_{\mu_k \in \Gamma'} (g_1 g^{h_j})^{l_k(\mu_i)\lambda_k},$$

$$d_{i,2} = g_2^{l_0(\mu_i)} \prod_{\mu_k \in \Gamma'} (g)^{l_k(\mu_i)\lambda_k}.$$

Заметим, что $g_1 g^{h_j} = g^{l_j}$, если $\gamma_j \neq T^*$.

Тогда

$$d_{i,1} = g^{\alpha_j l_0(\mu_i) b} g^{\alpha_j (\sum_{\mu_k \in \Gamma'} l_k(\mu_i) p(\mu_k))} = g^{\alpha_j (l_0(\mu_i) p(0) + (\sum_{\mu_k \in \Gamma'} l_k(\mu_i) p(\mu_k)))} =$$

$$= g^{l_j p(\mu_i)} = g^{l_j p(\mu_i)} = (g_1 g^{h_j})^{p(\mu_i)} = (g_1 g^{h_j})^{p(\mu_i)} =$$

$$(g_1 g^{H_1(\gamma_j, ID)})^{p(\mu_i)}$$

$$d_{i,2} = g^{l_0(\mu_i) b} g^{(\sum_{\mu_k \in \Gamma'} l_k(\mu_i) p(\mu_k))} = g^{l_0(\mu_i) p(0) + (\sum_{\mu_k \in \Gamma'} l_k(\mu_i) p(\mu_k))} = g^{p(\mu_i)}.$$

Таким образом, алгоритм C может успешно имитировать секретный ключ пользователя $\gamma_j = (mu_1, ..., \mu_n)$.

2. Запросы расшифрования

Для дешифровки запроса $C = (\gamma'_j, C_1, C_2, C_3)$ *пользователя* γ_j, *где* $|\gamma'_j \cap \gamma_j| \geq d$, *алгоритм* C *работает следующим образом:*

а) C *запускает указанный выше алгоритм экстракции секретного ключа для создания ключа* $K_{\gamma_j} = (d_{i,1}, d_{i,2})_{\mu_i \in \gamma_j}$;

б) C *выбирает любое множество* S, *удовлетворяющее условиям:* $S \subseteq \gamma_j \cup \gamma'_j$ *и* $|S| = d$. *После этого* C *вычисляет открытый текст* M *по лемме 1 и отправляет его Еве.*

Попытка взлома:

Противник Ева генерирует два сообщения M_0 *и* M_1. *Алгоритм* C *случайно выбирает* $\beta \in \{0,1\}$ *и шифрует* M_β *с помощью* T^*, *который получен от* b^*. *Шифртекст возвращается к Еве:*

$C^* = (T^*, C_1^*, C_2^*, C_3^*) = (T^*, g^c, (g^c)^{\alpha^*}, ZM_\beta)$

Если $Z = f(g,g)^{abc}$, *то* C^*- *корректная шифровка сообщения* M_β, *так как* $C_1^* = g^c$, $C_2^* = (g^c)^{\alpha^*} = (g^{\alpha^*})^c = (g^{h^*})^c = (g^{(T^*, ID)})^c$,

$C_3^* = ZM_\beta = f(g,g)^{abc} M_\beta = f(g_1, g_2)^c M_\beta$

2. Если Z *равномерно на* G_1, C_3^* *не зависит от* M_β. *Поэтому* C^* *не зависит от* β *с точки зрения Евы.*

Этап 2. Ева посылает запросы экстракции ключа и дешифрования как на этапе 1.

Предположение: Ева делает предположении о значении $\beta' \in \{0,1\}$. *Алгоритм* C *завершает игру следующим образом. Если* $\beta' = \beta$, *то* C *возвращает 1, что означает* $Z = f(g,g)^{abc}$. *В противном случае* C *возвращает 0, что означает, что* Z *выбрано случайным образом в* G_1.

Вероятностный анализ:

1) если $Z = f(g,g)^{abc}$, *то* $|P(\beta' = \beta) - \frac{1}{2}| \geq \varepsilon$

2) если $Z-$ *случайный элемент* G_1, *то* $P(\beta' = \beta) = \frac{1}{2}$

3)Отсюда

$$|P(C(f(g,g)^{abc}, g, g^a, g^b, g^c)) = 0| - P(C(Z, g, g^a, g^b, g^c)) = 0| \geq |(\frac{1}{2} \pm \varepsilon) - \frac{1}{2}| = \varepsilon$$

Временной анализ:

Время работы системы определяется умножением и возведением в степень на этапе запросов экстракции. Отсюда $t' = t + d(t_{MULT} + t_{EXP})q_E$.

Теорема доказана

Сравнение с существующими нечеткими системами личностного шифрования

Таблица 1: Сравнительный анализ

Система	Sahai [3]	Sarier [5]	Предложенная система
Размер открытого ключа	$u\|G\| + G_1$	$2\|G\|$	$3\|G\|$
Размер секретного ключа	nG	nG	$2n\|G\|$
Размер шифртекста	$n\|G\| + \|G_1\|$	$n\|G\| + \|M\|$	$2\|G\| + \|G_1\|$
Сложность генерации ключа	nt_{EXP}	nt_{EXP}	$2nt_{EXP}$
Сложность шифрования	$(n+1)t_{EXP}$	$t_{pair} + nt_{EXP}$	$3t_{EXP}$
Сложность расшифрования	dt_{PAIR}	dt_{PAIR}	$2t_{PAIR}$
Связанная задача	МБДХ	k-ИБДХ	БРДХ

Размер открытого и секретного ключей в [5] меньше, чем в предложенной схеме. При этом сложность генерации ключа на n (количество биометрических модальностей) операций возведения в степень больше, чем в [5]. Размер шифртекста в [6] равен $n|G| + |M|$, где $|M|-$ размер шифртекста. В предложенной схеме шифртекст имеет постоянный размер.

Сложность шифрования и дешифрования в предложенной схеме ниже, чем в [5].

При этом предложенная система основана на билинейной задаче распознавания Диффи-Хеллмана (БРДХ), в то время как в [5] система основана на задаче k-инверсной билинейной задаче диффи-Хеллмана, трудность которой ниже, чем БРДХ.

таким образом, предложенная схема обладает большей вычислительной эффективностью и более сильной безопасностью, чем [5]

Сравнительный анализ приведен в таблице 1.

Заключение

В этой главе была описана новая биометрическая система личностного шифрования, которая отличается от ближайших аналогов постоянным

размером шифртекста, меньшей сложностью шифрования и расшифрования и сводится к более трудной задаче, чем аналоги.

Список литературы

[1] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” in Proc. Eurocrypt, 2004, pp. 523–540.

[2] Shamir, A., 1984. Identity-Based Cryptosystems and Signature Schemes. Proc. Crypto, p.47-53.

[3] Sahai, A., Waters, B., 2005. Fuzzy Identity-Based Encryption. Proc. EUROCRYPT, p.457-473

[4] Burnett, A., Byrne, F., Dowling, T., Duffy, A., 2007. A biometric identity based signature scheme. Int. J.Network Secur., 5(3):317-326

[5] Sarier, N.D., 2008. A New Biometric Identity Based Encryption Scheme. Proc. ICYCS, p.2061-2066

[6] Sarier, N.D., 2010. Generic Constructions of Biometric Identity Based Encryption Systems. Proc. WISTP, p.90-105.

[7] Boneh, D., Franklin, M.K., 2001. Identity-Based Encryption from the Weil Pairing. Proc. CRYPTO, p.213-229.

[8] Shamir A. How to share a secret // Commun. ACM — New York City: ACM, 1979. — Vol. 22, Iss. 11. — P. 612-613.

[9] Cheon, J.H., 2006. Security Analysis of the Strong Diffie-Hellman Problem. Proc. EUROCRYPT, p.1-11

Компьютерные модели в геометрии и динамике

В. Ведюшкина (Фокичева)[*], А. Иванов[†], А. Тужилин[‡], А. Фоменко[§]

В работе описаны нетривиальные примеры моделирования сложных задач динамики и геометрии.

Важность компьютерного моделирования в современном мире трудно переоценить. Компьютерные модели играют важную роль не только при решении практических задач, но и при изучении чисто научных вопросов. Хорошая компьютерная модель часто позволяет не только опровергнуть гипотезу, но и сформулировать нетривиальную теорему, и даже наметить методы ее доказательства. Впрочем задачи, которые нужно моделировать, часто оказываются настолько сложны, что их непосредственное моделирование само становится нетривиальной задачей. Поэтому большой интерес представляют случаи, когда удается подменить одну задачу другой, более простой и наглядной, и, значит, легче поддающейся как изучению, так и моделированию. В данной работе мы приведем два таких нетривиальных примера. Первый относится к теории динамических систем. Как было недавно показано Фокичевой и Фоменко [11], многие классические динамические системы, описывающие движение твердого тела в тех или иных условиях, могут быть описаны с

[*]Ассистент кафедры дифференциальной геометрии и приложений, механико-математический факультет МГУ имени М.В.Ломоносова, e-mail: arinir@yandex.ru.

[†]Профессор кафедры дифференциальной геометрии и приложений, механико-математический факультет МГУ имени М.В.Ломоносова; профессор кафедры математического моделирования, МГТУ имени Н.Э.Баумана, e-mail: aoiva@mech.math.msu.su.

[‡]Профессор кафедры дифференциальной геометрии и приложений, механико-математический факультет МГУ имени М.В.Ломоносова, e-mail: tuz@mech.math.msu.su.

[§]Академик РАН, профессор, кафедры дифференциальной геометрии и приложений, механико-математический факультет МГУ имени М.В.Ломоносова, e-mail: atfomenko@mail.ru.

помощью более наглядных механических систем — биллиардов. Второй пример относится к метрической геометрии и связан с изучением кратчайших кривых в метрическом пространстве замкнутых ограниченных подмножеств некоторого метрического пространства. В качестве функции расстояния берется расстояние по Хаусдорфу. Оказывается, задача изучения множества кратчайших кривых, соединяющих пару точек в этом пространстве сводится к описанию реберных покрытий двудольных графов. Нетривиальный факт состоит в том, что количество таких покрытий не может быть любым. Первая такая «лакуна» была найдена в [36], где было показано, что среди натуральных чисел от 1 до 19 все, кроме 19, могут быть реализованы как количества реберных покрытий. Недавно последовательность «запрещенных» чисел удалось продолжить с помощью довольно сложного компьютерного моделирования.

Скрытые симметрии. Биллиарды и математическая физика.

Введение.

Интегрируемость биллиарда в плоской области, ограниченной эллипсом, замечена в работе [2] Дж. Д. Биркгофа. Интегрируемость геодезического потока на эллипсоиде следует из теоремы Якоби-Шаля. При стремлении меньшей полуоси эллипсоида к нулю движение по геодезическим переходит в движение по ломаным, целиком лежащим в образе эллипсоида – плоской области, ограниченной эллипсом. Интегрируемость биллиарда сохраняется, если перейти к плоским областям, ограниченным дугами эллипсов и гипербол одного софокусного семейства, на границе которых нет точек излома с углами $\frac{3\pi}{2}$. В этом случае все углы в точках излома равны $\frac{\pi}{2}$, поскольку софокусные квадрики пересекаются всегда под прямым углом. В книге [3] В. В. Козлов, Д. В. Трещёв заметили, что эти динамические системы вполне интегрируемы по Лиувиллю (т.е. имеется дополнительный независимый интеграл Λ), а именно, что интегрируемость данных систем эквивалентна малой теореме Понселе. Для системы плоского биллиарда в эллипсе построены координаты, в которых движение представляется в виде периодического движения по торам. Такие системы с точностью до лиувиллевой эквивалентности подробно изучены в работах [5, 6] В. Драгович, М. Раднович, а также [7, 8] В.В. Фокичевой.

В работах В.В. Фокичевой классифицированы все локально-плоские

биллиарды, ограниченные дугами софокусных эллипсов и гипербол (при этом не обязательно изометрично вложимые в плоскость), а также области, не обязательно являющиеся плоскими, полученные склейками элементарных областей вдоль выпуклых сегментов границ.
Далее, В.В.Фокичева исследовала топологию слоений Лиувилля на изоэнергетических поверхностях таких биллиардов, вычислив меченые молекулы Фоменко-Цишанга – инварианты лиувиллевой эквивалентности.

Две гладкие интегрируемые системы называются лиувиллево эквивалентными, если существует диффеоморфизм, переводящий слоение Лиувилля одной системы в слоение Лиувилля другой системы. Если гладкие торы Лиувилля на всюду плотном множестве являются замыканиями нерезонансных траекторий (как в большинстве невырожденных классических случаев интегрируемости), то лиувиллева эквивалентность систем означает, что они имеют "одинаковые" замыкания решений (т.е. интегральных траекторий) на трёхмерных уровнях постоянной энергии. В случае биллиардов торы Лиувилля, слоение Лиувилля и интегральные траектории системы являются кусочно-гладкими, поэтому нерезонансность почти всех торов Лиувилля нами пока подробно не изучалась. Тем не менее, слоение Лиувилля и лиувиллева эквивалентность здесь корректно определены.

Топологический тип слоения Лиувилля полностью определяется инвариантом Фоменко–Цишанга, который является некоторым графом с числовыми метками (см. теорему А. Т. Фоменко и Х. Цишанга в [14], а также в книге [4] А. В. Болсинова, А. Т. Фоменко). Анализируя большое число вычисленных на настоящее время меченых молекул как различных биллиардов, так и других интегрируемых системы с двумя степенями свободы, А. Т. Фоменко сформулировал следующую гипотезу: многие достаточно сложные случаи интегрируемости (например, в динамике твердого тела) можно "моделировать" значительно более наглядными топологическими биллиардами. В частности, это позволяет эффективно предъявлять устойчивые и неустойчивые периодические решения (траектории) интегрируемых систем. Эта гипотеза получила подтверждение в работе В.В.Фокичевой и А.Т.Фоменко [11]. А именно, для многих интегрируемых случаев динамики твердого тела для ряда изоэнергетических поверхностей вычисление инварианта Фоменко-Цишанга позволило обнаружить лиувиллеву эквивалентность этих систем топологическим биллиардам путём сравнения меченых молекул (см. [11]). Тем самым, образно говоря, локально-плоские интегрируемые биллиарды "наглядно моделируют" многие достаточно сложные случаи интегрируемости в ди-

намике твердого тела.

Инварианты интегрируемых систем

Определение 0.1. Пусть $(M_1^4, \omega_1, f_1, g_1)$ и $(M_2^4, \omega_2, f_2, g_2)$ — две интегрируемые по Лиувиллю системы на симплектических многообразиях M_1^4 и M_2^4, обладающих, соответственно, интегралами f_1, g_1 и f_2, g_2. Рассмотрим изоэнергетические поверхности $Q_1^3 = \{x \in M_1^4 : f_1(x) = c_1\}$ и $Q_2^3 = \{x \in M_2^4 : f_2(x) = c_2\}$. Интегрируемые гамильтоновы системы называются *лиувиллево эквивалентными*, если существует послойный диффеоморфизм $Q_1^3 \to Q_2^3$, который, кроме того, сохраняет ориентацию 3-многообразий Q_1^3 и Q_2^3 и ориентацию всех критических окружностей, см. [13].

Пусть (M^4, ω, f_1, f_2) – интегрируемая по Лиувиллю невырожденная гамильтонова система на симплектическом многообразии M^4, обладающая интегралами f_1 и f_2. Изоэнергетическое многообразие $Q^3 = \{x \in M^4 : f_1(x) = c_1\}$ расслоено на регулярные двумерные поверхности уровня функции f_2, а именно на торы, цилиндры или плоскости (в силу теоремы Лиувилля) и особые слои. Это слоение называется слоением Лиувилля. Многообразие Q^3 фактически представляет собой склейку регулярных окрестностей особых слоев друг с другом по граничным торам. Рассмотрим базу возникающего слоения Лиувилля на Q^3. Эта база является одномерным графом W, называемым графом Кронрода-Риба функции $f_2|_{Q^3}$. Структура слоения в малой окрестности особого слоя, отвечающего любой вершине этого графа, описывается комбинаторным объектом, называемым атомом. Граф, для каждой вершины которого указан соответствующий атом, называется инвариантом (грубой молекулой) Фоменко. В вершинах W расположены "атомы", описывающие соответствующие бифуркации торов Лиувилля. На каждом ребре графа W можно указать стрелкой ориентацию этого ребра, см. подробности [4, 13].

Приведём примеры часто встречающихся двумерных атомов. Атом A гомеоморфен диску – он расслоен на концентрические окружности, стягивающиеся на особый слой – центральную точку. Атом B представляет собой перестройку одной окружности в две, особым слоем является "восьмерка". Атом C_2 представляет собой перестройку двух окружностей в две. Эти атомы представлены на рис. 1.

Рассмотрим топологически устойчивую интегрируемую систему с боттовским интегралом f (см. [4, 13]) на Q^3 и пусть L – связный особый слой

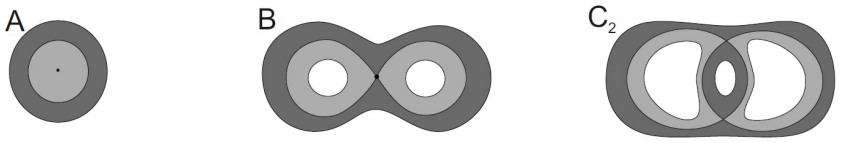


Рис. 1: Двумерные атомы A, B и C_2.

слоения Лиувилля на Q. Пусть $U(L)$ – связная инвариантная трехмерная окрестность этого слоя. Тогда $U(L)$ – 3-многообразие со структурой слоения Лиувилля, называемое 3-атомом. Точнее, два таких многообразия будем считать лиувиллево эквивалентными, если во-первых, между ними существует послойный диффеоморфизм, а во-вторых, этот диффеоморфизм сохраняет ориентацию 3-многообразий и ориентацию на критических окружностях, задаваемых гамильтоновым потоком.

Такой класс эквивалентности многообразия $U(L)$ называется 3-атомом.

Теорема 1 (А. Т. Фоменко [4, 13]). *1. Многообразие $U(L)$, т.е. 3-атом, несёт на себе структуру расслоения Зейферта, где особые слои имеют тип (2,1).*

2. База расслоения Зейферта на 3-атоме $U(L)$ имеет естественную структуру 2-атома.

3. Проекция $\pi : (U(L), L) \to (P^2, K)$ устанавливает взаимно-однозначное соответствие между 3-атомами и 2-атомами.

4. Особые слои типа $(2, 1)$ в $U(L)$ соответствуют "звездочкам" на 2-атоме (P^2, K).

Трехмерный атом без звездочек послойно гомеоморфен прямому произведению соответствующего двумерного атома на окружность. Простейший 3-атом со звездочкой, а именно атом A^*, получается из двумерного атома B косым умножением на окружность: необходимо "прокрутить" атом B на π. В результате, атому A^* будет соответствовать перестройка одного тора в один.

Для описания топологии слоения необходимо выбрать пары так называемых допустимых базисов на граничных торах и указать матрицы перехода от одного базиса к другому. Структура атома-бифуркации задаёт правило выбора допустимого базиса. Подробное изложение см. в работах [4, 12, 13, 14]. Таким образом в точке каждого ребра грубой молекулы W,

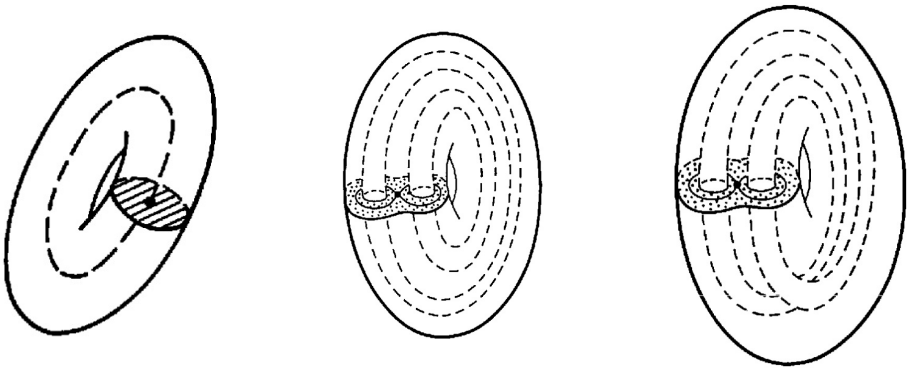


Рис. 2: Трехмерные атомы A, B, A^*

представляющей собой тор Лиувилля, определены два допустимых базиса. Для каждой такой пары базисов можно указать матрицу перехода от одного базиса к другому, которая называется матрицей склейки. Так как в допустимом базисе однозначно выбирается лишь один цикл (дополнительный цикл выбирается неоднозначно), то полученная матрица склейки может меняться при замене одних допустимых базисов на другие. Однако, по матрице склейки можно определить ряд чисел-меток, которые для всех таких матриц будут совпадать (см. [4, 12, 13, 14]). Эти числовые метки – r, ε и n – инвариантны относительно допустимых замен базисов на граничных торах (см. леммы 4.5 и 4.6 книги [4]).

Определение 0.2. Молекула W, снабжённая числовыми метками r, ε и n_k, называется меченой молекулой W^* или инвариантом Фоменко-Цишанга.

Теорема 2 (А. Т. Фоменко, Х. Цишанг [4])**.** *Две невырожденные топологически устойчивые интегрируемые гамильтоновы системы на регулярных изоэнергетических поверхностях* $Q_1^3 = \{x \in M_1^4 : f_1(x) = c_1\}$ *и* $Q_2^3 = \{x \in M_2^4 : f_2(x) = c_2\}$ *лиувиллево эквивалентны тогда и только тогда, когда их меченые молекулы совпадают.*

Топологические интегрируемые биллиарды.

Пусть область Ω на плоскости $\mathbb{R}^2$ такова, что граница области является кусочно-гладкой кривой, причем в точках излома этой кривой углы равны $\frac{\pi}{2}$. Рассмотрим динамическую систему, описывающую движение (материальной) точки внутри Ω с естественным отражением на границе

$P = \partial\Omega$. Эту систему назовём "биллиардом в области". Будем считать, что в точках, где граница P не гладкая (тогда, как было сказано, угол излома обязательно равен $\frac{\pi}{2}$) траектории системы можно доопределить по непрерывности: а именно, попав в вершину угла границы, материальная точка, не теряя скорости, отразится назад по той же траектории. Таким образом, фазовым пространством системы является многообразие

$$M^4 := \{(x, v) | \quad x \in \Omega, v \in T_x\mathbb{R}^2 \ , |v| > 0\}/\sim$$

где отношение эквивалентности задаётся так

$$(x_1, v_1) \sim (x_2, v_2) \Leftrightarrow x_1 = x_2 \in P, \quad |v_1| = |v_2| \quad \text{и} \quad v_1 - v_2 \perp T_{x_1}P.$$

Здесь через T_xP обозначена касательная плоскость к области Ω в точке x, а через $|v|$ – евклидова длина вектора v.

Система биллиарда в общем случае не является гладкой, так как склейка в точках границы, как правило, не позволяет ввести гладкую структуру в декартовых координатах. Необходимо видоизменить определения выше с учетом граничных точек. Используемый нами подход и определения предложены А. Т. Фоменко; см. также работы В.Лазуткина [17] и Е. А. Кудрявцевой [15].

Для класса биллиардов, ограниченных дугами софокусных эллипсов и гипербол кусочно-гладкая теорема Лиувилля доказана в работе В.В.Фокичевой [10]. В настоящей работе мы пользуемся этими результатами.

Пусть плоская область Ω ограничена сегментами софокусных квадрик.

Теорема 3 (Якоби, Шаль [3])**.** *Касательные прямые к геодезической линии на квадрике в n-мерном евклидовом пространстве, проведенные во всех точках геодезической, касаются кроме этой квадрики еще $n-2$ конфокальных с ней квадрик, одних и тех же для всех точек данной геодезической.*

В плоском двумерном случае из теоремы Якоби-Шаля следует, что касательные в любой точке биллиардной траектории внутри области Ω касаются эллипса или гиперболы, софокусных с семейством квадрик, образующих границу P области Ω.

Относительно стандартной симплектической структуры на плоскости, функции $|v|$ — модуль вектора скорости – и Λ — параметр софокусной квадрики коммутируют. Так как они сохраняются вдоль траекторий

биллиарда, значит в пределе они коммутируют и на границе области. Таким образом, данная "биллиардная" система обладает двумя независимыми (см. [3]) интегралами:

1. $|v|$ — модуль вектора скорости,

2. Λ — параметр софокусной квадрики.

В данной работе под софокусными квадриками мы понимаем семейство софокусных эллипсов и гипербол. Биллиард в области, ограниченной дугами софокусных парабол, также интегрируем. Слоения Лиувилля таких биллиардов с точностью до лиувиллевой эквивалентности классифицированы в работе [9].

Фиксируем декартовы координаты (x, y) на плоскости $\mathbb{R}^2$. Рассмотрим семейство софокусных квадрик – кривых, задаваемых соотношением

$$x^2(b-\lambda) + y^2(a-\lambda) = (a-\lambda)(b-\lambda), \tag{0.1}$$

где $a > b > 0$ – фиксированные параметры семейства, а λ – параметр квадрики. При $\lambda < b$ ($b < \lambda < a$) соотношение задает семейство софокусных эллипсов (соответственно гипербол). При $\lambda = b$ соотношение задаёт прямую Ox, которую можно рассмотреть как объединение двух вырожденных гипербол – лучей из фокусов семейства и вырожденного эллипса – отрезка между фокусами. При $\lambda = a$ соотношение задаёт прямую Oy, которую можно рассмотреть как предельную гиперболу. В дальнейших рассуждениях прямую Oy мы будем считать гиперболой.

В качестве примера рассмотрим биллиард в эллипсе с параметром $\lambda = 0$. Покажем, как ведут себя траектории на разных уровнях интеграла Λ (подробнее, см. [3]). Пусть $\Lambda = 0$. Этому значению интеграла соответствуют две траектории, соответствующие движениям по границе эллипса и закручивающиеся в разные стороны. При $\Lambda \in (0, b)$ траектории касаются эллипса с параметром Λ – они также разбиваются на два класса – закручивающиеся по и против часовой стрелки. Значению интеграла $\Lambda = b$ соответствует особый слой 3-атома B (см. [7]): на нём лежат траектории, последовательно проходящие через фокусы семейства 0.1. Критической окружностью является траектория, проходящая вдоль большей оси эллипса. При $\Lambda \in (b, a)$ касательные к траектории касаются гиперболы с параметром Λ. Значению параметра $\Lambda = a$ отвечает вертикальная траектория вдоль меньшей оси эллипса.

В дальнейшем вместо слов "область" или "биллиардная область" мы будем писать "биллиард".

Определение 0.3. *Простейшим элементарным компактным (плоским) биллиардом* назовём плоское, компактное, изометрично вложимое в плоскость многообразие с краем, граница которого при этом вложении ограничена дугами софокусных эллипсов и гипербол и не содержит углов, превышающих π. *Составным элементарным компактным (локально-плоским) биллиардом* назовем компактное локально-плоское многообразие, которое получается в результате нескольких склеек из конечного числа простейших элементарных биллиардов вдоль некоторых граничных дуг гипербол таким образом что, во-первых, склеиваемые биллиарды при их вложениях в плоскость локально находятся по разные стороны от дуги склейки (в случае если дуга является прямолинейным отрезком мы опускаем это требование), во-вторых, при этом на границе области не образуются углы, превышающие π, в третьих, граничные дуги склеиваются при помощи изометрий. При этом мы не требуем, чтобы существовало изометричное вложение в плоскость составного элементарного биллиарда целиком. Простейшие и составные элементарные биллиарды для краткости мы будет называть просто *элементарными*.

Определение 0.4. Элементарный биллиард (Ω, U_i), ограниченный дугами квадрик из софокусного семейства (0.1), называется **эквивалентным** другому элементарному биллиарду (Ω', U_i'), ограниченному дугами квадрик из того же семейства (0.1), если (Ω', U_i') можно получить из (Ω, U_i) путем композиции следующих преобразований.

- Последовательным изменением сегментов границы в образах некоторых простейших элементарных биллиардов U_i при их изометричных вложениях в плоскость путем непрерывной деформации в классе квадрик (0.1), так, чтобы значение параметра λ изменяемого сегмента границы не принимало значения значения b. При этом потребуем, чтобы одновременно менялись и оставались равными друг другу значения параметра λ для квадрик (гипербол), содержащих образы общей граничной дуги любых двух пересекающихся простейших элементарных биллиардов при их изометричных вложениях в плоскость, согласованных на этой дуге до деформации (а потому также во время и после деформации), а также одновременно меняются и остаются равными друг другу значения параметра λ для квадрик (эллипсов), содержащих образы эллиптических граничных сегментов (разных элементарных биллиардов), имеющих общую вершину.

- Симметрией относительно оси семейства (0.1) во всех простейших

элементарных биллиардах U_i одновременно;

- объединением нескольких простейших элементарных биллиардов в один или же путем разбиения одного элементарного биллиарда на более мелкие.

Мы будем различать граничные сегменты четырёх типов: эллипс, дуга невырожденной гиперболы, заключённая между двумя эллипсами, дуга невырожденного эллипса, заключённая между двумя гиперболами, отрезок фокальной прямой.

Пусть дан набор компактных биллиардов Ω_i, ограниченных дугами одного и того же софокусного семейства квадрик. Введём понятие обобщенного биллиарда. Обобщенный биллиард Δ состоит из нескольких элементарных биллиардов Ω_i, склеенных по общим выпуклым эллиптическим сегментам границы (и, возможно, по некоторым гиперболическим, с образованием так называемых конических точек) при этом мы запрещаем все склейки, приводящие либо к углам больше чем π на границе полученного обобщенного биллиарда, либо к углам больше чем 2π во внутренних точках этого биллиарда.

Траектория обобщенного биллиарда "перескакивает" с одного элементарного биллиарда на другой в точках пересечения с рёбрами склейки и отражается по стандартному закону отражения при ударе о границу биллиарда Δ (см. рис. 3).

Оговорим отдельно случай конической точки, в которой склеиваются два угла различных элементарных биллиардов Ω, входящих в состав биллиарда Δ. В этом случае, как легко понять из соображений непрерывности, закон отражения будет выглядеть так – материальная точка, проходя по элементарному биллиарду Ω, попав в коническую точку, отразится по той же прямой и будет продолжать движение на тому же элементарному биллиарду Ω (см. рис. 3). То есть, "перескакивание" материальной точки в конце ребра склейки возможно, только если локально в этой вершине излома определена склейка четырех элементарных биллиардов.

При таком определении фазового многообразия M^4 сохраняется интегрируемость системы.

Определение 0.5. Обобщённый биллиард Δ, склеенный из элементарных биллиардов Ω_i вдоль ребер склейки f_{ij} называется *эквивалентным* другому обобщённому биллиарду Δ', склеенному из Ω'_i вдоль ребер склейки f'_{ij}, если Δ' можно получить из Δ путем замены элементарных биллиардов Ω_i на им эквивалентные.

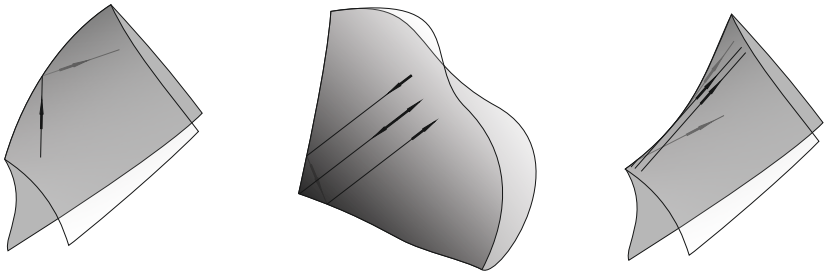


Рис. 3: Слева показано движение в обобщенном биллиарде на выпуклой границе склейки двух элементарных биллиардов, на рисунке по центру показано, как именно движение в конической точке доопределяется по непрерывности. На рисунке справа видно, что если граница склейки является невыпуклой, то для траекторий, касательных к границе склейки при ударе нельзя определить непрерывное продолжение – после удара о невыпуклую границу они могут как остаться на том же, так и перейти не другой лист, как пределы двух типов траекторий.

Моделирование некоторых систем математической физики с помощью биллиардов.

Вычисление инвариантов Фоменко-Цишанга элементарных и обобщенных биллиардов позволило обнаружить их совпадение в большом числе случаев с инвариантами, вычисленными ранее в случаях интегрируемости в динамике твердого тела (Эйлера, Лагранжа, Ковалевской, Жуковского, Горячева-Чаплыгина-Сретенского, Ковалевской-Яхьи, Клебша и Соколова). Это позволило доказать лиувиллеву эквивалентность случаев интегрируемости в динамике твердого тела элементарным и обобщенным биллиардам. В работах [10, 11] приведён список в то время обнаруженных лиувиллево эквивалентных слоений и указаны области на бифуркационных диаграммах случаев Эйлера, Лагранжа, Ковалевской, Жуковского, Горячева-Чаплыгина-Сретенского, соответствующие этим изоэнергетическим 3-поверхностям. Для каждого инварианта указан биллиард моделирующий поведение решений на данных изоэнергетических поверхностях.

В настоящее время школой А.Т.Фоменко вычислены новые инварианты лиувиллевой эквивалентности. В частности, С.С.Николаенко в работе [28] полностью классифицировал изоэнергетические 3-многообразия системы Чаплыгина в динамике твердого тела в жидкости, а в работе [29]

им были вычислены инварианты Фоменко-Цишанга для интегрируемых систем типа Горячева. В статье [30] Г.М.Сечкин изучил топологию динамики эллипсоида вращения, движущегося по гладкой горизонтальной плоскости под действием силы тяжести, также дав ответ в терминах молекул Фоменко-Цишанга.

Теорема 4 ([11]). *Следующие случаи динамики твердого тела моделируются (лиувиллево эквивалентны) следующим обобщенным биллиардам:*

- *случай Эйлера, см. [4], полностью моделируется обобщенными биллиардами, указанными на рисунках 4а,з,и, соответствующих зонам I, II, III энергии H, соответственно;*
- *случай Лагранжа, см. [4, 24], моделируется обобщенными биллиардами, указанными на рисунке 4в – зона энергии 5;*
- *случай Ковалевской, см. [4], моделируется обобщенными биллиардами, указанными на рисунке 4в – зона энергии 5;*
- *случай Горячева-Чаплыгина-Сретенского, см. [4, 23, 24] моделируется обобщенными биллиардами, указанными на рисунках 4в– зона энергии 4, изоэнергетическая поверхность $Q^3 \simeq S^1 \times S^2$,*

  4 ж – зона энергии 2, изоэнергетическая поверхность $Q^3 \simeq S^3$;
- *случай Жуковского, см. [4, 19, 20] моделируется обобщенными биллиардами, указанными на рисунках 4б – зона энергии 11, изоэнергетическая поверхность $Q^3 \simeq RP^3$, 4в – зона энергии 2, изоэнергетическая поверхность $Q^3 \simeq S^1 \times S^2$, 4г – зона энергии 8, изоэнергетическая поверхность $Q^3 \simeq S^3$, 4е – зона энергии 12, изоэнергетическая поверхность $Q^3 \simeq RP^3$;*
- *случай Ковалевской-Яхьи, см. [27], моделируется обобщенными биллиардами, указанными на рисунках 4в – зона энергии h_{16}, изоэнергетическая поверхность $Q^3 \simeq S^1 \times S^2$, 4д – зона энергии h_{18}, изоэнергетическая поверхность $Q^3 \simeq S^3$;*
- *случай Клебша, см. [25], моделируется обобщенными биллиардами, указанными на рисунках 4д – зона энергии 2, изоэнергетическая поверхность $Q^3 \simeq S^3$, 4з – зоны энергии 10,12, изоэнергетическая поверхность $Q^3 \simeq S^1 \times S^2$, 4и – зона энергии 5, изоэнергетическая поверхность $Q^3 \simeq RP^3$;*

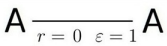
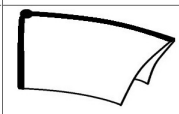
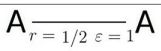
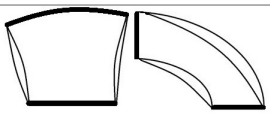
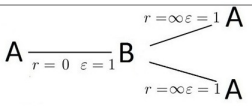
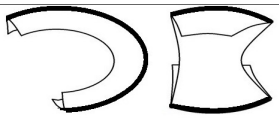
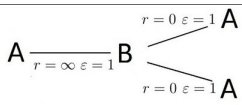
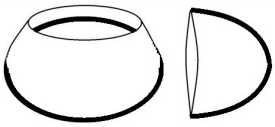
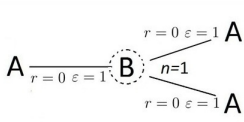
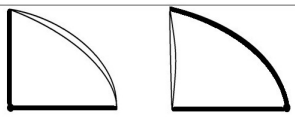
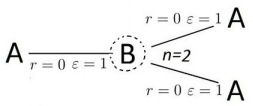
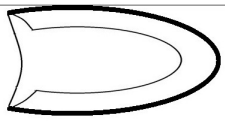
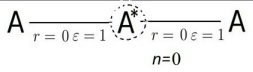
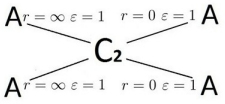
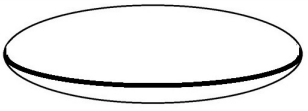
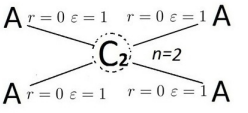
	Обобщенный биллиард	Инвариант Фоменко-Цишанга, описывающий обобщенный биллиард	Эквивалентные известные случаи интегрируемости для твердого тела
а			Лагранж, Эйлер, Горячев, Чаплыгин, эллипсоид вращения на гладкой плоскости
б			Лагранж, Жуковский, эллипсоид вращения на гладкой плоскости
в			Ковалевская, Горячев-Чаплыгин-Сретенский, Жуковский, Ковалевская-Яхья
г			Жуковский, Горячев
д			Клебш, Соколов, Ковалевская-Яхья, Горячев
е			Жуковский, эллипсоид вращения на гладкой плоскости
ж			Горячев-Чаплыгин-Сретенский
з			Эйлер, Клебш, Чаплыгин
и			Эйлер, Клебш, Соколов, Чаплыгин

Рис. 4:

- *случай Соколова, см. [26], моделируется обобщенными биллиардами, указанными на рисунках 4д –зона энергии B, изоэнергетическая поверхность $Q^3 \simeq S^3$, 4и –зона энергии I, изоэнергетическая поверхность $Q^3 \simeq RP^3$.*

- *случай Чаплыгина в динамике твердого тела в жидкости, см. [28], моделируется обобщенными биллиардами, указанными на рисунках 4а,з,и, отвечающих зонам энергии (1), (2) и (3) соответственно;*

- *случай Горячева, см. [28], моделируется обобщенными биллиардами, указанными на рисунке 4а, – зоны энергии (1) и (3), 4г – зона энергии (2), 4д – зона энергии (4);*

- *случай динамики эллипсоида вращения, движущегося по гладкой горизонтальной плоскости под действием силы тяжести, см. [30], моделируется обобщенными биллиардами, указанными на рисунке 4а,б, е.*

Наглядный пример: известный случай Эйлера моделируется простым биллиардом.

В случае Эйлера топология слоения изоэнергетической поверхности Q^3 при нулевой постоянной площадей позволяет наглядно продемонстрировать поведение периодических решений. Напомним следующий известный эксперимент. Рассмотрим обычную книгу (вместо книги можно взять деревянный брусок в форме книги). Ориентируем её в горизонтальной плоскости, как показано на рис. 5 и подбросим вверх, закрутив книгу вокруг ее горизонтальной оси симметрии, проходящей через центр книги. Затем поймаем книгу и посмотрим, в каком положении она вернулась к нам. Оказывается, результат существенно зависит от того, как мы ориентировали книгу перед началом броска. У книги есть три взаимно перпендикулярных оси симметрии. Если подбросить книгу, закрутив ее вокруг оси, отвечающей наименьшему моменту инерции, то книга вернется назад в том же положении, какое она занимала до броска. Если книга подброшена и закручена вокруг оси, отвечающей максимальному моменту инерции, то эффект будет тот же. Совсем другая картина возникнет, когда мы подбросим книгу, закрутив ее вокруг оси, отвечающей среднему моменту инерции. Если в начале корешок книги был в левой руке, то поймав книгу в воздухе, вы обнаружите, что корешок оказался в вашей правой руке.

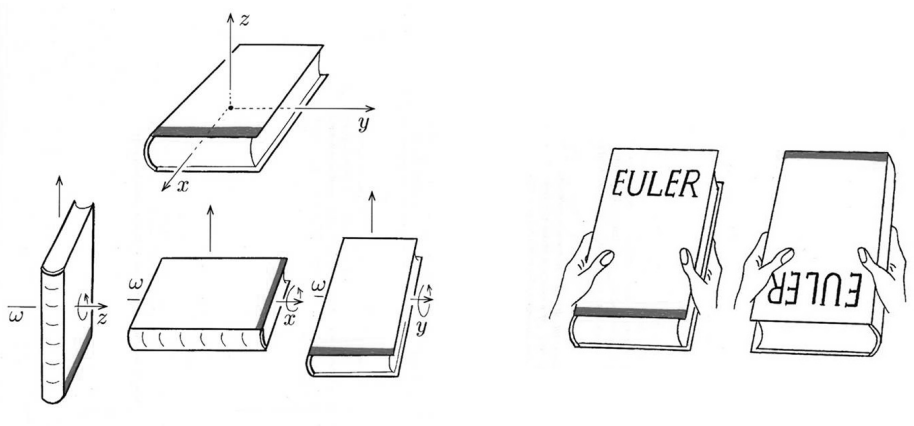


Рис. 5: Эксперимент с книгой.

Это любопытное обстоятельство объясняется так. Полет книги хорошо моделирует случай Эйлера в динамике тяжелого твердого тела. Достаточно забыть о движении центра масс книги, т. е. рассматривать только ее "чистое вращение" вокруг центра масс. Кроме того, можно считать, что постоянная площадей здесь равняется нулю. Дело в том, что при каждом из бросков мы закручиваем книгу вокруг горизонтальной оси, идущей по одному из собственных направлений тензора инерции. Следовательно, вектор кинетического момента пропорционален вектору угловой скорости. Сила тяжести направлена вертикально вниз, то есть ортогональна кинетическому моменту книги. Поскольку постоянная площадей получается как скалярное произведение кинетического момента на вектор силы тяжести, следовательно, в данном эксперименте эта постоянная равна нулю. Поэтому мы попадаем в ситуацию случая Эйлера с нулевой постоянной площадей. Полет книги можно интерпретировать как движение по интегральной траектории динамической системы случая Эйлера на изоэнергетической трехмерной поверхности. Качественный характер движения определяется топологией слоения Лиувилля. Три движения книги в пространстве отвечают трем типам интегральных траекторий.

Первый тип – это устойчивые периодические траектории двух "верхних атомов" A на молекуле. Механически — это вращение книги вокруг минимальной оси ее эллипсоида инерции. Движение устойчиво, и книга возвращается в прежнее положение.

Второй тип — это устойчивые периодические траектории двух "нижних атомов" A на молекуле. Это – вращение книги вокруг максимальной оси эллипсоида инерции. Такое движение также устойчиво, что мы и видим.

Третий тип определяется двумя гиперболическими периодическими траекториями, отвечающими седловому атому C_2. Это — две траектории, проходящие через его вершины. Полет книги в данном случае задается интегральной траекторией, начинающейся вблизи первого седлового периодического решения. Теоретически можно было бы закрутить книгу так, чтобы соответствующая точка все время двигалась бы по седловой периодической траектории. Но на практике этого сделать нельзя. Неизбежно присутствующее малое возмущение заставит книгу двигаться по интегральной траектории, которая лишь сначала близка к седловому периодическому решению. Но затем траектория быстро удаляется от него и через некоторое время начинает приближаться ко второму седловому периодическому решению. Интегральная траектория в действительности движется по плоскому кольцу (на особом слое 3-атома C_2), "сматываясь" с его наружной границы и "наматываясь" на внутреннюю границу кольца. Таким образом, в тот момент, когда вы ловите книгу, интегральная траектория уже почти достигла второго периодического решения. А это и есть в точности эффект "переворачивания корешка книги". Закрутив книгу вокруг ее средней оси инерции, вы заставляете интегральную траекторию двигаться от одной седловой вершины атома C_2 к другой его седловой вершине.

Эту картину можно наглядно смоделировать на обобщенном биллиарде, склеенном из двух областей, ограниченных эллипсами. Рассмотрим малую окрестность $B_\varepsilon(x_0)$ точки x_0, лежащей на фиксированной критической траектории 3-атома C_2, описывающего бифуркацию линий уровня функции Λ в изоэнергетической поверхности такого обобщенного биллиарда.

Пусть точка $x \in B_\varepsilon(x_0)$ также лежит на особом слое, но уже не принадлежит критической траектории. В этом случае, она лежит на одном из четырех колец – траектории на двух из них бесконечно приближаются к фиксированной критической окружности, а на двух других – "разматываются" с неё, бесконечно приближаясь к другой критической окружности. Это поведение траекторий изображено на верхних рисунках 6 ниже.

Пусть точка $x \in B_\varepsilon(x_0)$ не лежит на особом слое. В этом случае она лежит на эллиптическом или гиперболическом торе, в зависимости от

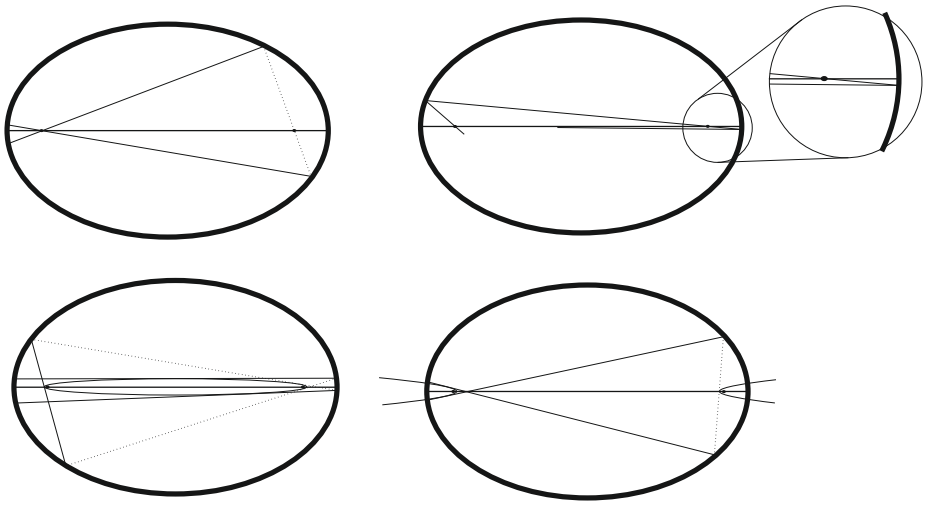


Рис. 6: На верхних рисунках изображены траектории, лежащие на особом слое атома C_2, описывающего бифуркацию линий уровня функции Λ в изоэнергетической поверхности обобщенного биллиарда, склеенного из двух областей, ограниченных эллипсами. На нижних – траектории, лежащие на эллиптическом (слева) и гиперболическом (справа) торах. Траектория выделена сплошной линией при прохождении по вехнему экземпляру биллиарда, ограниченного эллипсом и пунктиром – по нижнему. Жирными точками выделены фокусы.

того квадрики какого типа касаются её касательные. В обоих случаях (см. нижние рисунки 6 ниже) видно, что траектория, проходящая через точку x, через короткое время будет приближаться к другой критической окружности.

Заметим, что в случае с книгой мы не могли попасть из-за неточности начальных данных строго на особый слой, что приводило к тому что корешок книги при вращении вокруг средней оси переворачивался. Так и траектория обобщенного биллиарда, будучи изначально близка к одной критической окружности, через короткое время будет “закручиваться” в другую сторону.

Геометрия пространства замкнутых ограниченных подмножеств метрического пространства

Напомним, что *метрическим пространством* называется множество X, на парах элементов $x, y \in X$ которого, называемых точками, задана так называемая *метрика* $|xy|$, моделирующая расстояние между ними. Метрика должна обладать следующими свойствами: это неотрицательная функция на $X \times X$ симметричная, невырожденная, т.е. $|xy| = 0$, если и только если $x = y$, и удовлетворяющая неравенству треугольника $|xz| \leq |xy| + |yz|$.

Сравнение подмножеств фиксированного метрического пространства (например, евклидова пространства $\mathbb{R}^n$) — важная задача как с математической, так и с практической точки зрения. Один из возможных способов такого сравнения — ввести расстояние между подмножествами, которое, говоря неформально, будет численно характеризовать насколько «далеки друг от друга» рассматриваемые подмножества. Исследованиям пространств компактов посвящено много работ, начиная от классических работ Хаусдорфа [32] и Громова [33], и заканчивая недавними работами Иванова, Тужилина и их учеников [34], [35] и [38].

Есть много естественных способов задать «расстояние» между подмножествами $A, B \subset X$ метрического пространства X. Например $|AB| = \inf\big\{|ab| : a \in A, b \in B\big\}$. Однако, полученная функция не будет метрикой (в данном случае нарушается невырожденность и неравенство треугольника).

Метрика Хаусдорфа

В 1914 году Феликс Хаусдорф [32] предложил следующую конструкцию.

Пусть $B_r(A) = \{x \in X : |xA| \leq r\}$, где $r > 0$, $A \subset X$ и $|xA| = \inf\{|xa| : a \in A\}$ для $x \in X$. Для непустых $A, B \subset X$ положим

$$d_H(A, B) = \inf\big\{r : A \subset B_r(B) \ \&\ B_r(A) \supset B\big\}.$$

d_H называется *расстоянием по Хаусдорфу*. Хаусдорф показал, что функция d_H является метрикой на множестве $\mathcal{H}(X)$ всех замкнутых ограниченных подмножеств метрического пространства X.

Например, пусть X — плоскость с обычным евклидовым расстоянием, A — круг с центром $(0, 0)$ и радиусом 0.3, B — круг с центром $(2, 0)$ и радиусом 1, см. рис. 7. Легко проверить, что в данном случае $d_H(A, B) = 3$.

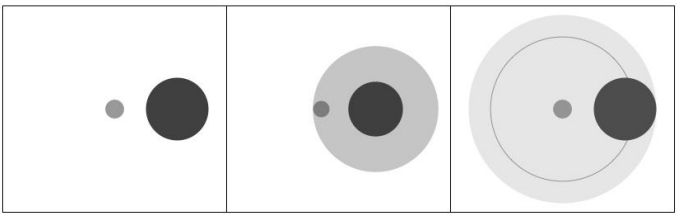


Рис. 7: Слева: $A, B \subset \mathbb{R}^2$; в центре: $B \subset B_r(A)$, $r = 2.3$, справа: $B_r(A) \supset B$, $r = 3$, а для $r = 2.3$ — включения нет.

Пространства $\mathcal{H}(X)$ довольно хорошо изучены. Например, хорошо известно, что следующие свойства одновременно или имеют или не имеют место у пространств X и $\mathcal{H}(X)$: полнота, полная ограниченность (т.е. наличие конечных ε-сетей), компактность. Для дальнейшего нам понадобится еще одно свойство.

Напомним, что метрика пространства X называется *внутренней*, если $|xy| = \inf\{|\gamma| : \gamma$ — непрерывная кривая, соединяющая x и $y\}$, где через $|\gamma|$ обозначена длина кривой γ в метрическом пространстве X, и *строго внутренней*, если каждая пара точек x, y соединяется некоторой *кратчайшей кривой* γ, т.е. такой, что $|\gamma| = |xy|$.

Предложение 0.1. *Если X — ограниченно компактное пространство со строго внутренней метрикой, то $\mathcal{H}(X)$ — также ограниченно компактное, и метрика Хаусдорфа — строго внутренняя.*

Явная конструкция кратчайших в $\mathcal{H}(X)$

Пусть W — произвольное метрическое пространство, $a, b \in W$, $|ab| = r$, $s \in [0, r]$. Будем говорить, что $c \in W$ *находится в s-положении между a и b*, если $|ac| = s$ и $|cb| = r - s$.

Предложение 0.2. *Пусть X — произвольное метрическое пространство и $A, B \in \mathcal{H}(X)$, $r = d_H(A, B)$, $s \in [0, r]$. Тогда если множество $C \in \mathcal{H}(X)$ находится в s-положении между A и B, то $C \subset B_s(A) \cap B_{r-s}(B)$.*

Множество $B_s(A) \cap B_{r-s}(B)$ будем обозначать через $C_s(A, B)$ или, если понятно, о каких A и B идет речь, то просто через C_s.

Рассмотрим тот же пример, см. рис. 8: пусть снова $A \in \mathcal{H}(\mathbb{R}^2)$ — круг с центром $(0, 0)$ и радиусом 0.3, $B \in \mathcal{H}(\mathbb{R}^2)$ — круг с центром $(2, 0)$ и радиусом 1. Расстояние $d_H(A, B) = 3$.

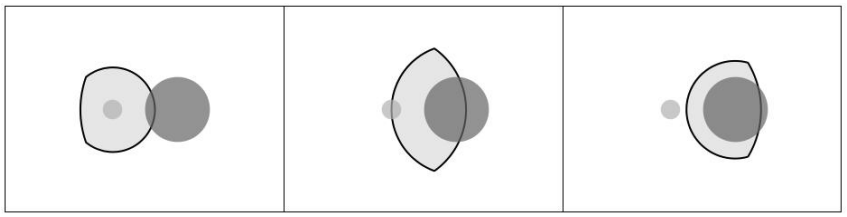


Рис. 8: Множество $C_s(A, B)$ для $s = 1$, $s = 2$, $s = 2.5$ (слева направо).

В качестве следующего примера рассмотрим одноточечные компактные подмножества произвольного метрического пространства.

Предложение 0.3. *Пусть X — произвольное метрическое пространство и $A = \{a\}$, $B = \{b\}$, $r = |ab|$, $s \in [0, r]$. Тогда*

1. *C_s представляет собой множество всех точек из X, находящихся между a и b в s-положении;*

2. *C_s находится в s-положении между A и B, если и только если $C_s \neq \emptyset$;*

3. *множество $C \subset X$ находится в s-положении между A и B, если и только C — непустое замкнутое подмножество C_s.*

Например, если $X = \mathbb{R}^n$, то C_s — точка отрезка $[a, b]$, отстоящая от a на расстояние s. Если же X — плоскость с нормой $\|(x, y)\| = |x| + |y|$, $A = \{(0, 0)\}$, $B = \{(3, 2)\}$, см. рис 9. Тогда $d_H(A, B) = 5$. В этом случае в s-положении находится бесконечно много подмножеств. Каждое из них порождает кратчайшую, соединяющую A и B, см. рис. 10.

Следующие результаты были известны только для случая $X = \mathbb{R}^n$. Оказалось, что доказательства практически дословно проходят в более общем случае.

Теорема 5 (Иванов, Тужилин, 2016)**.** *Пусть X — полное локально компактное пространство с внутренней метрикой. Тогда для любых A, $B \in \mathcal{H}(X)$, $r = d_H(A, B)$, $s \in [0, r]$, множество $C_s = C_s(A, B)$ принадлежит $\mathcal{H}(X)$ и находится в s-положении между A и B.*

Теорема 6 (Иванов, Тужилин, 2016)**.** *Пусть X — полное локально компактное пространство с внутренней метрикой, $A, B \in \mathcal{H}(X)$, и $r =$*

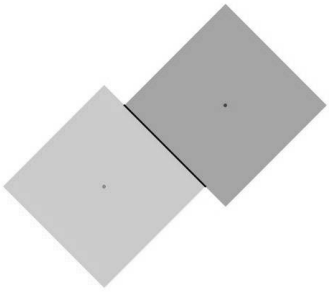


Рис. 9: Множество $C_s(A, B)$ при $s = 2.5$, любое замкнутое непустое подмножество $C \subset C_s(A, B)$ находится в s-положении.

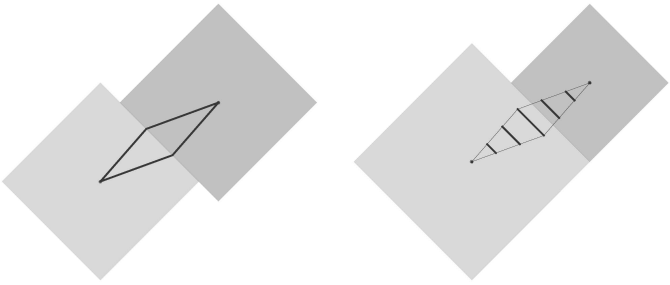


Рис. 10: Точки A и B соединяет бесконечно много кратчайших. Слева — две из них, состоящие из одноточечных подмножеств; справа одна, состоящая из параллельных отрезков.

$d_H(A, B)$. *Тогда* $\gamma(s) = C_s(A, B)$, $s \in [a, b]$, *является кратчайшей кривой, соединяющей* A *и* B, *причем длина кривой* γ *равна* $d_H(A, B)$, *а параметр* s — *натуральный.*

Сколько может быть кратчайших кривых?

Легко построить примеры подмножеств, которые соединяет единственная кратчайшая, а также бесконечное семейство кратчайших. Из теоремы 6 вытекает, что если X — полное локально компактное пространство с внутренней метрикой, то каждому $C \in \mathcal{H}(X)$, находящемуся в s-положении между A и B, соответствует кратчайшая, соединяющая A и B. Поэтому, если число кратчайших конечно, то в s-положении может

быть лишь конечное число множеств (для каждого значения s).

Следствие 1. *Пусть $A, B \in \mathcal{H}(X)$, $r = d_H(A, B) > 0$. Предположим, что существуют $a \in A$ и $b \in B$, для которых $|ab| < r$. Тогда при каждом $0 < s < r$ имеется бесконечно много $C \in \mathcal{H}(X)$, которые находятся в s-положении между A и B, и, значит, бесконечно много кратчайших.*

Следствие 2. *Предположим, что для $A \neq B \in \mathcal{H}(X)$, $r = d_H(A, B)$ и некоторого $s \in (0, r)$ имеется лишь конечное число элементов $C \in \mathcal{H}(X)$, находящихся в s-положении между A и B. Тогда для любых $a \in A$ и $b \in B$ имеем $|ab| \geq r$ и $|aB| = |Ab| = r$.*

Пусть X — произвольное метрическое пространство. Пару $\{A, B\}$ различных множеств из $\mathcal{H}(X)$, $r = d_H(A, B)$, назовем *конфигурацией*, если для любых $a \in A$ и $b \in B$ имеем $|ab| \geq r$ (или, что равносильно, $|aB| = |Ab| = r$). Конфигурацию назовем *конечной*, если для каждого s имеется лишь конечное число элементов в s-положении.

В качестве примера рассмотрим множества $A, B \subset \mathbb{R}^2$ — вершины правильного шестиугольника, взятые через одну. Для каждого s множество $C_s(A, B)$ состоит из 6 точек, см. рис. 11.

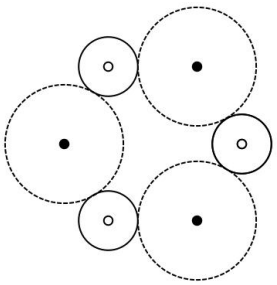


Рис. 11: Множество $C_s(A, B)$ для $s = 1/3$ состоит их 6 точек пересечения пар разноцветных окружностей.

Пусть X — ограниченно компактное пространство со строго внутренней метрикой. Пусть также любые две точки соединяются единственной, с точностью до параметризации, кратчайшей кривой, и кратчайшие кривые, содержащие общий невырожденный фрагмент, лежат в одной и той же кратчайшей кривой.

Теорема 7. *Пусть $\{A, B\}$ — произвольная конечная конфигурация и $r = d_H(A, B) > 0$. Тогда количество множеств $C \in \mathcal{H}(X)$ в s-положении*

не зависит от $s \in (0, r)$ *и равно количеству кратчайших, соединяющих* A *и* B.

Пусть $\{A, B\}$ —конечная конфигурация. Построим двудольный граф, ребра которого — суть пары $\{a, b\}$, $a \in A$, $b \in B$, для которых $d_H(A, B) = |ab|$. Элементы множество $C_s(A, B)$ находятся во взаимно однозначном соответствии с ребрами этого графа. Подмножество $C \subset C_s(A, B)$ находится в s-положении, если и только если соотвествующие ребра образуют покрытие множества вершин графа. На рис. 12 приведен двудольный граф для множеств A и B из предыдущего примера.

Несложно показать, что для каждого двудольного графа существуют множества A, $B \subset \mathbb{R}^n$ (для некоторого n), образующие конечную конфигурацию с таким двудольным графом. Таким образом, задача сводится к изучению возможного числа реберных покрытий двудольных графов.

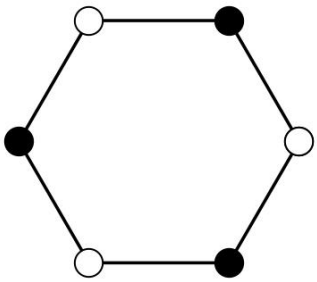


Рис. 12: Двудольный граф, соотвествующий $C_s(A, B)$. Для данного двудольного графа существует 18 реберных покрытий.

Назовем натуральное число n *хорошим*, если существует двудольный граф, у которого ровно n реберных покрытий. Blackburn, Lund, Schlicker, Sigmon, Zupan [36] открыли удивительный факт: среди чисел от 1 до 36 все числа хорошие, за исключением 19. В 2013 году K. Honigs [37] и З. Овсянников независимо выяснили, что 37 — тоже нехорошее число.

Как продолжить последовательность 19, 37?

З. Овсянников [38] предложил следующий метод, основанный на разложении двудольных графов на так называемые *атомарные*.

Семейство подграфов $G_1, \ldots, G_k$ назовем *разложением* графа G, если $G = \cup_i G_i$, любая пара графов G_i, G_j не имеет общих ребер, имеют не

более одной общей вершины, и граф этого разбиения (т.е. граф, вершины которого — подграфы G_i, и две вершины смежны если и только если соответсвующие G_i пересекаются) — дерево.

Граф называется *атомарным*, если его нельзя разложить на два или более подграфа. З. Овсянников [38] показал, что существует ровно семь различных двудольных атомарных графов, число реберных покрытий которых не более 67. Они представлены на рис. 13. З. Овсянников также описал элементарные операции, позволяющие из атомарных графов и уже полученных двудольных графов, последовательно построить все двудольные графы, а также выписал формулы пересчета числа реберных покрытий результирующего графа (довольно сложные).

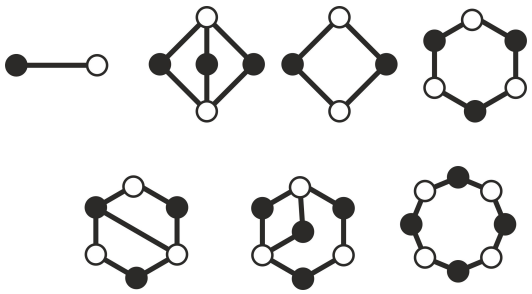


Рис. 13: Атомарные графы с числом реберных покрытий не больше 67.

Был разработан алгоритм последовательного перебора всех двудольных графов, подсчета числа их реберных покрытий и проверки достаточности перебора (чтобы утверждать, что данное число реализуется — достаточно предъявить пример, а чтобы утверждать, что не реализуется, необходимо доказать, что перебрано уже достаточно графов).

Теорема 8 (Овсянников [38])**.** *Для натуральных чисел от* 1 *до* 1000*, не существует двудольных графов с* 19*,* 37*,* 51*,* 59*,* 67 *реберными покрытиями.*

Кроме того, возможно также не хорошими являются числа 82*,* 97*,* 149*,* 197*,* 233*,* 257*,* 291*,* 379*. Все остальные числа от* 1 *до* 1000 *— хорошие.*

Насколько нам известно, найденная последовательность 19, 37, 51, 59, 67 пока нигде не встречалась. Было бы интересно продолжить исследования, в частности, провести более масштабные компьютерные вычисления и продолжить последовательность.

Список литературы

[1] Табачников С.Л., *Геометрия и биллиарды* // НИЦ «Регулярная и хаотическая динамика», Ижевский институт компьютерных исследований, Москва, Ижевск, 2011.

[2] Биркгоф Дж.Д., *Динамические системы* // Издательский дом «Удмуртский университет», Ижевск, 1999.

[3] Козлов В.В., Трещёв Д.В., *Генетическое введение в динамику систем с ударами* // Изд-во МГУ, Москва, 1991.

[4] Болсинов А.В., Фоменко А.Т., *Интегрируемые гамильтоновы системы. Геометрия, топология, классификация* , Т. 1, 2 // НИЦ "Регулярная и хаотическая динамика", Москва, Ижевск, 1999.

[5] Dragovic V., Radnovic M., "Bifurcations of Liouville tori in elliptical billiards," Regul. Chaotic Dyn., Математический ин-т им.В.А.Стеклова РАН, **14** (4–5), 479 (2009).

[6] Драгович В., Раднович М., *Интегрируемые биллиарды, квадрики и многомерные поризмы Понселе* // НИЦ "Регулярная и хаотическая динамика", Москва, Ижевск 2010.

[7] Фокичева В.В., "Описание особенностей системы "биллиард в эллипсе"," Вестн. Моск. ун-та. Матем. Механ., Издательство Московского университета, Москва, No. 5, 31 (2012).

[8] Фокичева В.В., "Описание особенностей системы бильярда в областях, ограниченных софокусными эллипсами и гиперболами," Вестн. Моск. ун-та. Сер. 1, Матем. Мех., No. 4, 18 (2014) [англ. пер.: Fokicheva V. V., "Description of singularities for billiard systems bounded by confocal ellipses or hyperbolas", Moscow Univ. Math. Bull, **69** (4), 148 (2014).

[9] Фокичева В.В., "Классификация биллиардных движений в областях, ограниченных софокусными параболами," Матем. сб., **205** (8), 139 (2014) [англ. пер.: Fokicheva V. V., "Classification of billiard motions in domains bounded by confocal parabolas", Sb. Math., **205** (8), 1201 (2014).

[10] Фокичева В.В., "Топологическая классификация биллиардов в локально плоских областях, ограниченных дугами софокусных квадрик," Матем. сб., **206** (10), 127 (2015).

[11] Фокичева В.В., Фоменко А.Т., "Интегрируемые биллиарды моделируют важные интегрируемые случаи динамики твёрдого тела," ДАН, **465** (2), 1 (2015).

[12] Фоменко А.Т., Цишанг Х., "О типичных топологических свойствах интегрируемых гамильтоновых систем," Изв. АН СССР, **52** (2) 378 (1988).

[13] Фоменко А.Т., "Симплектическая топология вполне интегрируемых гамильтоновых систем," Успехи матем. наук, **44** (1), 145 (1989).

[14] Фоменко А.Т., Цишанг Х., "Топологический инвариант и критерий эквивалентности интегрируемых гамильтоновых систем с двумя степенями свободы," Изв. АН СССР, **54** (3), 546 (1990).

[15] Кудрявцева Е.А., "Интегрируемые по Лиувиллю обобщенные биллиардные потоки и теоремы типа Понселе," Фундаментальная и прикладная математика, **20** (3), 113 (2015).

[16] Кудрявцева Е.А., Никонов И.М., Фоменко А.Т., "Максимально симметричные клеточные разбиения поверхностей и их накрытия," Матем. сб., **199** (9), 3 (2008).

[17] Lazutkin V., *KAM theory and semiclassical approximations to eigenfunctions* // Springer–Verlag, Berlin, 1993.

[18] Арнольд В.И., *Математические методы классической механики*, Наука, Москва, 1989.

[19] Ошемков А.А., "Описание изоэнергетических поверхностей интегрируемых гамильтоновых систем с двумя степенями свободы," Труды семинара по векторному и тензорному анализу. Вып. 23, Изд-во МГУ, Москва. 1988, сс. 122–132.

[20] Oshemkov A.A., Fomenko A.T., "Invariants for the Main Integrable Cases of the Rigid Body Motion Equations," in *Advances in Soviet Mathematics*, v. 6, Ed.: Fomenko A.T., AMS, Providence, 1991, pp. 67-146.

[21] Болсинов А.В., Фоменко А.Т., "Геодезический поток эллипсоида траекторно эквивалентен интегрируемому случаю Эйлера в динамике твердого тела," Доклады РАН, **339** (3), 293 (1994).

[22] Болсинов А.В., Фоменко А.Т., "Траекторная классификация геодезических потоков на двумерных эллипсоидах. Задача Якоби траекторно эквивалентна интегрируемому случаю Эйлера в динамике твердого тела," Функциональный анализ и его приложения, **29** (3), 1 (1995).

[23] Орел О.Е., "Функция вращения для интегрируемых задач, сводящихся к уравнениям Абеля. Траекторная классификация систем Горячева-Чаплыгина," Матем. сборник, **186** (2), 105 (1995).

[24] Орел О.Е., Такахаши Ш., "Траекторная классификация интегрируемых задач Лагранжа и Горячева-Чаплыгина методами компьютерного анализа," Матем. сборник, **187** (1), 95 (1996).

[25] Морозов П.В., "Лиувиллева классификация интегрируемых систем случая Клебша," Матем. сб., **193** (10), 113 (2002).

[26] Морозов П.В., "Топология слоений Лиувилля случаев интегрируемости Стеклова и Соколова уравнений Кирхгофа," Матем. сб., **195** (3), 69 (2004).

[27] Славина Н.С., "Классификация системы Ковалевской-Яхьи с точностью до лиувиллевой эквивалентности," Доклады РАН, серия: математика, **452** (3), 252 (2013).

[28] Николаенко С.С., "Топологическая классификация систем Чаплыгина в динамике твердого тела в жидкости," Матем. сб., **205** (2), 75 (2014).

[29] Николаенко С.С., "Топологическая классификация интегрируемого случая Горячева в динамике твердого тела," Матем. сб., **205** (2), 123 (2016).

[30] Сечкин Г.М., "Топология динамики неоднородного эллипсоида вращения на гладкой плоскости," дипломная работа, МГУ имени М.В. Ломоносова, механико-математический факультет, кафедра дифференциальной геометрии и приложений, 2015.

[31] Козлов В.В., *Симметрии, топология и резонансы в гамильтоновой механике*, Изд-во Удмуртского гос. ун-та, Ижевск, 1995.

[32] Hausdorff F., *Grundzüge der Mengenlehre*, Veit, Leipzig, 1914.

[33] Gromov M., "Groups of Polynomial Growth and Expanding Maps," Inst. Hautes Études Sci. Publ. Math., **53**, pp. 53–73 (1981).

[34] Иванов А. О., Николаева Н. К., Тужилин А. А., "Метрика Громова–Хаусдорфа на пространстве метрических компактов – строго внутренняя," Матем. заметки, **100** (6), 947 (2016).

[35] Ivanov A. O., Tropin A. M., Tuzhilin A. A., "Fermat–Steiner problem in the metric space of compact sets endowed with Hausdorff distance," J. of Geometry, (2016).

[36] Blackburn C.C., Lund K., Schliker S., Sigmon P., and Zupan A., "A Missing Prime Configuration in the Hausdorff Metric Geometry," J. Geom, **92**, pp. 28–59 (2009).

[37] Honigs K., "Missing Edge Coverings of Bipartite Graphs and the Gemetry of the Hausdorff Metric," J. Geom., **104**, pp. 107–125 (2013).

[38] Овсянников З.Н., "Количество реберных покрытий двудольных графов или кратчайших с фиксированными концами в пространстве компактов в $\mathbb{R}^n$," Докл. РАН, **466** (4), 402 (2016).

О покрытиях и разбиениях натуральных чисел, имеющих два последовательных пропуска длины 1

П. С. Дергач, Е. Д. Данилевская

В статье приводится результат о нахождении минимального количества $L(n)$ арифметических прогрессий, необходимых для того, чтобы получить в объединении все натуральные числа, не сравнимые по модулю n с 0 и -2. Здесь n — произвольное натуральное число. При этом прогрессии могут пересекаться. Приводится точное значение для функции $L(n)$, а также конструктивное разбиение этого подмножества натурального ряда на $L(n)$ арифметических прогрессий.

Ключевые слова: натуральный ряд, арифметическая прогрессия, декомпозиция.

Введение

В рамках данной курсовой работы продолжаются исследования задачи о разбиении прогрессивных множеств на минимальное количество арифметических прогрессий. Прогрессивными множествами называем подмножества натурального ряда, образованные объединением конечного количества арифметических прогрессий. В курсовой работе задача решается в предположении, что прогрессивное множество состоит из всех таких натуральных чисел, которые по некоторому фиксированному натуральному числу n не дают остатки 0 и $n-2$. То есть, это множество содержит $n-2$ последовательных натуральных чисел, один пропуск, число, один пропуск и дальше опять $n-2$ чисел, пропуск, число,пропуск и так далее. О решении похожих задач можно прочитать в статьях [1-5]. О других интересных аспектах исследований авторов и других ученых в смежных областях к тематике данной работы можно прочитать в [6-16].

Основные определения и результаты

Множество натуральных чисел обозначаем через $\mathbb{N}$. Множество целых неотрицательных чисел обозначаем через $\mathbb{N}_0$. Пусть $a \in \mathbb{N}$, $b \in \mathbb{N}_0$. Тогда *арифметической прогрессией с началом a и шагом b* называется множество

$$(a, b) := \{a + ib \mid i \in \mathbb{N}_0\}.$$

Через $T(n)$ обозначаем множество

$$T(n) := \mathbb{N} \setminus ((n-2, n) \cup (n, n)).$$

Пусть $n \in \mathbb{N}$. Через $L(n)$ обозначаем минимальное количество арифметических прогрессий, на которые можно разбить множество $T(n)$.

Множество $X \subseteq \mathbb{N}$ называем *опорным семейством для множества* $Y \subseteq \mathbb{N}$, если для любых $x_1, x_2 \in X, x_1 < x_2$ выполнено

$$(x_1, x_2 - x_1) \cap Y \neq \emptyset.$$

Теорема 1. *Пусть $n \in \mathbb{N}$ и $n = p_1^{a_1} \cdot p_2^{a_2} \dots p_t^{a_t}$ — разложение числа n на простые множители и $p_1 < p_2 < \dots < p_t$. Тогда в зависимости от случаев*

$$L(n) = 2a_1 - 3, \quad p_1 = 2, t = 1;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + (2a_1 - 2), \quad p_1 = 2, t = 2;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + 1, \quad p_1 = 2, t > 2, a_1 = 1;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + (2a_1 - 2), \quad p_1 = 2, t > 2, a_1 > 1;$$

$$L(n) = (2a_1 - 1)(p_1 - 1) - 1, \quad p_1 > 2, t = 1;$$

$$L(n) = (2a_1 - 1)(p_1 - 1) + \dots + (2a_t - 1)(p_t - 1), \quad p_1 > 2, t > 1.$$

Доказательство вспомогательных утверждений

Лемма 1. Для любых $a, c \in \mathbb{N}_0$ и $b, d \in \mathbb{N}$ верно

$$(a, b) \cap (c, d) \neq \emptyset \Longleftrightarrow a \equiv c \ (mod \ \text{НОД}(b, d)).$$

Доказательство леммы см. в [1].

Лемма 2. Пусть $n \in \mathbb{N}$, $X \subseteq T(n)$, $Y = (n-2, n) \cup (n, n)$ и X - опорное семейство для Y. Тогда

$$L(n) \geqslant |X|.$$

Доказательство.

В любом разбиении множества $T(n)$ на арифметические прогрессии ни в какой из прогрессий не будет одновременно два числа из опорного семейства. В самом деле, если бы это было не так, то тогда для некоторых чисел $x_1, x_2 \in X$ прогрессия $(x_1, x_2 - x_1)$ лежала бы целиком в какой-то прогрессии разбиения и при этом пересекалась бы с множеством Y. Но ни одна из прогрессий разбиения с Y пересекаться не будет, так как

$$T(n) = \mathbb{N} \setminus ((n-2, n) \cup (n, n)).$$

Лемма доказана.

Доказательство основного утверждения

Теорема 1. *Пусть $n \in \mathbb{N}$ и $n = p_1^{a_1} \cdot p_2^{a_2} \ldots p_t^{a_t}$ — разложение числа n на простые множители и $p_1 < p_2 < \ldots < p_t$. Тогда в зависимости от случаев*

$$L(n) = 2a_1 - 3, \quad p_1 = 2, t = 1;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + (2a_1 - 2), \quad p_1 = 2, t = 2;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + \ldots + (2a_t - 1)(p_t - 1) + 1, \quad p_1 = 2, t > 2, a_1 = 1;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + \ldots + (2a_t - 1)(p_t - 1) + (2a_1 - 2), \quad p_1 = 2, t > 2, a_1 > 1;$$

$$L(n) = (2a_1 - 1)(p_1 - 1) - 1, \quad p_1 > 2, t = 1;$$

$$L(n) = (2a_1 - 1)(p_1 - 1) + \ldots + (2a_t - 1)(p_t - 1), \quad p_1 > 2, t > 1.$$

Доказательство.

Пусть $p_1 = 2, t = 1$. Докажем тогда, что

$$L(n) = L(2^{a_1}) = 2a_1 - 3.$$

Сначала представим $T(n)$ в виде объединения $2a_1 - 3$ арифметических прогрессий. Это можно сделать следующим образом:

$$T(n) = (1,2) \cup (2,8) \cup (4,8) \cup \ldots \cup (2^{a_1-1} - 2, 2^{a_1}) \cup (2^{a_1-1}, 2^{a_1}) =$$

$$= (1,2) \cup ((2,8) \cup \ldots \cup (2^{a_1-1} - 2, 2^{a_1})) \cup ((4,8) \cup \ldots \cup (2^{a_1-1}, 2^{a_1})).$$

Видно, что здесь $1 + (a_1 - 2) + (a_1 - 2) = 2a_1 - 3$ прогрессий. И множество

$$(4,8) \cup \ldots \cup (2^{a_1-1}, 2^{a_1})$$

покрывает все четные числа, делящиеся на 4, но не дающие остатка 0 по модулю 2^{a_1}. А множество

$$(2,8) \cup \ldots \cup (2^{a_1-1} - 2, 2^{a_1})$$

покрывает все четные числа, не делящиеся на 4 и не дающие остатка $2^{a_1} - 2$ по модулю 2^{a_1}. Поэтому

$$L(2^{a_1}) \leqslant 2a_1 - 3.$$

Покажем, что

$$L(2^{a_1}) \geqslant 2a_1 - 3.$$

Рассмотрим множества

$$X_1 := \{1\},$$

$$X_2 := \{2, 6, 14, \ldots, 2^{a_1-1} - 2\},$$

$$X_3 := \{4, 8, 16, \ldots, , 2^{a_1-1}\},$$

$$Y := (2^{a_1} - 2, 2^{a_1}) \cup (2^{a_1}, 2^{a_1}).$$

Покажем, что множество

$$X := X_1 \cup X_2 \cup X_3$$

будет опорным семейством для множества Y. Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (2^{a_1} - 2, 2^{a_1}) \neq \emptyset, \tag{1}$$

$$(x_1, x_2 - x_1) \cap (2^{a_1}, 2^{a_1}) \neq \emptyset. \tag{2}$$

Возможны случаи:
Случай 1.

$x_1 \in X_1, x_2 \in X_2$. Тогда НОД$(x_2 - x_1, 2^{a_1}) = 1$ и по лемме 1 верно (1).
Случай 2.
$x_1 \in X_1, x_2 \in X_3$. Случай аналогичен предыдущему.
Случай 3.
$x_1 \in X_2, x_2 \in X_2$. Пусть

$$x_1 = 2^{d_1} - 2,\ x_2 = 2^{d_2} - 2.$$

Тогда НОД$(x_2 - x_1, 2^{a_1}) = 2^{d_1}$ и по лемме 1 верно (1).
Случай 4.
$x_1 \in X_2, x_2 \in X_3$. Пусть

$$x_1 = 2^{d_1} - 2,\ x_2 = 2^{d_2}.$$

Тогда НОД$(x_2 - x_1, 2^{a_1}) = 2$ и по лемме 1 верно (1).
Случай 5.
$x_1 \in X_3, x_2 \in X_2$. Случай аналогичен предыдущему.
Случай 6.
$x_1 \in X_3, x_2 \in X_3$. Пусть

$$x_1 = 2^{d_1},\ x_2 = 2^{d_2}.$$

Тогда НОД$(x_2 - x_1, 2^{a_1}) = 2^{d_1}$ и по лемме 1 верно (2).
Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y. Но в множестве X всего

$$|X_1| + |X_2| + |X_3| = 1 + (a_1 - 2) + (a_1 - 2)$$

элементов. Поэтому по лемме 2 получаем $L(2^{a_1}) \geqslant 2a_1 - 3$. В случае, когда $p_1 = 2, t = 1$, утверждение теоремы доказано.

Пусть $p_1 = 2, t = 2$. Докажем тогда, что

$$L(n) = L(2^{a_1} p_2^{a_2}) = (2a_2 - 1)(p_2 - 1) + (2a_1 - 2).$$

Здесь возможны два варианта:

$$1) a_1 = 1; \qquad 2) a_1 > 1.$$

В первом варианте для доказательства верхней оценки нужно представить $T(n)$ в виде объединения $(2a_2 - 1)(p_2 - 1)$ арифметических прогрессий. Это можно сделать следующим образом:

$$T(n) = (1, 2) \cup ((2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \ldots \cup (2p_2 - 4, 2p_2)) \cup$$

$$\cup((2p_2-2,2p_2^2)\cup(4p_2-2,2p_2^2)\cup(6p_2-2,2p_2^2)\cup\ldots\cup((2p_2-2)p_2-2,2p_2^2))\cup$$
$$\cup((2p_2^2-2,2p_2^3)\cup(4p_2^2-2,2p_2^3)\cup(6p_2^2-2,2p_2^3)\cup\ldots\cup((2p_2-2)p_2^2-2,2p_2^3))\cup$$
$$\cup\ldots\cup((2p_2^{a_2-1}-2,2p_2^{a_2})\cup(4p_2^{a_2-1}-2,2p_2^{a_2})\cup(6p_2^{a_2-1}-2,2p_2^{a_2})\cup$$
$$\cup\ldots\cup((2p_2-2)p_2^{a_2-1}-2,2p_2^{a_2}))\cup$$
$$\cup((2p_2,2p_2^2)\cup(4p_2,2p_2^2)\cup(6p_2,2p_2^2)\cup\ldots\cup((2p_2-2)p_2,2p_2^2))\cup$$
$$\cup((2p_2^2,2p_2^3)\cup(4p_2^2,2p_2^3)\cup(6p_2^2,2p_2^3)\cup\ldots\cup((2p_2-2)p_2^2,2p_2^3))\cup\ldots\cup$$
$$\cup((2p_2^{a_2-1},2p_2^{a_2})\cup(4p_2^{a_2-1},2p_2^{a_2})\cup(6p_2^{a_2-1},2p_2^{a_2})\cup\ldots\cup((2p_2-2)p_2^{a_2-1},2p_2^{a_2})).$$

Видно, что здесь $1+(p_2-2)+2(a_1-1)(p_2-1)=(2a_2-1)(p_2-1)$ прогрессий. Множество

$$(2,2p_2)\cup(4,2p_2)\cup(6,2p_2)\cup\ldots\cup(2p_2-4,2p_2)$$

покрывает все четные числа, не дающие остатков 0 и p_2-2 по модулю p_2. Множество

$$((2p_2-2,2p_2^2)\cup(4p_2-2,2p_2^2)\cup(6p_2-2,2p_2^2)\cup\ldots\cup((2p_2-2)p_2-2,2p_2^2))\cup$$
$$\cup((2p_2^2-2,2p_2^3)\cup(4p_2^2-2,2p_2^3)\cup(6p_2^2-2,2p_2^3)\cup\ldots\cup((2p_2-2)p_2^2-2,2p_2^3))\cup$$
$$\cup\ldots\cup((2p_2^{a_2-1}-2,2p_2^{a_2})\cup(4p_2^{a_2-1}-2,2p_2^{a_2})\cup$$
$$\cup(6p_2^{a_2-1}-2,2p_2^{a_2})\cup\ldots\cup((2p_2-2)p_2^{a_2-1}-2,2p_2^{a_2}))$$

покрывает все четные числа, дающие остаток p_2-2 по модулю p_2 и не дающие остатка $p_2^{a_2}-2$ по модулю $p_2^{a_2}$. И множество

$$((2p_2,2p_2^2)\cup(4p_2,2p_2^2)\cup(6p_2,2p_2^2)\cup\ldots\cup((2p_2-2)p_2,2p_2^2))\cup$$
$$\cup((2p_2^2,2p_2^3)\cup(4p_2^2,2p_2^3)\cup(6p_2^2,2p_2^3)\cup\ldots\cup((2p_2-2)p_2^2,2p_2^3))\cup\ldots\cup$$
$$\cup((2p_2^{a_2-1},2p_2^{a_2})\cup(4p_2^{a_2-1},2p_2^{a_2})\cup(6p_2^{a_2-1},2p_2^{a_2})\cup\ldots\cup((2p_2-2)p_2^{a_2-1},2p_2^{a_2}))$$

покрывает все четные числа, дающие остаток 0 по модулю p_2 и не дающие остатка 0 по модулю $p_2^{a_2}$. Поэтому

$$L(2p_2^{a_2})\leqslant(2a_2-1)(p_2-1).$$

Для доказательства нижней оценки введем обозначения

$$X_1:=\{p_2^{a_2}\},$$

$$X_2 := \{2, 4, 6, \ldots, 2(p_2 - 2)\},$$
$$X_3^1 := \{2p_2 - 2, 4p_2 - 2, 6p_2 - 2, \ldots, 2(p_2 - 1)p_2 - 2\},$$
$$X_3^2 := \{2p_2^2 - 2, 4p_2^2 - 2, 6p_2^2 - 2, \ldots, 2(p_2 - 1)p_2^2 - 2\},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$X_3^{a_2-1} := \{2p_2^{a_2-1} - 2, 4p_2^{a_2-1} - 2, 6p_2^{a_2-1} - 2, \ldots, 2(p_2 - 1)p_2^{a_2-1} - 2\},$$
$$X_4^1 := \{2p_2, 4p_2, 6p_2, \ldots, 2(p_2 - 1)p_2\},$$
$$X_4^2 := \{2p_2^2, 4p_2^2, 6p_2^2, \ldots, 2(p_2 - 1)p_2^2\},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$X_4^{a_2-1} := \{2p_2^{a_2-1}, 4p_2^{a_2-1}, 6p_2^{a_2-1}, \ldots, 2(p_2 - 1)p_2^{a_2-1}\},$$
$$Y := (2p_2^{a_2} - 2, 2p_2^{a_2}) \cup (2p_2^{a_2}, 2p_2^{a_2})$$

и покажем, что множество

$$X := X_1 \cup X_2 \cup X_3^1 \cup \ldots \cup X_3^{a_2-1} \cup X_4^1 \cup \ldots \cup X_4^{a_2-1}$$

будет опорным семейством для множества Y. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (2p_2^{a_2} - 2, 2p_2^{a_2}) \neq \emptyset, \tag{3}$$

$$(x_1, x_2 - x_1) \cap (2p_2^{a_2}, 2p_2^{a_2}) \neq \emptyset. \tag{4}$$

Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Возможны случаи:
Случай 1.
$x_1 \in X_1, x_2 \in X_2$ или $x_2 \in X_1, x_1 \in X_2$. Тогда НОД$(x_2 - x_1, 2p_2^{a_2}) = 1$ и по лемме 1 верно (3).
Случай 2.
$x_1 \in X_1, x_2 \in X_3^i$ или $x_2 \in X_1, x_1 \in X_3^i$. Случай аналогичен предыдущему.
Случай 3.
$x_1 \in X_1, x_2 \in X_4^i$ или $x_2 \in X_1, x_1 \in X_4^i$. Тогда НОД$(x_2 - x_1, 2p_2^{a_2}) = p_2^i$ и по лемме 1 верно (4).
Случай 4.
$x_1 \in X_2, x_2 \in X_2$. Тогда НОД$(x_2 - x_1, 2p_2^{a_2}) = 2$ и по лемме 1 верно (3).
Случай 5.
$x_1 \in X_2, x_2 \in X_3^i$ или $x_2 \in X_2, x_1 \in X_3^i$. Случай аналогичен предыдущему.
Случай 6.

$x_1 \in X_2, x_2 \in X_4^i$ или $x_2 \in X_2, x_1 \in X_4^i$. Случай аналогичен предыдущему.
Случай 7.
$x_1 \in X_3^i, x_2 \in X_3^i$. Тогда НОД$(x_2 - x_1, 2p_2^{a_2}) = 2p_2^i$ и по лемме 1 верно (3).
Случай 8.
$x_1 \in X_3^i, x_2 \in X_3^j, i < j$. Случай аналогичен предыдущему.
Случай 9.
$x_1 \in X_3^i, x_2 \in X_3^j, i > j$. Тогда НОД$(x_2 - x_1, 2p_2^{a_2}) = 2p_2^j$ и по лемме 1 верно (3).
Случай 10.
$x_1 \in X_3^i, x_2 \in X_4^j$. Тогда НОД$(x_2 - x_1, 2p_2^{a_2}) = 2$ и по лемме 1 верно (3).
Случай 11.
$x_1 \in X_4^i, x_2 \in X_4^i$. Тогда НОД$(x_2 - x_1, 2p_2^{a_2}) = 2p_2^i$ и по лемме 1 верно (4).
Случай 12.
$x_1 \in X_4^i, x_2 \in X_4^j, i < j$. Случай аналогичен предыдущему.
Случай 13.
$x_1 \in X_4^i, x_2 \in X_4^j, i > j$. Тогда НОД$(x_2 - x_1, 2p_2^{a_2}) = 2p_2^j$ и по лемме 1 верно (4).
Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y. Но в множестве X всего

$$|X_1| + |X_2| + |X_3^1| + \ldots + |X_3^{a_2-1}| + |X_4^1| + \ldots + |X_4^{a_2-1}| =$$

$$= 1 + (p_2 - 2) + 2(a_2 - 1)(p_2 - 1) = (2a_2 - 1)(p_2 - 1)$$

элементов. Поэтому по лемме 2 получаем $L(2p_2^{a_2}) \geqslant (2a_2 - 1)(p_2 - 1)$.
Во втором варианте для доказательства верхней оценки нужно представить $T(n)$ в виде объединения $(2a_2-1)(p_2-1)+(2a_1-2)$ арифметических прогрессий. Это можно сделать следующим образом:

$$T(n) = (1, 2) \cup ((2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \ldots \cup (2p_2 - 4, 2p_2)) \cup$$

$$\cup((4p_2 - 2, 8p_2) \cup (8p_2 - 2, 16p_2) \cup \ldots \cup ((2^{a_1-1}p_2 - 2, 2^{a_1}p_2)) \cup$$

$$\cup((2^{a_1}p_2 - 2, 2^{a_1}p_2^2) \cup (2^{a_1}p_2^2 - 2, 2^{a_1}p_2^3) \cup \ldots \cup (2^{a_1}p_2^{a_2-1} - 2, 2^{a_1}p_2^{a_2})) \cup$$

$$\cup((2 \cdot 2^{a_1}p_2 - 2, 2^{a_1}p_2^2) \cup (2 \cdot 2^{a_1}p_2^2 - 2, 2^{a_1}p_2^3) \cup \ldots \cup$$

$$\cup(2 \cdot 2^{a_1}p_2^{a_2-1} - 2, 2^{a_1}p_2^{a_2})) \cup \ldots \cup (((p_2 - 1)2^{a_1}p_2 - 2, 2^{a_1}p_2^2) \cup$$

$$\cup((p_2 - 1)2^{a_1}p_2^2 - 2, 2^{a_1}p_2^3) \cup \ldots \cup ((p_2 - 1)2^{a_1}p_2^{a_2-1} - 2, 2^{a_1}p_2^{a_2})) \cup$$

$$\cup((4p_2, 8p_2) \cup (8p_2, 16p_2) \cup \ldots \cup ((2^{a_1-1}p_2, 2^{a_1}p_2)) \cup$$

$$\cup((2^{a_1}p_2, 2^{a_1}p_2^2) \cup (2^{a_1}p_2^2, 2^{a_1}p_2^3) \cup \ldots \cup (2^{a_1}p_2^{a_2-1}, 2^{a_1}p_2^{a_2}))\cup$$
$$\cup((2\cdot 2^{a_1}p_2, 2^{a_1}p_2^2) \cup (2\cdot 2^{a_1}p_2^2, 2^{a_1}p_2^3) \cup \ldots \cup (2\cdot 2^{a_1}p_2^{a_2-1}, 2^{a_1}p_2^{a_2}))\cup$$
$$\cup \ldots \cup (((p_2-1)2^{a_1}p_2, 2^{a_1}p_2^2) \cup ((p_2-1)2^{a_1}p_2^2, 2^{a_1}p_2^3)\cup$$
$$\cup \ldots \cup ((p_2-1)2^{a_1}p_2^{a_2-1}, 2^{a_1}p_2^{a_2})) \cup ((2p_2-2, 4p_2) \cup (2p_2, 4p_2)).$$

Видно, что здесь

$$1 + (p_2-2) + 2(a_1-2) + 2(a_1-1)(p_2-1) + 2 =$$
$$= (2a_2-1)(p_2-1) + (2a_1-2)$$

прогрессий. Множество

$$(2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \ldots \cup (2p_2-4, 2p_2)$$

покрывает все четные числа, не дающие остатков 0 и p_2-2 по модулю p_2. Множество

$$((4p_2-2, 8p_2) \cup (8p_2-2, 16p_2) \cup \ldots \cup ((2^{a_1-1}p_2-2, 2^{a_1}p_2))\cup$$
$$\cup((2^{a_1}p_2-2, 2^{a_1}p_2^2) \cup (2^{a_1}p_2^2-2, 2^{a_1}p_2^3) \cup \ldots \cup (2^{a_1}p_2^{a_2-1}-2, 2^{a_1}p_2^{a_2}))\cup$$
$$\cup((2\cdot 2^{a_1}p_2-2, 2^{a_1}p_2^2) \cup (2\cdot 2^{a_1}p_2^2-2, 2^{a_1}p_2^3) \cup \ldots \cup (2\cdot 2^{a_1}p_2^{a_2-1}-2, 2^{a_1}p_2^{a_2}))\cup$$
$$\cup \ldots \cup (((p_2-1)2^{a_1}p_2-2, 2^{a_1}p_2^2) \cup ((p_2-1)2^{a_1}p_2^2-2, 2^{a_1}p_2^3)\cup$$
$$\cup \ldots \cup ((p_2-1)2^{a_1}p_2^{a_2-1}-2, 2^{a_1}p_2^{a_2}))$$

покрывает все числа, дающие остаток 2 по модулю 4, дающие остаток p_2-2 по модулю p_2 и не дающие остатка $2^{a_1}p_2^{a_2}-2$ по модулю $2^{a_1}p_2^{a_2}$. И множество

$$((4p_2, 8p_2) \cup (8p_2, 16p_2) \cup \ldots \cup ((2^{a_1-1}p_2, 2^{a_1}p_2))\cup$$
$$\cup((2^{a_1}p_2, 2^{a_1}p_2^2) \cup (2^{a_1}p_2^2, 2^{a_1}p_2^3) \cup \ldots \cup (2^{a_1}p_2^{a_2-1}, 2^{a_1}p_2^{a_2}))\cup$$
$$\cup((2\cdot 2^{a_1}p_2, 2^{a_1}p_2^2) \cup (2\cdot 2^{a_1}p_2^2, 2^{a_1}p_2^3) \cup \ldots \cup (2\cdot 2^{a_1}p_2^{a_2-1}, 2^{a_1}p_2^{a_2}))\cup$$
$$\cup \ldots \cup (((p_2-1)2^{a_1}p_2, 2^{a_1}p_2^2) \cup ((p_2-1)2^{a_1}p_2^2, 2^{a_1}p_2^3)\cup$$
$$\cup \ldots \cup ((p_2-1)2^{a_1}p_2^{a_2-1}, 2^{a_1}p_2^{a_2})))$$

покрывает все числа, дающие остаток 0 по модулю 4, дающие остаток 0 по модулю p_2 и не дающие остатка 0 по модулю $2^{a_1}p_2^{a_2}$. Множество

$$(2p_2-2, 4p_2)$$

покрывает все числа, дающие остаток 0 по модулю 4 и дающие остаток $p_2 - 2$ по модулю p_2. Наконец, множество

$$(2p_2, 4p_2)$$

покрывает все числа, дающие остаток 2 по модулю 4 и дающие остаток 0 по модулю p_2. Поэтому

$$L(2p_2^{a_2}) \leqslant (2a_2 - 1)(p_2 - 1) + (2a_1 - 2).$$

Для доказательства нижней оценки введем обозначения

$$X_1 := \{p_2^{a_2}\},$$

$$X_2 := \{4p_2^{a_2} - 2, 8p_2^{a_2} - 2, \ldots, 2^{a_1-1}p_2^{a_2} - 2\},$$
$$X_3 := \{4p_2^{a_2}, 8p_2^{a_2}, \ldots, 2^{a_1-1}p_2^{a_2}\},$$
$$X_4^1 := \{2^{a_1}p_2 - 2, 2 \cdot 2^{a_1}p_2 - 2, \ldots, (a_2 - 1)2^{a_1}p_2 - 2\},$$
$$X_4^2 := \{2^{a_1}p_2^2 - 2, 2 \cdot 2^{a_1}p_2^2 - 2, \ldots, (a_2 - 1)2^{a_1}p_2^2 - 2\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$X_4^{a_2-1} := \{2^{a_1}p_2^{a_2-1} - 2, 2 \cdot 2^{a_1}p_2^{a_2-1} - 2, \ldots, (a_2 - 1)2^{a_1}p_2^{a_2-1} - 2\},$$
$$X_5^1 := \{2^{a_1}p_2, 2 \cdot 2^{a_1}p_2, \ldots, (a_2 - 1)2^{a_1}p_2\},$$
$$X_5^2 := \{2^{a_1}p_2^2, 2 \cdot 2^{a_1}p_2^2, \ldots, (a_2 - 1)2^{a_1}p_2^2\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$X_5^{a_2-1} := \{2^{a_1}p_2^{a_2-1}, 2 \cdot 2^{a_1}p_2^{a_2-1}, \ldots, (a_2 - 1)2^{a_1}p_2^{a_2-1}\},$$
$$X_6 := \{a, b, c_1, \ldots, c_{p_2-3}, c_{p_2-1}\},$$
$$Y := (2^{a_2}p_2^{a_2} - 2, 2^{a_2}p_2^{a_2}) \cup (2^{a_2}p_2^{a_2}, 2^{a_2}p_2^{a_2}),$$

где $a \equiv 0 \ mod\ 2^{a_1}$, $a \equiv -2 \ mod\ p_2^{a_2}$, $b \equiv -2 \ mod\ 2^{a_1}$, $b \equiv 0 \ mod\ p_2^{a_2}$, $c_i \equiv 0 \ mod\ 2^{a_1}$, $c_i \equiv i \ mod\ p_2^{a_2}$. Покажем, что множество

$$X := X_1 \cup X_2 \cup X_3 \cup X_4^1 \cup \ldots \cup X_4^{a_2-1} \cup X_5^1 \cup \ldots \cup X_5^{a_2-1} \cup X_6$$

будет опорным семейством для множества Y. Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (2^{a_1}p_2^{a_2} - 2, 2^{a_1}p_2^{a_2}) \neq \emptyset, \tag{5}$$

$$(x_1, x_2 - x_1) \cap (2^{a_1} p_2^{a_2}, 2^{a_1} p_2^{a_2}) \neq \emptyset. \tag{6}$$

Возможны случаи:

Случай 1.

$x_1 \in X_1, x_2 \in X_2$ или $x_2 \in X_1, x_1 \in X_2$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 1$ и по лемме 1 верно (5).

Случай 2.

$x_1 \in X_1, x_2 \in X_3$ или $x_2 \in X_1, x_1 \in X_3$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = p_2^{a_2}$ и по лемме 1 верно (6).

Случай 3.

$x_1 \in X_1, x_2 \in X_4^i$ или $x_2 \in X_1, x_1 \in X_4^i$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 1$ и по лемме 1 верно (5).

Случай 4.

$x_1 \in X_1, x_2 \in X_5^i$ или $x_2 \in X_1, x_1 \in X_5^i$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = p_2^i$ и по лемме 1 верно (6).

Случай 5.

$x_1 \in X_1, x_2 = a$ или $x_2 \in X_1, x_1 = a$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 1$ и по лемме 1 верно (5).

Случай 6.

$x_1 \in X_1, x_2 = b$ или $x_2 \in X_1, x_1 = b$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = p_2^{a_2}$ и по лемме 1 верно (6).

Случай 7.

$x_1 \in X_1, x_2 = c_i$ или $x_2 \in X_1, x_1 = c_i$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 1$ и по лемме 1 верно (5).

Случай 8.

$x_1 \in X_2, x_2 \in X_2$, то есть $x_1 = 2^{i_1} p_2^{a_2} - 2$, $x_2 = 2^{i_2} p_2^{a_2} - 2$. Тогда верно НОД$(x_2 - x_1, 2p_2^{a_2}) = 2^{i_1} p_2^{a_2}$ и по лемме 1 получаем (5).

Случай 9.

$x_1 \in X_2, x_2 \in X_3$ или $x_2 \in X_2, x_1 \in X_3$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 10.

$x_1 \in X_2, x_2 \in X_4^i$ или $x_2 \in X_2, x_1 \in X_4^i$. Пусть элемент из X_2 равен $2^j p_2^{a_2} - 2$. Тогда имеет место НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^j p_2^i$ и по лемме 1 верно (5).

Случай 11.

$x_1 \in X_2, x_2 \in X_5^i$ или $x_2 \in X_2, x_1 \in X_5^i$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 12.

$x_1 \in X_2, x_2 = a$ или $x_2 \in X_2, x_1 = a$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2p_2^{a_2}$ и

по лемме 1 верно (5).

Случай 13.

$x_1 \in X_2, x_2 = b$ или $x_2 \in X_2, x_1 = b$. Пусть элемент из X_2 равен $2^j p_2^{a_2} - 2$. Тогда имеет место НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^j$ и по лемме 1 верно (5).

Случай 14.

$x_1 \in X_2, x_2 = c_i$ или $x_2 \in X_2, x_1 = c_i$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 15.

$x_1 \in X_3, x_2 \in X_3$, то есть $x_1 = 2^{i_1} p_2^{a_2}$, $x_2 = 2^{i_2} p_2^{a_2}$. Тогда верно, что НОД$(x_2 - x_1, 2p_2^{a_2}) = 2^{i_1} p_2^{a_2}$ и по лемме 1 получаем (6).

Случай 16.

$x_1 \in X_3, x_2 \in X_4^i$ или $x_2 \in X_3, x_1 \in X_4^i$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 17.

$x_1 \in X_3, x_2 \in X_5^i$ или $x_2 \in X_3, x_1 \in X_5^i$. Пусть элемент из X_3 равен $2^j p_2^{a_2}$. Тогда имеет место НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^j p_2^i$ и по лемме 1 верно (6).

Случай 18.

$x_1 \in X_3, x_2 = a$ или $x_2 \in X_3, x_1 = a$. Пусть элемент из X_3 равен $2^j p_2^{a_2}$. Тогда имеет место равенство НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^j$ и по лемме 1 верно (6).

Случай 19.

$x_1 \in X_3, x_2 = b$ или $x_2 \in X_3, x_1 = b$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2p_2^{a_2}$ и по лемме 1 верно (6).

Случай 20.

$x_1 \in X_3, x_2 = c_i$ или $x_2 \in X_3, x_1 = c_i$. Пусть элемент из X_3 равен $2^j p_2^{a_2}$. Тогда имеет место равенство НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^j$ и по лемме 1 верно (6).

Случай 21.

$x_1 \in X_4^i, x_2 \in X_4^i$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1} p_2^i$ и по лемме 1 верно (5).

Случай 22.

$x_1 \in X_4^i, x_2 \in X_4^j, i < j$. Случай аналогичен предыдущему.

Случай 23.

$x_1 \in X_4^i, x_2 \in X_4^j, i > j$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1} p_2^j$ и по лемме 1 верно (5).

Случай 24.

$x_1 \in X_4^i, x_2 \in X_5^j$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 25.

$x_1 \in X_4^i, x_2 = a$ или $x_2 \in X_4^i, x_1 = a$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2p_2^i$ и по лемме 1 верно (5).

Случай 26.

$x_1 \in X_4^i, x_2 = b$ или $x_2 \in X_4^i, x_1 = b$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1}$ и по лемме 1 верно (5).

Случай 27.

$x_1 \in X_4^i, x_2 = c_i$ или $x_2 \in X_4^i, x_1 = c_i$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 28.

$x_1 \in X_5^i, x_2 \in X_5^i$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1} p_2^i$ и по лемме 1 верно (6).

Случай 29.

$x_1 \in X_5^i, x_2 \in X_5^j, i < j$. Случай аналогичен предыдущему.

Случай 30. $x_1 \in X_5^i, x_2 \in X_5^j, i > j$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1} p_2^j$ и по лемме 1 верно (6).

Случай 31.

$x_1 \in X_5^i, x_2 = a$ или $x_2 \in X_5^i, x_1 = a$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1}$ и по лемме 1 верно (6).

Случай 32.

$x_1 \in X_5^i, x_2 = b$ или $x_2 \in X_5^i, x_1 = b$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2p_2^i$ и по лемме 1 верно (6).

Случай 33.

$x_1 \in X_5^i, x_2 = c_i$ или $x_2 \in X_5^i, x_1 = c_i$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1}$ и по лемме 1 верно (6).

Случай 34.

$x_1 = a, x_2 = b$ или $x_2 = a, x_1 = b$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 35.

$x_1 = a, x_2 = c$ или $x_2 = a, x_1 = c$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1}$ и по лемме 1 верно (6).

Случай 36.

$x_1 = b, x_2 = c$ или $x_2 = b, x_1 = c$. Тогда НОД$(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y. Но в множестве X всего

$$|X_1| + |X_2| + |X_3| + |X_4^1| + \ldots + |X_4^{a_2-1}| + |X_5^1| + \ldots + |X_5^{a_2-1}| + |X_6| =$$

$$= 1 + 2(a_1 - 2) + 2(a_2 - 1)(p_2 - 1) + 2 + (p_2 - 2) =$$

$$= (2a_2 - 1)(p_2 - 1) + 2(a_1 - 1)$$

элементов. Поэтому по лемме 2 получаем

$$L(2p_2^{a_2}) \geqslant (2a_2 - 1)(p_2 - 1) + 2(a_1 - 1).$$

В случае, когда $p_1 = 2, t = 2$, утверждение теоремы доказано.

Пусть $p_1 = 2, t > 2, a_1 = 1$. Докажем тогда, что

$$L(n) = L(2p_2^{a_2} \dots p_t^{a_t}) = (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + 1.$$

для доказательства верхней оценки нужно представить $T(n)$ в виде объединения

$$(2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + 1$$

арифметических прогрессий. Это можно сделать следующим образом:

$$T(n) = (1, 2) \cup ((2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \dots \cup (2p_2 - 4, 2p_2)) \cup$$

$$\cup((2, 2p_3) \cup (4, 2p_3) \cup (6, 2p_3) \cup \dots \cup (2p_3 - 4, 2p_3)) \cup \dots \cup$$

$$\cup((2, 2p_t) \cup (4, 2p_t) \cup (6, 2p_t) \cup \dots \cup (2p_t - 4, 2p_t)) \cup$$

$$\cup((1 \cdot 2p_2p_3 \dots p_t - 2, 2p_2^2p_3 \dots p_t) \cup (2 \cdot 2p_2p_3 \dots p_t - 2, 2p_2^2p_3 \dots p_t) \cup$$

$$\cup \dots \cup ((p_2 - 1) \cdot 2p_2p_3 \dots p_t - 2, 2p_2^2p_3 \dots p_t)) \cup$$

$$\cup((1 \cdot 2p_2^2p_3 \dots p_t - 2, 2p_2^3p_3 \dots p_t) \cup (2 \cdot 2p_2^2p_3 \dots p_t - 2, 2p_2^3p_3 \dots p_t) \cup$$

$$\cup \dots \cup ((p_2 - 1) \cdot 2p_2^2p_3 \dots p_t - 2, 2p_2^3p_3 \dots p_t)) \cup$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\cup((1 \cdot 2p_2^{a_2-1}p_3 \dots p_t - 2, 2p_2^{a_2}p_3 \dots p_t) \cup$$

$$\cup(2 \cdot 2p_2^{a_2-1}p_3 \dots p_t - 2, 2p_2^{a_2}p_3 \dots p_t) \cup \dots \cup$$

$$\cup((p_2 - 1) \cdot 2p_2^{a_2-1}p_3 \dots p_t - 2, 2p_2^{a_2}p_3 \dots p_t)) \cup$$

$$\cup((1 \cdot 2p_2^{a_2}p_3 \dots p_t - 2, 2p_2^{a_2}p_3^2p_4 \dots p_t) \cup$$

$$\cup(2 \cdot 2p_2^{a_2}p_3 \dots p_t - 2, 2p_2^{a_2}p_3^2p_4 \dots p_t) \cup$$

$$\cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2}p_3 \dots p_t - 2, 2p_2^{a_2}p_3^2p_4 \dots p_t)) \cup$$

$$\cup((1 \cdot 2p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2p_2^{a_2}p_3^3p_4 \dots p_t) \cup$$

$$\cup(2 \cdot 2p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2p_2^{a_2}p_3^3p_4 \dots p_t) \cup$$

$$\cup\ldots\cup((p_3-1)\cdot 2p_2^{a_2}p_3^2p_4\ldots p_t-2,2p_2^{a_2}p_3^3p_4\ldots p_t))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t-2,2p_2^{a_2}p_3^{a_3}p_4\ldots p_t)\cup$$

$$\cup(2\cdot 2p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t-2,2p_2^{a_2}p_3^3a_3p_4\ldots p_t)\cup$$

$$\cup\ldots\cup((p_3-1)\cdot 2p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t-2,2p_2^{a_2}p_3^{a_3}p_4\ldots p_t))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t-2,2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$

$$\cup(2\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t-2,2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$

$$\cup\ldots\cup((p_t-1)\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t-2,2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2))\cup$$

$$\cup((1\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2-2,2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$

$$\cup(2\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2-2,2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$

$$\cup\ldots\cup((p_t-1)\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2-2,2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$

$$\cup(2\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup\ldots\cup$$

$$\cup((p_t-1)\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t}))\cup$$

$$\cup((1\cdot 2p_2p_3\ldots p_t,2p_2^2p_3\ldots p_t)\cup(2\cdot 2p_2p_3\ldots p_t,2p_2^2p_3\ldots p_t)\cup\ldots\cup$$

$$\cup((p_2-1)\cdot 2p_2p_3\ldots p_t,2p_2^2p_3\ldots p_t))\cup$$

$$\cup((1\cdot 2p_2^2p_3\ldots p_t,2p_2^3p_3\ldots p_t)\cup(2\cdot 2p_2^2p_3\ldots p_t,2p_2^3p_3\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot 2p_2^2p_3\ldots p_t,2p_2^3p_3\ldots p_t))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2p_2^{a_2-1}p_3\ldots p_t,2p_2^{a_2}p_3\ldots p_t)\cup$$

$$\cup(2\cdot 2p_2^{a_2-1}p_3\ldots p_t,2p_2^{a_2}p_3\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot 2p_2^{a_2-1}p_3\ldots p_t,2p_2^{a_2}p_3\ldots p_t))\cup$$

$$\cup((1\cdot 2p_2^{a_2}p_3\ldots p_t,2p_2^{a_2}p_3^2p_4\ldots p_t)\cup$$

$$\cup(2\cdot 2p_2^{a_2}p_3\ldots p_t,2p_2^{a_2}p_3^2p_4\ldots p_t)\cup$$

$$\cup\ldots\cup((p_3-1)\cdot 2p_2^{a_2}p_3\ldots p_t,2p_2^{a_2}p_3^2p_4\ldots p_t))\cup$$

$$\cup((1\cdot 2p_2^{a_2}p_3^2p_4\dots p_t, 2p_2^{a_2}p_3^3p_4\dots p_t)\cup$$

$$\cup(2\cdot 2p_2^{a_2}p_3^2p_4\dots p_t, 2p_2^{a_2}p_3^3p_4\dots p_t)\cup$$

$$\cup\dots\cup((p_3-1)\cdot 2p_2^{a_2}p_3^2p_4\dots p_t, 2p_2^{a_2}p_3^3p_4\dots p_t))\cup$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\cup((1\cdot 2p_2^{a_2}p_3^{a_3-1}p_4\dots p_t, 2p_2^{a_2}p_3^{a_3}p_4\dots p_t)\cup$$

$$\cup(2\cdot 2p_2^{a_2}p_3^{a_3-1}p_4\dots p_t, 2p_2^{a_2}p_3^3a_3p_4\dots p_t)\cup$$

$$\cup\dots\cup((p_3-1)\cdot 2p_2^{a_2}p_3^{a_3-1}p_4\dots p_t, 2p_2^{a_2}p_3^{a_3}p_4\dots p_t))\cup$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\cup((1\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t, 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^2)\cup$$

$$\cup(2\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t, 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^2)\cup$$

$$\cup\dots\cup((p_t-1)\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t, 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^2))\cup$$

$$\cup((1\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^2, 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^3)\cup$$

$$\cup(2\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^2, 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^3)\cup$$

$$\cup\dots\cup((p_t-1)\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^2, 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^3))\cup$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\cup((1\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$

$$\cup(2\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$

$$\cup\dots\cup((p_t-1)\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t}))\cup$$

$$\cup(2a_1, 2p_2p_t)\cup(2a_2, 2p_2p_3)\cup\dots\cup(2a_{t-1}, 2p_{t-1}p_t),$$

где при $i=1$ имеем $1\leqslant a_1\leqslant p_2p_t$, $a_1\equiv 0 \mod p_t$, $a_1\equiv -1 \mod p_2$ и при $2\leqslant i\leqslant t-1$ имеем $1\leqslant a_i\leqslant p_ip_{i+1}$, $a_i\equiv 0 \mod p_i$, $a_i\equiv -1 \mod p_{i+1}$. Здесь серия

$$((2,2p_2)\cup(4,2p_2)\cup(6,2p_2)\cup\dots\cup(2p_2-4,2p_2))\cup$$

$$\cup((2,2p_3)\cup(4,2p_3)\cup(6,2p_3)\cup\dots\cup(2p_3-4,2p_3))\cup\dots\cup$$

$$\cup((2,2p_t)\cup(4,2p_t)\cup(6,2p_t)\cup\dots\cup(2p_t-4,2p_t))$$

накрывает все четные числа, не сравнимые с 0 и -2 по модулям $p_2, \ldots, p_t$. Серия

$$((1 \cdot 2p_2p_3 \ldots p_t - 2, 2p_2^2p_3 \ldots p_t) \cup (2 \cdot 2p_2p_3 \ldots p_t - 2, 2p_2^2p_3 \ldots p_t) \cup$$

$$\cup \ldots \cup ((p_2 - 1) \cdot 2p_2p_3 \ldots p_t - 2, 2p_2^2p_3 \ldots p_t)) \cup$$

$$\cup ((1 \cdot 2p_2^2p_3 \ldots p_t - 2, 2p_2^3p_3 \ldots p_t) \cup (2 \cdot 2p_2^2p_3 \ldots p_t - 2, 2p_2^3p_3 \ldots p_t) \cup$$

$$\cup \ldots \cup ((p_2 - 1) \cdot 2p_2^2p_3 \ldots p_t - 2, 2p_2^3p_3 \ldots p_t)) \cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup ((1 \cdot 2p_2^{a_2-1}p_3 \ldots p_t - 2, 2p_2^{a_2}p_3 \ldots p_t) \cup$$

$$\cup (2 \cdot 2p_2^{a_2-1}p_3 \ldots p_t - 2, 2p_2^{a_2}p_3 \ldots p_t) \cup$$

$$\cup \ldots \cup ((p_2 - 1) \cdot 2p_2^{a_2-1}p_3 \ldots p_t - 2, 2p_2^{a_2}p_3 \ldots p_t)) \cup$$

$$\cup ((1 \cdot 2p_2^{a_2}p_3 \ldots p_t - 2, 2p_2^{a_2}p_3^2p_4 \ldots p_t) \cup$$

$$\cup (2 \cdot 2p_2^{a_2}p_3 \ldots p_t - 2, 2p_2^{a_2}p_3^2p_4 \ldots p_t) \cup$$

$$\cup \ldots \cup ((p_3 - 1) \cdot 2p_2^{a_2}p_3 \ldots p_t - 2, 2p_2^{a_2}p_3^2p_4 \ldots p_t)) \cup$$

$$\cup ((1 \cdot 2p_2^{a_2}p_3^2p_4 \ldots p_t - 2, 2p_2^{a_2}p_3^3p_4 \ldots p_t) \cup$$

$$\cup (2 \cdot 2p_2^{a_2}p_3^2p_4 \ldots p_t - 2, 2p_2^{a_2}p_3^3p_4 \ldots p_t) \cup$$

$$\cup \ldots \cup ((p_3 - 1) \cdot 2p_2^{a_2}p_3^2p_4 \ldots p_t - 2, 2p_2^{a_2}p_3^3p_4 \ldots p_t)) \cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup ((1 \cdot 2p_2^{a_2}p_3^{a_3-1}p_4 \ldots p_t - 2, 2p_2^{a_2}p_3^{a_3}p_4 \ldots p_t) \cup$$

$$\cup (2 \cdot 2p_2^{a_2}p_3^{a_3-1}p_4 \ldots p_t - 2, 2p_2^{a_2}p_3^3a_3p_4 \ldots p_t) \cup$$

$$\cup \ldots \cup ((p_3 - 1) \cdot 2p_2^{a_2}p_3^{a_3-1}p_4 \ldots p_t - 2, 2p_2^{a_2}p_3^{a_3}p_4 \ldots p_t)) \cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup ((1 \cdot 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t - 2, 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t^2) \cup$$

$$\cup (2 \cdot 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t - 2, 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t^2) \cup$$

$$\cup \ldots \cup ((p_t - 1) \cdot 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t - 2, 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t^2)) \cup$$

$$\cup ((1 \cdot 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t^2 - 2, 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t^3) \cup$$

$$\cup (2 \cdot 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t^2 - 2, 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t^3) \cup \ldots \cup$$

$$\cup ((p_t - 1) \cdot 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t^2 - 2, 2p_2^{a_2} \ldots p_{t-1}^{a_{t-1}}p_t^3)) \cup$$

. . . .

$$\cup((1\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$

$$\cup(2\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$

$$\cup\ldots\cup((p_t-1)\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^{a_t}))$$

накрывает все четные числа, сравнимые с -2 по модулям $p_2,\ldots,p_t$, но не сравнимые с -2 по модулю $2p_2^{a_2}\dots p_t^{a_t}$. Серия

$$((1\cdot 2p_2p_3\dots p_t,2p_2^2p_3\dots p_t)\cup(2\cdot 2p_2p_3\dots p_t,2p_2^2p_3\dots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot 2p_2p_3\dots p_t,2p_2^2p_3\dots p_t))\cup$$

$$\cup((1\cdot 2p_2^2p_3\dots p_t,2p_2^3p_3\dots p_t)\cup(2\cdot 2p_2^2p_3\dots p_t,2p_2^3p_3\dots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot 2p_2^2p_3\dots p_t,2p_2^3p_3\dots p_t))\cup$$

. . . .

$$\cup((1\cdot 2p_2^{a_2-1}p_3\dots p_t,2p_2^{a_2}p_3\dots p_t)\cup$$

$$\cup(2\cdot 2p_2^{a_2-1}p_3\dots p_t,2p_2^{a_2}p_3\dots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot 2p_2^{a_2-1}p_3\dots p_t,2p_2^{a_2}p_3\dots p_t))\cup$$

$$\cup((1\cdot 2p_2^{a_2}p_3\dots p_t,2p_2^{a_2}p_3^2p_4\dots p_t)\cup$$

$$\cup(2\cdot 2p_2^{a_2}p_3\dots p_t,2p_2^{a_2}p_3^2p_4\dots p_t)\cup$$

$$\cup\ldots\cup((p_3-1)\cdot 2p_2^{a_2}p_3\dots p_t,2p_2^{a_2}p_3^2p_4\dots p_t))\cup$$

$$\cup((1\cdot 2p_2^{a_2}p_3^2p_4\dots p_t,2p_2^{a_2}p_3^3p_4\dots p_t)\cup$$

$$\cup(2\cdot 2p_2^{a_2}p_3^2p_4\dots p_t,2p_2^{a_2}p_3^3p_4\dots p_t)\cup$$

$$\cup\ldots\cup((p_3-1)\cdot 2p_2^{a_2}p_3^2p_4\dots p_t,2p_2^{a_2}p_3^3p_4\dots p_t))\cup$$

. . . .

$$\cup((1\cdot 2p_2^{a_2}p_3^{a_3-1}p_4\dots p_t,2p_2^{a_2}p_3^{a_3}p_4\dots p_t)\cup$$

$$\cup(2\cdot 2p_2^{a_2}p_3^{a_3-1}p_4\dots p_t,2p_2^{a_2}p_3^3a_3p_4\dots p_t)\cup$$

$$\cup\ldots\cup((p_3-1)\cdot 2p_2^{a_2}p_3^{a_3-1}p_4\dots p_t,2p_2^{a_2}p_3^{a_3}p_4\dots p_t))\cup$$

. . . .

$$\cup((1\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t,2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^2)\cup$$

$$\cup(2\cdot 2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t,2p_2^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^2)\cup$$

$$\cup\ldots\cup((p_t-1)\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t, 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2))\cup$$
$$\cup((1\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2, 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup(2\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2, 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup\ldots\cup((p_t-1)\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2, 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3))\cup$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\cup((1\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup(2\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup\ldots\cup((p_t-1)\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t}))$$

накрывает все четные числа, сравнимые с 0 по модулям $2p_2,\ldots,2p_t$, но не сравнимые с 0 по модулю $2p_2^{a_2}\ldots p_t^{a_t}$. Наконец, серия

$$(2a_1, 2p_2p_t)\cup(2a_2, 2p_2p_3)\cup\ldots\cup(2a_{t-1}, 2p_{t-1}p_t)$$

накрывает все четные числа, сравнимые с 0 или -2 по модулям $p_2,\ldots,p_t$, но не сравнимые с 0 или -2 по модулю $2p_2\ldots p_t$. Поэтому

$$L(n)\leqslant 1+\sum_{i=2}^{t}(p_i-2)+2\sum_{i=2}^{t}(a_i-1)(p_i-1)+(t-1)=$$
$$=(2a_2-1)(p_2-1)+\ldots+(2a_t-1)(p_t-1)+1.$$

Для доказательства нижней оценки введем обозначения

$$X_1:=\{p_2^{a_2}\ldots p_t^{a_t}\},$$
$$X_2^{2,1}:=\{1\cdot 2p_2p_3^{a_3}\ldots p_t^{a_t}-2, 2\cdot 2p_2p_3^{a_3}\ldots p_t^{a_t}-2,\ldots,(p_2-1)\cdot 2p_2p_3^{a_3}\ldots p_t^{a_t}-2\},$$
$$X_2^{2,2}:=\{1\cdot 2p_2^2p_3^{a_3}\ldots p_t^{a_t}-2, 2\cdot 2p_2^2p_3^{a_3}\ldots p_t^{a_t}-2,\ldots,(p_2-1)\cdot 2p_2^2p_3^{a_3}\ldots p_t^{a_t}-2\},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$X_2^{2,a_2-1}:=\{1\cdot 2p_2^{a_2-1}p_3^{a_3}\ldots p_t^{a_t}-2,\ldots,(p_2-1)\cdot 2p_2^{a_2-1}p_3^{a_3}\ldots p_t^{a_t}-2\},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$X_2^{t,1}:=\{1\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t-2,\ldots,(p_t-1)\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t-2\},$$
$$X_2^{t,2}:=\{1\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2-2,\ldots,(p_t-1)\cdot 2p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2-2\},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$X_2^{t,a_t-1} := \{1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_{t-1}-1} - 2, \dots, (p_t-1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2\},$$

$$X_3^{2,1} := \{1 \cdot 2p_2 p_3^{a_3} \dots p_t^{a_t}, 2 \cdot 2p_2 p_3^{a_3} \dots p_t^{a_t}, \dots, (p_2-1) \cdot 2p_2 p_3^{a_3} \dots p_t^{a_t}\},$$

$$X_3^{2,2} := \{1 \cdot 2p_2^2 p_3^{a_3} \dots p_t^{a_t}, 2 \cdot 2p_2^2 p_3^{a_3} \dots p_t^{a_t}, \dots, (p_2-1) \cdot 2p_2^2 p_3^{a_3} \dots p_t^{a_t}\},$$

. . . .

$$X_3^{2,a_2-1} := \{1 \cdot 2p_2^{a_2-1} p_3^{a_3} \dots p_t^{a_t}, \dots, (p_2-1) \cdot 2p_2^{a_2-1} p_3^{a_3} \dots p_t^{a_t}\},$$

. . . .

$$X_3^{t,1} := \{1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, \dots, (p_t-1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t\},$$

$$X_3^{t,2} := \{1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, \dots, (p_t-1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2\},$$

. . . .

$$X_3^{t,a_t-1} := \{1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_{t-1}-1}, \dots, (p_t-1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}\},$$

$$X_4^2 := \{2b_{2,1}, \dots, 2b_{2,p_2-2}\},$$

. . . .

$$X_4^t := \{2b_{t,1}, \dots, 2b_{t,p_t-2}\},$$

$$X_5 := \{2c_2, \dots, 2c_{t-1}, 2c_t\},$$

$$Y := (2p_2^{a_2} \dots p_t^{a_t} - 2, 2p_2^{a_2} \dots p_t^{a_t}) \cup (2p_2^{a_2} \dots p_t^{a_t}, 2p_2^{a_2} \dots p_t^{a_t}),$$

где

$$b_{i,j} \equiv j \mod p_i^{a_i}, \quad b_{i,j} \equiv 0 \mod \frac{n}{2p_i^{a_i}},$$

$$c_i \equiv -1 \mod p_i^{a_i}, \quad c_i \equiv 0 \mod \frac{n}{2p_i^{a_i}}.$$

Покажем, что множество

$$X := X_1 \cup X_2^{2,1} \cup \dots \cup X_2^{t,a_t-1} \cup$$

$$\cup X_3^{2,1} \cup \dots \cup X_3^{t,a_t-1} \cup X_4^2 \cup \dots \cup X_4^t \cup X_5$$

будет опорным семейством для множества Y. Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (n-2, n) \neq \emptyset, \tag{7}$$

$$(x_1, x_2 - x_1) \cap (n, n) \neq \emptyset. \tag{8}$$

Возможны случаи:
Случай 1.
$x_1 \in X_1, x_2 \in X_2^{i,j}$ или $x_2 \in X_1, x_1 \in X_2^{i,j}$. Тогда НОД$(x_2 - x_1, n) = 1$ и значит по лемме 1 верно (7).
Случай 2.
$x_1 \in X_1, x_2 \in X_3^{i,j}$ или $x_2 \in X_1, x_1 \in X_3^{i,j}$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{2p_i^{a_i}} p_i^j$ и по лемме 1 верно (8).
Случай 3.
$x_1 \in X_1, x_2 \in X_4^i$ или $x_2 \in X_1, x_1 \in X_4^i$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{2p_i^{a_i}}$ и по лемме 1 верно (8).
Случай 4.
$x_1 \in X_1, x_2 = c_i$ или $x_2 \in X_1, x_1 = c_i$. Случай аналогичен предыдущему.
Случай 5.
$x_1 \in X_2^{i,j_1}, x_2 \in X_2^{i,j_2}$, $j_1 \leqslant j_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_1}$ и по лемме 1 верно (7).
Случай 6.
$x_1 \in X_2^{i,j_1}, x_2 \in X_2^{i,j_2}$, $j_1 > j_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_2}$ и по лемме 1 верно (7).
Случай 7.
$x_1 \in X_2^{i_1,j_1}, x_2 \in X_2^{i_2,j_2}$, $i_1 \neq i_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_{i_1}^{a_{i_1}} p_{i_2}^{a_{i_2}}} p_{i_1}^{j_1} p_{i_2}^{j_2}$ и по лемме 1 верно (7).
Случай 8.
$x_1 \in X_2^{i_1,j_1}, x_2 \in X_3^{i_2,j_2}$ или $x_2 \in X_2^{i_1,j_1}, x_1 \in X_3^{i_2,j_2}$. Тогда верно, что НОД$(x_2 - x_1, n) = 2$ и значит по лемме 1 получаем (7).
Случай 9.
$x_1 \in X_2^{i,j}, x_2 \in X_4^k$ или $x_2 \in X_2^{i,j}, x_1 \in X_4^k$. Случай аналогичен предыдущему.
Случай 10.
$x_1 \in X_2^{i,j}, x_2 = c_i$ или $x_2 \in X_2^{i,j}, x_1 = c_i$. Тогда НОД$(x_2 - x_1, n) = 2p_i^j$ и по лемме 1 верно (7).
Случай 11.
$x_1 \in X_2^{i_1,j}, x_2 = c_{i_2}$, $i_1 \neq i_2$ или $x_2 \in X_2^{i_1,j}, x_1 = c_{i_2}$, $i_1 \neq i_2$. Тогда НОД$(x_2 - x_1, n) = 2p_{i_2}^{a_{i_2}}$ и по лемме 1 верно (7).
Случай 12.
$x_1 \in X_3^{i,j_1}, x_2 \in X_3^{i,j_2}$, $j_1 \leqslant j_2$. Случай аналогичен случаю 5.
Случай 13.
$x_1 \in X_3^{i,j_1}, x_2 \in X_3^{i,j_2}$, $j_1 > j_2$. Случай аналогичен случаю 6.

Случай 14.
$x_1 \in X_3^{i_1,j_1}, x_2 \in X_3^{i_2,j_2}$, $i_1 \neq i_2$. Случай аналогичен случаю 7.
Случай 15.
$x_1 \in X_3^{i,j}, x_2 \in X_4^i$ или $x_2 \in X_3^{i,j}, x_1 \in X_4^i$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}}$ и по лемме 1 верно (8).
Случай 16.
$x_1 \in X_3^{i,j}, x_2 \in X_4^k$, $i \neq k$ или $x_2 \in X_3^{i,j}, x_1 \in X_4^i$, $i \neq k$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_k^{a_k}} p_i^j$ и по лемме 1 верно (8).
Случай 17.
$x_1 \in X_3^{i,j}, x_2 = c_i$ или $x_2 \in X_2^{i,j}, x_1 = c_i$. Случай аналогичен случаю 15.
Случай 18.
$x_1 \in X_3^{i,j}, x_2 = c_k$, $i \neq k$ или $x_2 \in X_3^{i,j}, x_1 = c_k$, $i \neq k$. Случай аналогичен случаю 16.
Случай 19.
$x_1 \in X_4^i, x_2 \in X_4^i$. Случай аналогичен случаю 15.
Случай 20.
$x_1 \in X_4^i, x_2 \in X_4^j$, $i \neq j$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_j^{a_j}}$ и по лемме 1 верно (8).
Случай 21.
$x_1 \in X_4^i, x_2 = c_i$ или $x_1 \in X_4^i, x_2 = c_i$. Случай аналогичен случаю 15.
Случай 22.
$x_1 \in X_4^i, x_2 = c_j$, $i \neq j$ или $x_2 \in X_4^i, x_1 = c_j$, $i \neq j$. Случай аналогичен случаю 20.
Случай 23.
$x_1 = c_i, x_2 = c_j$. Случай аналогичен случаю 20.
Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y. Но в множестве X всего

$$|X_1|+|X_2^{2,1}|+\ldots+|X_2^{t,a_t-1}|+|X_3^{2,1}|+\ldots+|X_3^{t,a_t-1}|+|X_4^2|+\ldots+|X_4^t|+|X_5| =$$

$$= 1+2(p_2-1)(a_2-1)+\ldots+2(p_t-1)(a_t-1)+(p_2-2)+\ldots+(p_t-2)+(t-1) =$$

$$= (2a_2-1)(p_2-1)+\ldots+(2a_t-1)(p_t-1)+1.$$

элементов. Поэтому по лемме 2 получаем

$$L(2p_2^{a_2}\ldots p_t^{a_t}) \geqslant (2a_2-1)(p_2-1)+\ldots+(2a_t-1)(p_t-1)+1.$$

В случае, когда $p_1 = 2, t > 2, a_1 = 1$, утверждение теоремы доказано.

Пусть $p_1 = 2, t > 2, a_1 > 1$. Докажем тогда, что

$$L(n) = L(2^{a_1} p_2^{a_2} \dots p_t^{a_t}) = (2a_2-1)(p_2-1)+\dots+(2a_t-1)(p_t-1)+(2a_1-2).$$

Для доказательства верхней оценки нужно представить $T(n)$ в виде объединения

$$(2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + (2a_1 - 2)$$

арифметических прогрессий. Это можно сделать следующим образом:

$$T(n) = (1, 2) \cup ((2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \dots \cup (2p_2 - 4, 2p_2))\cup$$
$$\cup((2, 2p_3) \cup (4, 2p_3) \cup (6, 2p_3) \cup \dots \cup (2p_3 - 4, 2p_3)) \cup \dots \cup$$
$$\cup((2, 2p_t) \cup (4, 2p_t) \cup (6, 2p_t) \cup \dots \cup (2p_t - 4, 2p_t))\cup$$
$$\cup((4p_2 \dots p_t - 2, 8p_2 \dots p_t) \cup (8p_2 \dots p_t - 2, 16p_2 \dots p_t)\cup$$
$$\cup \dots \cup (2^{a_1-1}p_2 \dots p_t - 2, 2^{a_1}p_2 \dots p_t))\cup$$
$$\cup((1 \cdot 2^{a_1}p_2p_3 \dots p_t - 2, 2^{a_1}p_2^2p_3 \dots p_t)\cup$$
$$\cup(2 \cdot 2^{a_1}p_2p_3 \dots p_t - 2, 2^{a_1}p_2^2p_3 \dots p_t)\cup$$
$$\cup \dots \cup ((p_2 - 1) \cdot 2^{a_1}p_2p_3 \dots p_t - 2, 2^{a_1}p_2^2p_3 \dots p_t))\cup$$
$$\cup((1 \cdot 2^{a_1}p_2^2p_3 \dots p_t - 2, 2p_2^3p_3 \dots p_t)\cup$$
$$\cup(2 \cdot 2^{a_1}p_2^2p_3 \dots p_t - 2, 2^{a_1}p_2^3p_3 \dots p_t)\cup$$
$$\cup \dots \cup ((p_2 - 1) \cdot 2^{a_1}p_2^2p_3 \dots p_t - 2, 2^{a_1}p_2^3p_3 \dots p_t))\cup$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\cup((1 \cdot 2^{a_1}p_2^{a_2-1}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3 \dots p_t)\cup$$
$$\cup(2 \cdot 2^{a_1}p_2^{a_2-1}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3 \dots p_t)\cup$$
$$\cup \dots \cup ((p_2 - 1) \cdot 2^{a_1}p_2^{a_2-1}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3 \dots p_t))\cup$$
$$\cup((1 \cdot 2^{a_1}p_2^{a_2}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3^2p_4 \dots p_t)\cup$$
$$\cup(2 \cdot 2^{a_1}p_2^{a_2}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3^2p_4 \dots p_t)\cup$$
$$\cup \dots \cup ((p_3 - 1) \cdot 2^{a_1}p_2^{a_2}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3^2p_4 \dots p_t))\cup$$
$$\cup((1 \cdot 2^{a_1}p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3^3p_4 \dots p_t)\cup$$
$$\cup(2 \cdot 2^{a_1}p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3^3p_4 \dots p_t)\cup$$

$$\cup\ldots\cup((p_3-1)\cdot 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t-2,2^{a_1}p_2^{a_2}p_3^3p_4\ldots p_t))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t-2,2^{a_1}p_2^{a_2}p_3^{a_3}p_4\ldots p_t)\cup$$

$$\cup(2\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t-2,2^{a_1}p_2^{a_2}p_3^3a_3p_4\ldots p_t)\cup$$

$$\cup\ldots\cup((p_3-1)\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t-2,2^{a_1}p_2^{a_2}p_3^{a_3}p_4\ldots p_t))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t-2,2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$

$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t-2,2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$

$$\cup\ldots\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t-2,2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2))\cup$$

$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2-2,2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$

$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2-2,2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$

$$\cup\ldots\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2-2,2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$

$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup\ldots\cup$$

$$\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t}))\cup$$

$$\cup((4p_2\ldots p_t,8p_2\ldots p_t)\cup(8p_2\ldots p_t,16p_2\ldots p_t)\cup\ldots\cup$$

$$\cup(2^{a_1-1}p_2\ldots p_t,2^{a_1}p_2\ldots p_t))\cup$$

$$\cup((1\cdot 2^{a_1}p_2p_3\ldots p_t,2^{a_1}p_2^2p_3\ldots p_t)\cup$$

$$\cup(2\cdot 2^{a_1}p_2p_3\ldots p_t,2^{a_1}p_2^2p_3\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot 2^{a_1}p_2p_3\ldots p_t,2^{a_1}p_2^2p_3\ldots p_t))\cup$$

$$\cup((1\cdot 2^{a_1}p_2^2p_3\ldots p_t,2p_2^3p_3\ldots p_t)\cup$$

$$\cup(2\cdot 2^{a_1}p_2^2p_3\ldots p_t,2^{a_1}p_2^3p_3\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot 2^{a_1}p_2^2p_3\ldots p_t,2^{a_1}p_2^3p_3\ldots p_t))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2^{a_1}p_2^{a_2-1}p_3\ldots p_t,2^{a_1}p_2^{a_2}p_3\ldots p_t)\cup$$

$$\cup(2\cdot 2^{a_1}p_2^{a_2-1}p_3\ldots p_t,2^{a_1}p_2^{a_2}p_3\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot 2^{a_1}p_2^{a_2-1}p_3\ldots p_t, 2^{a_1}p_2^{a_2}p_3\ldots p_t))\cup$$
$$\cup((1\cdot 2^{a_1}p_2^{a_2}p_3\ldots p_t, 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t)\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}p_3\ldots p_t, 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t)\cup$$
$$\cup\ldots\cup((p_3-1)\cdot 2^{a_1}p_2^{a_2}p_3\ldots p_t, 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t))\cup$$
$$\cup((1\cdot 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^3p_4\ldots p_t)\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^3p_4\ldots p_t)\cup$$
$$\cup\ldots\cup((p_3-1)\cdot 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^3p_4\ldots p_t))\cup$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\cup((1\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^{a_3}p_4\ldots p_t)\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^3a_3p_4\ldots p_t)\cup$$
$$\cup\ldots\cup((p_3-1)\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^{a_3}p_4\ldots p_t))\cup$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$
$$\cup\ldots\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2))\cup$$
$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup\ldots\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3))\cup$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup\ldots\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t}))\cup$$
$$\cup((2a_1, 4p_2)\cup(2a_2, 2p_2p_3)\ldots\cup(2a_{t-1}, 2p_{t-1}p_t)\cup(2a_t, 4p_t)),$$

где при $1\leqslant i\leqslant t-1$ имеем

$$1\leqslant a_i\leqslant p_ip_{i+1},\quad a_i\equiv 0 \mod p_i,\quad a_i\equiv -1 \mod p_{i+1}$$

и при $i = t$ имеем

$$1 \leqslant a_t \leqslant 2p_t, \quad a_t \equiv 0 \mod p_t, \quad a_t \equiv -1 \mod 2.$$

Здесь серия

$$((2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \ldots \cup (2p_2 - 4, 2p_2)) \cup$$

$$\cup((2, 2p_3) \cup (4, 2p_3) \cup (6, 2p_3) \cup \ldots \cup$$

$$\cup(2p_3 - 4, 2p_3)) \cup \ldots \cup ((2, 2p_t) \cup (4, 2p_t) \cup (6, 2p_t) \cup \ldots \cup (2p_t - 4, 2p_t))$$

накрывает все четные числа, не сравнимые с 0 и -2 по модулям $p_2, \ldots, p_t$. Серия

$$((4p_2 \ldots p_t - 2, 8p_2 \ldots p_t) \cup (8p_2 \ldots p_t - 2, 16p_2 \ldots p_t) \cup$$

$$\cup \ldots \cup (2^{a_1 - 1} p_2 \ldots p_t - 2, 2^{a_1} p_2 \ldots p_t)) \cup$$

$$\cup((1 \cdot 2^{a_1} p_2 p_3 \ldots p_t - 2, 2^{a_1} p_2^2 p_3 \ldots p_t) \cup$$

$$\cup(2 \cdot 2^{a_1} p_2 p_3 \ldots p_t - 2, 2^{a_1} p_2^2 p_3 \ldots p_t) \cup$$

$$\cup \ldots \cup ((p_2 - 1) \cdot 2^{a_1} p_2 p_3 \ldots p_t - 2, 2^{a_1} p_2^2 p_3 \ldots p_t)) \cup$$

$$\cup((1 \cdot 2^{a_1} p_2^2 p_3 \ldots p_t - 2, 2p_2^3 p_3 \ldots p_t) \cup$$

$$\cup(2 \cdot 2^{a_1} p_2^2 p_3 \ldots p_t - 2, 2^{a_1} p_2^3 p_3 \ldots p_t) \cup$$

$$\cup \ldots \cup ((p_2 - 1) \cdot 2^{a_1} p_2^2 p_3 \ldots p_t - 2, 2^{a_1} p_2^3 p_3 \ldots p_t)) \cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1 \cdot 2^{a_1} p_2^{a_2 - 1} p_3 \ldots p_t - 2, 2^{a_1} p_2^{a_2} p_3 \ldots p_t) \cup$$

$$\cup(2 \cdot 2^{a_1} p_2^{a_2 - 1} p_3 \ldots p_t - 2, 2^{a_1} p_2^{a_2} p_3 \ldots p_t) \cup$$

$$\cup \ldots \cup ((p_2 - 1) \cdot 2^{a_1} p_2^{a_2 - 1} p_3 \ldots p_t - 2, 2^{a_1} p_2^{a_2} p_3 \ldots p_t)) \cup$$

$$\cup((1 \cdot 2^{a_1} p_2^{a_2} p_3 \ldots p_t - 2, 2^{a_1} p_2^{a_2} p_3^2 p_4 \ldots p_t) \cup$$

$$\cup(2 \cdot 2^{a_1} p_2^{a_2} p_3 \ldots p_t - 2, 2^{a_1} p_2^{a_2} p_3^2 p_4 \ldots p_t) \cup$$

$$\cup \ldots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3 \ldots p_t - 2, 2^{a_1} p_2^{a_2} p_3^2 p_4 \ldots p_t)) \cup$$

$$\cup((1 \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \ldots p_t - 2, 2^{a_1} p_2^{a_2} p_3^3 p_4 \ldots p_t) \cup$$

$$\cup(2 \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \ldots p_t - 2, 2^{a_1} p_2^{a_2} p_3^3 p_4 \ldots p_t) \cup$$

$$\cup \ldots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \ldots p_t - 2, 2^{a_1} p_2^{a_2} p_3^3 p_4 \ldots p_t)) \cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t-2, 2^{a_1}p_2^{a_2}p_3^{a_3}p_4\ldots p_t)\cup$$

$$\cup(2\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t-2, 2^{a_1}p_2^{a_2}p_3^{3}a_3p_4\ldots p_t)\cup$$

$$\cup\ldots\cup((p_3-1)\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t-2, 2^{a_1}p_2^{a_2}p_3^{a_3}p_4\ldots p_t))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t-2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$

$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t-2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$

$$\cup\ldots\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t-2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2))\cup$$

$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2-2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$

$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2-2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup\ldots\cup$$

$$\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2-2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$

$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$

$$\cup\ldots\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t}))$$

накрывает все четные числа, сравнимые с -2 по модулям $4, p_2, \ldots, p_t$, но не сравнимые с -2 по модулю $2^{a_1}p_2^{a_2}\ldots p_t^{a_t}$. Серия

$$((4p_2\ldots p_t, 8p_2\ldots p_t)\cup(8p_2\ldots p_t, 16p_2\ldots p_t)\cup$$

$$\cup\ldots\cup(2^{a_1-1}p_2\ldots p_t, 2^{a_1}p_2\ldots p_t))\cup$$

$$\cup((1\cdot 2^{a_1}p_2p_3\ldots p_t, 2^{a_1}p_2^2p_3\ldots p_t)\cup(2\cdot 2^{a_1}p_2p_3\ldots p_t, 2^{a_1}p_2^2p_3\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot 2^{a_1}p_2p_3\ldots p_t, 2^{a_1}p_2^2p_3\ldots p_t))\cup$$

$$\cup((1\cdot 2^{a_1}p_2^2p_3\ldots p_t, 2p_2^3p_3\ldots p_t)\cup(2\cdot 2^{a_1}p_2^2p_3\ldots p_t, 2^{a_1}p_2^3p_3\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot 2^{a_1}p_2^2p_3\ldots p_t, 2^{a_1}p_2^3p_3\ldots p_t))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot 2^{a_1}p_2^{a_2-1}p_3\ldots p_t, 2^{a_1}p_2^{a_2}p_3\ldots p_t)\cup$$

$$\cup(2\cdot 2^{a_1}p_2^{a_2-1}p_3\ldots p_t, 2^{a_1}p_2^{a_2}p_3\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot 2^{a_1}p_2^{a_2-1}p_3\ldots p_t, 2^{a_1}p_2^{a_2}p_3\ldots p_t))\cup$$

$$\cup((1\cdot 2^{a_1}p_2^{a_2}p_3\ldots p_t, 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t)\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}p_3\ldots p_t, 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t)\cup$$
$$\cup\ldots\cup((p_3-1)\cdot 2^{a_1}p_2^{a_2}p_3\ldots p_t, 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t))\cup$$
$$\cup((1\cdot 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^3p_4\ldots p_t)\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^3p_4\ldots p_t)\cup$$
$$\cup\ldots\cup((p_3-1)\cdot 2^{a_1}p_2^{a_2}p_3^2p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^3p_4\ldots p_t))\cup$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\cup((1\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^{a_3}p_4\ldots p_t)\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^3a_3p_4\ldots p_t)\cup$$
$$\cup\ldots\cup((p_3-1)\cdot 2^{a_1}p_2^{a_2}p_3^{a_3-1}p_4\ldots p_t, 2^{a_1}p_2^{a_2}p_3^{a_3}p_4\ldots p_t))\cup$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$
$$\cup\ldots\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2))\cup$$
$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup\ldots\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^2, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^3))\cup$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\cup((1\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup(2\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup\ldots\cup((p_t-1)\cdot 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, 2^{a_1}p_2^{a_2}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t}))$$

накрывает все четные числа, сравнимые с 0 по модулям $4, p_2, \ldots, p_t$, но не сравнимые с 0 по модулю $2^{a_1}p_2^{a_2}\ldots p_t^{a_t}$. Наконец, серия

$$(2a_1, 4p_2)\cup(2a_2, 2p_2p_3)\ldots\cup(2a_{t-1}, 2p_{t-1}p_t)\cup(2a_t, 4p_t)$$

накрывает все четные числа, сравнимые с 0 или -2 по модулям $4, p_2, \ldots, p_t$, но не сравнимые с 0 или -2 по модулю $4p_2\ldots p_t$. Поэтому

$$L(n)\leqslant 1+\sum_{i=2}^{t}(p_i-2)+2(a_1-2)+2\sum_{i=2}^{t}(a_i-1)(p_i-1)+t=$$

$$= (2a_2 - 1)(p_2 - 1) + \ldots + (2a_t - 1)(p_t - 1) + (2a_1 - 2).$$

Для доказательства нижней оценки введем обозначения

$$X_1 := \{p_2^{a_2} \ldots p_t^{a_t}\},$$

$$X_2^2 := \{2^2 p_2^{a_2} \ldots p_t^{a_t} - 2\}, \ldots, X_2^{a_1-1} := \{2^{a_1-1} p_2^{a_2} \ldots p_t^{a_t} - 2\},$$

$$X_3^2 := \{2^2 p_2^{a_2} \ldots p_t^{a_t}\}, \ldots, X_3^{a_1-1} := \{2^{a_1-1} p_2^{a_2} \ldots p_t^{a_t}\},$$

$$X_4^{2,1} := \{1 \cdot 2^{a_1} p_2 p_3^{a_3} \ldots p_t^{a_t} - 2, \ldots, (p_2 - 1) \cdot 2^{a_1} p_2 p_3^{a_3} \ldots p_t^{a_t} - 2\},$$

$$X_4^{2,2} := \{1 \cdot 2^{a_1} p_2^2 p_3^{a_3} \ldots p_t^{a_t} - 2, \ldots, (p_2 - 1) \cdot 2^{a_1} p_2^2 p_3^{a_3} \ldots p_t^{a_t} - 2\},$$

. . . . . .

$$X_4^{2,a_2-1} := \{1 \cdot 2^{a_1} p_2^{a_2-1} p_3^{a_3} \ldots p_t^{a_t} - 2, \ldots, (p_2 - 1) \cdot 2^{a_1} p_2^{a_2-1} p_3^{a_3} \ldots p_t^{a_t} - 2\},$$

. . . . . .

$$X_3^{t,1} := \{1 \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t - 2, \ldots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t - 2\},$$

$$X_4^{t,2} := \{1 \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t^2 - 2, \ldots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t^2 - 2\},$$

. . . . . .

$$X_4^{t,a_t-1} := \{1 \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, \ldots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2\},$$

$$X_5^{2,1} := \{1 \cdot 2^{a_1} p_2 p_3^{a_3} \ldots p_t^{a_t}, \ldots, (p_2 - 1) \cdot 2^{a_1} p_2 p_3^{a_3} \ldots p_t^{a_t}\},$$

$$X_5^{2,2} := \{1 \cdot 2^{a_1} p_2^2 p_3^{a_3} \ldots p_t^{a_t}, \ldots, (p_2 - 1) \cdot 2^{a_1} p_2^2 p_3^{a_3} \ldots p_t^{a_t}\},$$

. . . . . .

$$X_5^{2,a_2-1} := \{1 \cdot 2 p_2^{a_2-1} p_3^{a_3} \ldots p_t^{a_t}, \ldots, (p_2 - 1) \cdot 2^{a_1} p_2^{a_2-1} p_3^{a_3} \ldots p_t^{a_t}\},$$

. . . . . .

$$X_5^{t,1} := \{1 \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t, \ldots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t\},$$

$$X_5^{t,2} := \{1 \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t^2, \ldots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t^2\},$$

. . . . . .

$$X_5^{t,a_t-1} := \{1 \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, \ldots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \ldots p_{t-1}^{a_{t-1}} p_t^{a_t-1}\},$$

$$X_6^2 := \{2b_{2,1}, \ldots, 2b_{2,p_2-2}\},$$

. . . . . .

$$X_6^t := \{2b_{t,1}, \ldots, 2b_{t,p_t-2}\},$$

$$X_7 := \{2c_1, \ldots, 2c_{t-1}, 2c_t\},$$

$$Y := (2p_2^{a_2} \ldots p_t^{a_t} - 2, 2p_2^{a_2} \ldots p_t^{a_t}) \cup (2p_2^{a_2} \ldots p_t^{a_t}, 2p_2^{a_2} \ldots p_t^{a_t}),$$

где

$$b_{i,j} \equiv j \mod p_i^{a_i}, \quad b_{i,j} \equiv 0 \mod \frac{n}{2p_i^{a_i}},$$

$$c_1 \equiv -1 \mod 2^{a_1-1}, \quad c_1 \equiv 0 \mod \frac{n}{2^{a_1}}$$

и при $2 \leqslant i \leqslant t$ верно

$$c_i \equiv -1 \mod p_i^{a_i}, \quad c_i \equiv 0 \mod \frac{n}{2p_i^{a_i}}.$$

Покажем, что множество

$$X := X_1 \cup X_2^2 \cup \ldots \cup X_2^{a_1-1} \cup X_3^2 \cup \ldots \cup X_3^{a_1-1} \cup X_4^{2,1} \cup$$

$$\cup \ldots \cup X_4^{t,a_t-1} \cup X_5^{2,1} \cup \ldots \cup X_5^{t,a_t-1} \cup X_6^2 \cup \ldots \cup X_6^t \cup X_7$$

будет опорным семейством для множества Y. Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (n-2, n) \neq \emptyset, \tag{9}$$

$$(x_1, x_2 - x_1) \cap (n, n) \neq \emptyset. \tag{10}$$

Возможны случаи:

Случай 1.

$x_1 \in X_1, x_2 \in X_2^i$ или $x_2 \in X_1, x_1 \in X_2^i$. Тогда НОД$(x_2 - x_1, n) = 2$ и значит по лемме 1 верно (9).

Случай 2.

$x_1 \in X_1, x_2 \in X_3^i$ или $x_2 \in X_1, x_1 \in X_3^i$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{2^{a_1}}$ и по лемме 1 верно (10).

Случай 3.

$x_1 \in X_1, x_2 \in X_4^{i,j}$ или $x_2 \in X_1, x_1 \in X_4^{i,j}$. Тогда НОД$(x_2 - x_1, n) = 1$ и по лемме 1 верно (9).

Случай 4.

$x_1 \in X_1, x_2 \in X_5^{i,j}$ или $x_2 \in X_1, x_1 \in X_5^{i,j}$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{2^{a_1} p_i^{a_i}} p_i^j$ и по лемме 1 верно (10).

Случай 5.

$x_1 \in X_1, x_2 \in X_6^i$ или $x_2 \in X_1, x_1 \in X_6^i$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}}$ и по

лемме 1 верно (10).

Случай 6.

$x_1 \in X_1, x_2 = c_1$ или $x_2 \in X_1, x_1 = c_1$. Случай аналогичен случаю 2.

Случай 7.

$x_1 \in X_1, x_2 = c_i$, $i > 1$ или $x_2 \in X_1, x_1 = c_i$, $i > 1$. Тогда верно, что НОД$(x_2 - x_1, n) = \frac{n}{2^{a_1} p_i^{a_i}}$ и значит по лемме 1 получаем (10).

Случай 8.

$x_1 \in X_2^i, x_2 \in X_2^j$, $i < j$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{2^{a_1}} 2^i$ и по лемме 1 верно (9).

Случай 9.

$x_1 \in X_2^i, x_2 \in X_2^j$, $i > j$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{2^{a_1}} 2^j$ и по лемме 1 верно (9).

Случай 10.

$x_1 \in X_2^i, x_2 \in X_3^j$. Случай аналогичен случаю 1.

Случай 11.

$x_1 \in X_2^i, x_2 \in X_4^{j,k}$ или $x_2 \in X_2^i, x_1 \in X_4^{j,k}$. Тогда в этом случае верно, что НОД$(x_2 - x_1, n) = \frac{n}{2^{a_1} p_j^{a_j}} 2^i p_j^k$ и значит по лемме 1 получаем (9).

Случай 12.

$x_1 \in X_2^i, x_2 \in X_5^{j,k}$ или $x_2 \in X_2^i, x_1 \in X_5^{j,k}$. Случай аналогичен случаю 1.

Случай 13.

$x_1 \in X_2^i, x_2 \in X_6^j$ или $x_2 \in X_2^i, x_1 \in X_6^j$. Случай аналогичен случаю 1.

Случай 14.

$x_1 \in X_2^i, x_2 = c_1$ или $x_2 \in X_2^i, x_1 = c_1$. Тогда НОД$(x_2 - x_1, n) = 2^i$ и по лемме 1 верно (9).

Случай 15.

$x_1 \in X_2^i, x_2 = c_j$, $j > 1$ или $x_2 \in X_2^i, x_1 = c_j$, $j > 1$. Тогда верно, что НОД$(x_2 - x_1, n) = p_j^{a_j}$ и значит по лемме 1 получаем (9).

Случай 16.

$x_1 \in X_3^i, x_2 \in X_4^{j,k}$ или $x_2 \in X_3^i, x_1 \in X_4^{j,k}$. Случай аналогичен случаю 1.

Случай 17.

$x_1 \in X_3^i, x_2 \in X_5^{j,k}$ или $x_2 \in X_3^i, x_1 \in X_5^{j,k}$. Тогда в этом случае верно, что НОД$(x_2 - x_1, n) = \frac{n}{2^{a_1} p_j^{a_j}} 2^i p_j^k$ и значит по лемме 1 получаем (10).

Случай 18.

$x_1 \in X_3^i, x_2 \in X_6^j$ или $x_3 \in X_2^i, x_1 \in X_6^j$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{2^{a_1} p_j^{a_j}} 2^i$ и по лемме 1 верно (10).

Случай 19.

$x_1 \in X_3^i, x_2 = c_1$ или $x_2 \in X_3^i, x_1 = c_1$. Тогда НОД$(x_2 - x_1, n) = 2\frac{n}{2^{a_1}}$ и по

лемме 1 верно (10).

Случай 20.

$x_1 \in X_3^i, x_2 = c_j$, $j > 1$ или $x_2 \in X_3^i, x_1 = c_j$, $j > 1$. Случай аналогичен случаю 18.

Случай 21.

$x_1 \in X_4^{i,j_1}, x_2 \in X_4^{i,j_2}$, $j_1 \leqslant j_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_1}$ и по лемме 1 верно (9).

Случай 22.

$x_1 \in X_4^{i,j_1}, x_2 \in X_4^{i,j_2}$, $j_1 > j_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_2}$ и по лемме 1 верно (9).

Случай 23.

$x_1 \in X_4^{i_1,j_1}, x_2 \in X_4^{i_2,j_2}$, $i_1 \neq i_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_{i_1}^{a_{i_1}} p_{i_2}^{a_{i_2}}} p_{i_1}^{j_1} p_{i_2}^{j_2}$ и по лемме 1 верно (9).

Случай 24.

$x_1 \in X_4^{i_1,j_1}, x_2 \in X_5^{i_2,j_2}$. Случай аналогичен случаю 1.

Случай 25.

$x_1 \in X_4^{i,j}, x_2 \in X_6^k$ или $x_2 \in X_4^{i,j}, x_1 \in X_6^k$. Случай аналогичен случаю 1.

Случай 26.

$x_1 \in X_4^{i,j}, x_2 = c_1$ или $x_2 \in X_4^{i,j}, x_1 = c_1$. Тогда НОД$(x_2 - x_1, n) = 2^{a_1}$ и по лемме 1 верно (9).

Случай 27.

$x_1 \in X_4^{i,j}, x_2 = c_k$, $k > 1$ или $x_2 \in X_4^{i,j}, x_1 = c_i$, $k > 1$. Тогда верно, что НОД$(x_2 - x_1, n) = 2p_i^j$ и по лемме 1 получаем (9).

Случай 28.

$x_1 \in X_5^{i,j_1}, x_2 \in X_5^{i,j_2}$, $j_1 \leqslant j_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_1}$ и по лемме 1 верно (10).

Случай 29.

$x_1 \in X_5^{i,j_1}, x_2 \in X_5^{i,j_2}$, $j_1 > j_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_2}$ и по лемме 1 верно (10).

Случай 30.

$x_1 \in X_5^{i_1,j_1}, x_2 \in X_5^{i_2,j_2}$, $i_1 \neq i_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_{i_1}^{a_{i_1}} p_{i_2}^{a_{i_2}}} p_{i_1}^{j_1} p_{i_2}^{j_2}$ и по лемме 1 верно (10).

Случай 31.

$x_1 \in X_5^{i,j}, x_2 \in X_6^i$ или $x_2 \in X_5^{i,j}, x_1 \in X_6^i$. Случай аналогичен случаю 5.

Случай 32.

$x_1 \in X_5^{i,j}, x_2 \in X_6^k$, $i \neq k$ или $x_2 \in X_5^{i,j}, x_1 \in X_6^k$, $i \neq k$. Тогда верно, что

НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_k^{a_k}} p_i^j$ и по лемме 1 получаем (10).

Случай 33.

$x_1 \in X_5^{i,j}, x_2 = c_1$ или $x_2 \in X_5^{i,j}, x_1 = c_1$. Тогда НОД$(x_2 - x_1, n) = 2\frac{n}{2^{a_1} p_i^{a_i}} p_i^j$ и по лемме 1 верно (10).

Случай 34.

$x_1 \in X_5^{i,j}, x_2 = c_i$, или $x_2 \in X_5^{i,j}, x_1 = c_i$. Случай аналогичен случаю 5.

Случай 35.

$x_1 \in X_5^{i,j}, x_2 = c_k$, $k \neq i$ или $x_2 \in X_5^{i,j}, x_1 = c_k$, $k \neq i$. Тогда верно, что НОД$(x_2 - x_1, n) = \frac{n}{p_k^{a_k} p_i^{a_i}} p_i^j$ и по лемме 1 получаем (10).

Случай 36.

$x_1 \in X_6^i, x_2 \in X_6^i$. Случай аналогичен случаю 5.

Случай 37.

$x_1 \in X_6^i, x_2 \in X_6^j$, $i \neq j$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_j^{a_j}}$ и по лемме 1 верно (10).

Случай 38.

$x_1 \in X_6^i, x_2 = c_i$ или $x_1 \in X_6^i, x_2 = c_i$. Случай аналогичен случаю 5.

Случай 39.

$x_1 \in X_6^i, x_2 = c_1$ или $x_2 \in X_6^i, x_1 = c_1$. Тогда НОД$(x_2 - x_1, n) = 2\frac{n}{2^{a_1} p_i^{a_i}}$ и по лемме 1 верно (10).

Случай 40.

$x_1 \in X_6^i, x_2 = c_j$, $i \neq j \neq 1$ или $x_2 \in X_6^i, x_1 = c_j$, $i \neq j \neq 1$. Случай аналогичен случаю 37.

Случай 41.

$x_1 = c_1, x_2 = c_i, i > 1$ или $x_2 = c_1, x_1 = c_i, i > 1$. Случай аналогичен случаю 39.

Случай 42.

$x_1 = c_i, x_2 = c_j, i, j \neq 1$. Случай аналогичен случаю 37.

Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y. Но в множестве X всего

$$|X_1| + |X_2^2| + \ldots + |X_2^{a_1-1}| + |X_3^2| + \ldots + |X_3^{a_1-1}| +$$

$$+ |X_4^{2,1}| + \ldots + |X_4^{t,a_t-1}| + |X_5^{2,1}| +$$

$$+ \ldots + |X_5^{t,a_t-1}| + |X_6^2| + \ldots + |X_6^t| + |X_7| =$$

$$= 1 + 2(a_1 - 2) + 2(p_2 - 1)(a_2 - 1) +$$

$$+ \ldots + 2(p_t - 1)(a_t - 1) + (p_2 - 2) + \ldots + (p_t - 2) + t =$$

$$= (2a_2 - 1)(p_2 - 1) + \ldots + (2a_t - 1)(p_t - 1) + (2a_1 - 2)$$

элементов. Поэтому по лемме 2 получаем

$$L(2^{a_1}p_2^{a_2}\ldots p_t^{a_t}) \geqslant (2a_2 - 1)(p_2 - 1) + \ldots + (2a_t - 1)(p_t - 1) + (2a_1 - 2).$$

В случае, когда $p_1 = 2, t > 2, a_1 > 1$, утверждение теоремы доказано.

Пусть $p_1 > 2, t = 1$. Докажем тогда, что

$$L(n) = L(p_1^{a_1}) = (2a_1 - 1)(p_1 - 1) - 1.$$

Сначала представим $T(n)$ в виде объединения $(2a_1 - 1)(p_1 - 1) - 1$ арифметических прогрессий. Это можно сделать следующим образом:

$$T(n) = ((1, p_1) \cup (2, p_1) \cup \ldots \cup (p_1 - 3, p_1) \cup (p_1 - 1, p_1)) \cup$$

$$\cup((p_1 - 2, p_1^2) \cup (2p_1 - 2, p_1^2) \cup \ldots \cup ((p_1 - 1)p_1 - 2, p_1^2)) \cup$$

$$\cup((p_1^2 - 2, p_1^3) \cup (2p_1^2 - 2, p_1^3) \cup \ldots \cup ((p_1 - 1)p_1^2 - 2, p_1^3)) \cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((p_1^{a_1-1} - 2, p_1^{a_1}) \cup (2p_1^{a_1-1} - 2, p_1^{a_1}) \cup \ldots \cup ((p_1 - 1)p_1^{a_1-1} - 2, p_1^{a_1})) \cup$$

$$\cup((p_1, p_1^2) \cup (2p_1, p_1^2) \cup \ldots \cup ((p_1 - 1)p_1, p_1^2)) \cup$$

$$\cup((p_1^2, p_1^3) \cup (2p_1^2, p_1^3) \cup \ldots \cup ((p_1 - 1)p_1^2, p_1^3)) \cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((p_1^{a_1-1}, p_1^{a_1}) \cup (2p_1^{a_1-1}, p_1^{a_1}) \cup \ldots \cup ((p_1 - 1)p_1^{a_1-1}, p_1^{a_1})).$$

Видно, что здесь $(p_1-2)+2(a_1-1)(p_1-1) = (2a_1-1)(p_1-1)-1$ прогрессий. Множество

$$(1, p_1) \cup (2, p_1) \cup \ldots \cup (p_1 - 3, p_1) \cup (p_1 - 1, p_1)$$

покрывает все числа, не сравнимые с 0 или -2 по модулю p_1. Множество

$$((p_1 - 2, p_1^2) \cup (2p_1 - 2, p_1^2) \cup \ldots \cup ((p_1 - 1)p_1 - 2, p_1^2)) \cup$$

$$\cup((p_1^2 - 2, p_1^3) \cup (2p_1^2 - 2, p_1^3) \cup \ldots \cup ((p_1 - 1)p_1^2 - 2, p_1^3)) \cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((p_1^{a_1-1} - 2, p_1^{a_1}) \cup (2p_1^{a_1-1} - 2, p_1^{a_1}) \cup \ldots \cup ((p_1 - 1)p_1^{a_1-1} - 2, p_1^{a_1}))$$

покрывает все числа, сравнимые с -2 по модулю p_1, но не сравнимые с -2 по модулю $p_1^{a_1}$. Наконец, множество

$$\cup((p_1,p_1^2)\cup(2p_1,p_1^2)\cup\ldots\cup((p_1-1)p_1,p_1^2))\cup$$

$$\cup((p_1^2,p_1^3)\cup(2p_1^2,p_1^3)\cup\ldots\cup((p_1-1)p_1^2,p_1^3))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((p_1^{a_1-1},p_1^{a_1})\cup(2p_1^{a_1-1},p_1^{a_1})\cup\ldots\cup((p_1-1)p_1^{a_1-1},p_1^{a_1}))$$

покрывает все числа, сравнимые с 0 по модулю p_1, но не сравнимые с 0 по модулю $p_1^{a_1}$. Поэтому

$$L(p_1^{a_1})\leqslant(2a_1-1)(p_1-1)-1.$$

Покажем, что

$$L(p_1^{a_1})\geqslant(2a_1-1)(p_1-1)-1.$$

Рассмотрим множества

$$X_1:=\{1,2,\ldots,p_1-3,p_1-1\},$$

$$X_2^1:=\{p_1-2,2p_1-2,\ldots,(p_1-1)p_1-2\},$$

$$X_2^2:=\{p_1^2-2,2p_1^2-2,\ldots,(p_1-1)p_1^2-2\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$X_2^{a_1-1}:=\{p_1^{a_1-1}-2,2p_1^{a_1-1}-2,\ldots,(p_1-1)p_1^{a_1-1}-2\},$$

$$X_3^1:=\{p_1,2p_1,\ldots,(p_1-1)p_1\},$$

$$X_3^2:=\{p_1^2,2p_1^2,\ldots,(p_1-1)p_1^2\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$X_3^{a_1-1}:=\{p_1^{a_1-1},2p_1^{a_1-1},\ldots,(p_1-1)p_1^{a_1-1}\},$$

$$Y:=(2^{a_1}-2,2^{a_1})\cup(2^{a_1},2^{a_1}).$$

Покажем, что множество

$$X:=X_1\cup X_2^1\cup\ldots\cup X_2^{a_1-1}\cup X_3^1\cup\ldots\cup X_3^{a_1-1}$$

будет опорным семейством для множества Y. Пусть $x_1,x_2\in X$, $x_1<x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1,x_2-x_1)\cap(n-2,n)\neq\emptyset, \tag{11}$$

$$(x_1, x_2 - x_1) \cap (n, n) \neq \emptyset. \tag{12}$$

Возможны случаи:

Случай 1.

$x_1 \in X_1, x_2 \in X_1$. Тогда НОД$(x_2 - x_1, n) = 1$ и по лемме 1 верно (11).

Случай 2.

$x_1 \in X_1, x_2 \in X_2^i$ или $x_2 \in X_1, x_1 \in X_2^i$. Случай аналогичен случаю 1.

Случай 3.

$x_1 \in X_1, x_2 \in X_3^i$ или $x_2 \in X_1, x_1 \in X_3^i$. Случай аналогичен случаю 1.

Случай 4.

$x_1 \in X_2^i, x_2 \in X_2^i$. Тогда НОД$(x_2 - x_1, n) = p_1^i$ и по лемме 1 верно (11).

Случай 5.

$x_1 \in X_2^i, x_2 \in X_2^j, i < j$. Тогда НОД$(x_2 - x_1, n) = p_1^i$ и поэтому по лемме 1 получаем (11).

Случай 6.

$x_1 \in X_2^i, x_2 \in X_2^j, i > j$. Тогда НОД$(x_2 - x_1, n) = p_1^j$ и поэтому по лемме 1 получаем (11).

Случай 7.

$x_1 \in X_2^i, x_2 \in X_3^j$. Случай аналогичен случаю 1.

Случай 8.

$x_1 \in X_3^i, x_2 \in X_3^i$. Тогда НОД$(x_2 - x_1, n) = p_1^i$ и по лемме 1 верно (12).

Случай 9.

$x_1 \in X_3^i, x_2 \in X_3^j, i < j$. Тогда НОД$(x_2 - x_1, n) = p_1^i$ и поэтому по лемме 1 верно (12).

Случай 10.

$x_1 \in X_3^i, x_2 \in X_3^j, i > j$. Тогда НОД$(x_2 - x_1, n) = p_1^j$ и поэтому по лемме 1 верно (12).

Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y. Но в множестве X всего

$$|X_1| + |X_2^1| + |X_2^2| + \ldots + |X_2^{a_1-1}| + |X_3^1| + |X_3^2| + \ldots + |X_3^{a_1-1}| =$$
$$= (p_1 - 2) + 2(a_1 - 1)(p_1 - 1) = (2a_1 - 1)(p_1 - 1) - 1$$

элементов. Поэтому по лемме 2 получаем

$$L(p_1^{a_1}) \geqslant (2a_1 - 1)(p_1 - 1) - 1.$$

В случае, когда $p_1 > 2, t = 1$, утверждение теоремы доказано.

Пусть $p_1 > 2, t > 1$. Докажем тогда, что

$$L(n) = L(p_1^{a_1} \ldots p_t^{a_t}) = (2a_1 - 1)(p_1 - 1) + \ldots + (2a_t - 1)(p_t - 1).$$

Для доказательства верхней оценки нужно представить $T(n)$ в виде объединения

$$(2a_1-1)(p_1-1)+\ldots+(2a_t-1)(p_t-1)$$

арифметических прогрессий. Это можно сделать следующим образом:

$$T(n)=((1,p_1)\cup(2,p_1)\cup\ldots\cup(p_1-3,p_1)\cup(p_1-1,p_1))\cup$$

$$((1,p_2)\cup(2,p_2)\cup\ldots\cup(p_2-3,p_2)\cup(p_2-1,p_2))\cup$$

$$\cup\ldots\cup((1,p_t)\cup(2,p_t)\cup\ldots\cup(p_t-3,p_t)\cup(p_t-1,p_t))\cup$$

$$\cup((1\cdot p_1p_2\ldots p_t-2,p_1^2p_2\ldots p_t)\cup(2\cdot p_1p_2\ldots p_t-2,p_1^2p_2\ldots p_t)\cup$$

$$\cup\ldots\cup((p_1-1)\cdot p_1p_2\ldots p_t-2,p_1^2p_2\ldots p_t))\cup$$

$$\cup((1\cdot p_1^2p_2\ldots p_t-2,p_1^3p_2\ldots p_t)\cup(2\cdot p_1^2p_2\ldots p_t-2,p_1^3p_2\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot p_1^2p_2\ldots p_t-2,p_1^3p_2\ldots p_t))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot p_1^{a_1-1}p_2\ldots p_t-2,p_1^{a_1}p_2\ldots p_t)\cup$$

$$\cup(2\cdot p_1^{a_1-1}p_2\ldots p_t-2,p_1^{a_1}p_2\ldots p_t)\cup$$

$$\cup\ldots\cup((p_1-1)\cdot p_1^{a_1-1}p_2\ldots p_t-2,p_1^{a_1}p_2\ldots p_t))\cup$$

$$\cup((1\cdot p_1^{a_1}p_2\ldots p_t-2,p_1^{a_1}p_2^2p_3\ldots p_t)\cup$$

$$\cup(2\cdot p_1^{a_1}p_2\ldots p_t-2,p_1^{a_1}p_2^2p_3\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot p_1^{a_1}p_2\ldots p_t-2,p_1^{a_1}p_2^2p_3\ldots p_t))\cup$$

$$\cup((1\cdot p_1^{a_1}p_2^2p_3\ldots p_t-2,p_1^{a_1}p_2^3p_3\ldots p_t)\cup$$

$$\cup(2\cdot p_1^{a_1}p_2^2p_3\ldots p_t-2,p_1^{a_1}p_2^3p_3\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot p_1^{a_1}p_2^2p_3\ldots p_t-2,p_1^{a_1}p_2^3p_3\ldots p_t))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot p_1^{a_1}p_2^{a_2-1}p_3\ldots p_t-2,p_1^{a_1}p_2^{a_2}p_3\ldots p_t)\cup$$

$$\cup(2\cdot p_1^{a_1}p_2^{a_2-1}p_3\ldots p_t-2,p_1^{a_1}p_2^{a_2}p_3\ldots p_t)\cup$$

$$\cup\ldots\cup((p_2-1)\cdot p_1^{a_1}p_2^{a_2-1}p_3\ldots p_t-2,p_1^{a_1}p_2^{a_2}p_3\ldots p_t))\cup$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cup((1\cdot p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t-2,p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$

$$\cup(2\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2)\cup$$
$$\cup\dots\cup((p_t-1)\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2))\cup$$
$$\cup((1\cdot p_1^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^2-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup(2\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup\dots\cup((p_t-1)\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^3))\cup$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\cup((1\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup(2\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup\dots\cup((p_t-1)\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t}))\cup$$
$$\cup((1\cdot p_1p_2\dots p_t,p_1^2p_2\dots p_t)\cup(2\cdot p_1p_2\dots p_t,p_1^2p_2\dots p_t)\cup$$
$$\cup\dots\cup((p_1-1)\cdot p_1p_2\dots p_t,p_1^2p_2\dots p_t))\cup$$
$$\cup((1\cdot p_1^2p_2\dots p_t,p_1^3p_2\dots p_t)\cup(2\cdot p_1^2p_2\dots p_t,p_1^3p_2\dots p_t)\cup$$
$$\cup\dots\cup((p_1-1)\cdot p_1^2p_2\dots p_t,p_1^3p_2\dots p_t))\cup$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\cup((1\cdot p_1^{a_1-1}p_2\dots p_t,p_1^{a_1}p_2\dots p_t)\cup(2\cdot p_1^{a_2-1}p_2\dots p_t,p_1^{a_1}p_2\dots p_t)\cup$$
$$\cup\dots\cup((p_1-1)\cdot p_1^{a_1-1}p_2\dots p_t,p_1^{a_1}p_2\dots p_t))\cup$$
$$\cup((1\cdot p_1^{a_1}p_2\dots p_t,p_1^{a_1}p_2^2p_3\dots p_t)\cup$$
$$\cup(2\cdot p_1^{a_1}p_2\dots p_t,p_1^{a_1}p_2^2p_3\dots p_t)\cup$$
$$\cup\dots\cup((p_2-1)\cdot p_1^{a_1}p_2\dots p_t,p_1^{a_1}p_2^2p_3\dots p_t))\cup$$
$$\cup((1\cdot p_1^{a_1}p_2^2p_3\dots p_t,p_1^{a_1}p_2^3p_3\dots p_t)\cup$$
$$\cup(2\cdot p_1^{a_1}p_2^2p_3\dots p_t,p_1^{a_1}p_2^3p_3\dots p_t)\cup$$
$$\cup\dots\cup((p_2-1)\cdot p_1^{a_1}p_2^2p_3\dots p_t,p_1^{a_1}p_2^3p_3\dots p_t))\cup$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\cup((1\cdot p_1^{a_1}p_2^{a_2-1}p_3\dots p_t,p_1^{a_1}p_2^{a_2}p_3\dots p_t)\cup$$
$$\cup(2\cdot p_1^{a_1}p_2^{a_2-1}p_3\dots p_t,p_1^{a_1}p_2^{a_2}p_3\dots p_t)\cup$$
$$\cup\dots\cup((p_2-1)\cdot p_1^{a_1}p_2^{a_2-1}p_3\dots p_t,p_1^{a_1}p_2^{a_2}p_3\dots p_t))\cup$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\cup((1\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t, p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2)\cup$$
$$\cup(2\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t, p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2)\cup$$
$$\cup\dots\cup((p_t-1)\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t, p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2))\cup$$
$$\cup((1\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2, p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup(2\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2, p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup\dots\cup((p_t-1)\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2, p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^3))\cup$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\cup((1\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup(2\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup\dots\cup((p_t-1)\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t}))\cup$$
$$\cup((2a_1, 2p_1p_2)\cup(2a_2, 2p_2p_3)\dots\cup(2a_{t-1}, 2p_{t-1}p_t)\cup(2a_t, 2p_tp_1)),$$

где при $1\leqslant i\leqslant t-1$ имеем

$$1\leqslant a_i\leqslant p_ip_{i+1},\quad a_i\equiv 0 \mod p_i,\quad a_i\equiv -1 \mod p_{i+1}$$

и при $i=t$ имеем

$$1\leqslant a_t\leqslant p_1p_t,\quad a_t\equiv 0 \mod p_t,\quad a_t\equiv -1 \mod p_1.$$

Здесь серия

$$((1,p_1)\cup(2,p_1)\cup\dots\cup(p_1-3,p_1)\cup(p_1-1,p_1))\cup$$
$$((1,p_2)\cup(2,p_2)\cup\dots\cup(p_2-3,p_2)\cup(p_2-1,p_2))\cup$$
$$\cup\dots\cup((1,p_t)\cup(2,p_t)\cup\dots\cup(p_t-3,p_t)\cup(p_t-1,p_t))$$

накрывает все числа, не сравнимые с 0 и -2 по модулям $p_1,\dots,p_t$. Серия

$$((1\cdot p_1p_2\dots p_t-2, p_1^2p_2\dots p_t)\cup(2\cdot p_1p_2\dots p_t-2, p_1^2p_2\dots p_t)\cup$$
$$\cup\dots\cup((p_1-1)\cdot p_1p_2\dots p_t-2, p_1^2p_2\dots p_t))\cup$$
$$\cup((1\cdot p_1^2p_2\dots p_t-2, p_1^3p_2\dots p_t)\cup(2\cdot p_1^2p_2\dots p_t-2, p_1^3p_2\dots p_t)\cup$$
$$\cup\dots\cup((p_2-1)\cdot p_1^2p_2\dots p_t-2, p_1^3p_2\dots p_t))\cup$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\cup((1\cdot p_1^{a_1-1}p_2\dots p_t-2,p_1^{a_1}p_2\dots p_t)\cup$$
$$\cup(2\cdot p_1^{a_1-1}p_2\dots p_t-2,p_1^{a_1}p_2\dots p_t)\cup$$
$$\cup\dots\cup((p_1-1)\cdot p_1^{a_1-1}p_2\dots p_t-2,p_1^{a_1}p_2\dots p_t))\cup$$
$$\cup((1\cdot p_1^{a_1}p_2\dots p_t-2,p_1^{a_1}p_2^2p_3\dots p_t)\cup$$
$$\cup(2\cdot p_1^{a_1}p_2\dots p_t-2,p_1^{a_1}p_2^2p_3\dots p_t)\cup$$
$$\cup\dots\cup((p_2-1)\cdot p_1^{a_1}p_2\dots p_t-2,p_1^{a_1}p_2^2p_3\dots p_t))\cup$$
$$\cup((1\cdot p_1^{a_1}p_2^2p_3\dots p_t-2,p_1^{a_1}p_2^3p_3\dots p_t)\cup$$
$$\cup(2\cdot p_1^{a_1}p_2^2p_3\dots p_t-2,p_1^{a_1}p_2^3p_3\dots p_t)\cup$$
$$\cup\dots\cup((p_2-1)\cdot p_1^{a_1}p_2^2p_3\dots p_t-2,p_1^{a_1}p_2^3p_3\dots p_t))\cup$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\cup((1\cdot p_1^{a_1}p_2^{a_2-1}p_3\dots p_t-2,p_1^{a_1}p_2^{a_2}p_3\dots p_t)\cup$$
$$\cup(2\cdot p_1^{a_1}p_2^{a_2-1}p_3\dots p_t-2,p_1^{a_1}p_2^{a_2}p_3\dots p_t)\cup$$
$$\cup\dots\cup((p_2-1)\cdot p_1^{a_1}p_2^{a_2-1}p_3\dots p_t-2,p_1^{a_1}p_2^{a_2}p_3\dots p_t))\cup$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\cup((1\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2)\cup$$
$$\cup(2\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2)\cup$$
$$\cup\dots\cup((p_t-1)\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2))\cup$$
$$\cup((1\cdot p_1^{a_2}\dots p_{t-1}^{a_{t-1}}p_t^2-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup(2\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup\dots\cup((p_t-1)\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^2-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^3))\cup$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\cup((1\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup(2\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup\dots\cup((p_t-1)\cdot p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t-1}-2,p_1^{a_1}\dots p_{t-1}^{a_{t-1}}p_t^{a_t}))$$

накрывает все числа, сравнимые с -2 по модулям $p_1,\dots,p_t$, но не сравнимые с -2 по модулю $p_1^{a_1}\dots p_t^{a_t}$. Серия

$$((1\cdot p_1p_2\dots p_t,p_1^2p_2\dots p_t)\cup(2\cdot p_1p_2\dots p_t,p_1^2p_2\dots p_t)\cup$$

$$\cup\ldots\cup((p_1-1)\cdot p_1p_2\ldots p_t, p_1^2p_2\ldots p_t))\cup$$
$$\cup((1\cdot p_1^2p_2\ldots p_t, p_1^3p_2\ldots p_t)\cup(2\cdot p_1^2p_2\ldots p_t, p_1^3p_2\ldots p_t)\cup$$
$$\cup\ldots\cup((p_1-1)\cdot p_1^2p_2\ldots p_t, p_1^3p_2\ldots p_t))\cup$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\cup((1\cdot p_1^{a_1-1}p_2\ldots p_t, p_1^{a_1}p_2\ldots p_t)\cup$$
$$\cup(2\cdot p_1^{a_2-1}p_2\ldots p_t, p_1^{a_1}p_2\ldots p_t)\cup$$
$$\cup\ldots\cup((p_1-1)\cdot p_1^{a_1-1}p_2\ldots p_t, p_1^{a_1}p_2\ldots p_t))\cup$$
$$\cup((1\cdot p_1^{a_1}p_2\ldots p_t, p_1^{a_1}p_2^2p_3\ldots p_t)\cup$$
$$\cup(2\cdot p_1^{a_1}p_2\ldots p_t, p_1^{a_1}p_2^2p_3\ldots p_t)\cup$$
$$\cup\ldots\cup((p_2-1)\cdot p_1^{a_1}p_2\ldots p_t, p_1^{a_1}p_2^2p_3\ldots p_t))\cup$$
$$\cup((1\cdot p_1^{a_1}p_2^2p_3\ldots p_t, p_1^{a_1}p_2^3p_3\ldots p_t)\cup$$
$$\cup(2\cdot p_1^{a_1}p_2^2p_3\ldots p_t, p_1^{a_1}p_2^3p_3\ldots p_t)\cup$$
$$\cup\ldots\cup((p_2-1)\cdot p_1^{a_1}p_2^2p_3\ldots p_t, p_1^{a_1}p_2^3p_3\ldots p_t))\cup$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\cup((1\cdot p_1^{a_1}p_2^{a_2-1}p_3\ldots p_t, p_1^{a_1}p_2^{a_2}p_3\ldots p_t)\cup$$
$$\cup(2\cdot p_1^{a_1}p_2^{a_2-1}p_3\ldots p_t, p_1^{a_1}p_2^{a_2}p_3\ldots p_t)\cup$$
$$\cup\ldots\cup((p_2-1)\cdot p_1^{a_1}p_2^{a_2-1}p_3\ldots p_t, p_1^{a_1}p_2^{a_2}p_3\ldots p_t))\cup$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\cup((1\cdot p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t, p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$
$$\cup(2\cdot p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t, p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^2)\cup$$
$$\cup\ldots\cup((p_t-1)\cdot p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t, p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^2))\cup$$
$$\cup((1\cdot p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^2, p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup(2\cdot p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^2, p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^3)\cup$$
$$\cup\ldots\cup((p_t-1)\cdot p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^2, p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^3))\cup$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\cup((1\cdot p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$
$$\cup(2\cdot p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1}, p_1^{a_1}\ldots p_{t-1}^{a_{t-1}}p_t^{a_t})\cup$$

$$\cup \ldots \cup ((p_t - 1) \cdot p_1^{a_1} \ldots p_{t-1}^{a_{t-1}} p_t^{a_t - 1}, p_1^{a_1} \ldots p_{t-1}^{a_{t-1}} p_t^{a_t}))$$

накрывает все числа, сравнимые с 0 по модулям $p_1, \ldots, p_t$, но не сравнимые с 0 по модулю $p_1^{a_1} \ldots p_t^{a_t}$. Наконец, серия

$$(2a_1, 2p_1p_2) \cup (2a_2, 2p_2p_3) \ldots \cup (2a_{t-1}, 2p_{t-1}p_t) \cup (2a_t, 2p_tp_1)$$

накрывает все числа, сравнимые с 0 или -2 по модулям $p_1, \ldots, p_t$, но не сравнимые с 0 или -2 по модулю $p_1 \ldots p_t$. Поэтому

$$L(n) \leqslant \sum_{i=1}^{t}(p_i - 2) + 2\sum_{i=1}^{t}(a_i - 1)(p_i - 1) + t =$$

$$= (2a_1 - 1)(p_1 - 1) + \ldots + (2a_t - 1)(p_t - 1).$$

Для доказательства нижней оценки введем обозначения

$$X_1^{1,1} := \{1 \cdot p_1p_2^{a_2} \ldots p_t^{a_t} - 2, \ldots, (p_1 - 1) \cdot p_1p_2^{a_2} \ldots p_t^{a_t} - 2\},$$

$$X_1^{1,2} := \{1 \cdot p_1^2p_2^{a_2} \ldots p_t^{a_t} - 2, \ldots, (p_1 - 1) \cdot p_1^2p_2^{a_2} \ldots p_t^{a_t} - 2\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$X_1^{1,a_1-1} := \{1 \cdot p_1^{a_1-1}p_2^{a_2} \ldots p_t^{a_t} - 2, \ldots, (p_1 - 1) \cdot p_1^{a_1-1}p_2^{a_2} \ldots p_t^{a_t} - 2\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$X_1^{t,1} := \{1 \cdot p_1^{a_1} \ldots p_{t-1}^{a_{t-1}}p_t - 2, \ldots, (p_t - 1) \cdot p_1^{a_1} \ldots p_{t-1}^{a_{t-1}}p_t - 2\},$$

$$X_1^{t,2} := \{1 \cdot p_1^{a_1} \ldots p_{t-1}^{a_{t-1}}p_t^2 - 2, \ldots, (p_t - 1) \cdot p_1^{a_1} \ldots p_{t-1}^{a_{t-1}}p_t^2 - 2\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$X_1^{t,a_t-1} := \{1 \cdot p_1^{a_1} \ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1} - 2, \ldots, (p_t - 1) \cdot p_1^{a_1} \ldots p_{t-1}^{a_{t-1}}p_t^{a_t-1} - 2\},$$

$$X_2^{1,1} := \{1 \cdot p_1p_2^{a_2} \ldots p_t^{a_t}, \ldots, (p_1 - 1) \cdot p_1p_2^{a_2} \ldots p_t^{a_t}\},$$

$$X_2^{1,2} := \{1 \cdot p_1^2p_2^{a_2} \ldots p_t^{a_t}, \ldots, (p_1 - 1) \cdot p_1^2p_2^{a_2} \ldots p_t^{a_t}\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$X_2^{1,a_1-1} := \{1 \cdot p_1^{a_1-1}p_2^{a_2} \ldots p_t^{a_t}, \ldots, (p_1 - 1) \cdot p_1^{a_1-1}p_2^{a_2} \ldots p_t^{a_t}\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$X_2^{t,1} := \{1 \cdot p_1^{a_1} \ldots p_{t-1}^{a_{t-1}}p_t, \ldots, (p_t - 1) \cdot p_1^{a_1} \ldots p_{t-1}^{a_{t-1}}p_t\},$$

$$X_2^{t,2} := \{1 \cdot p_1^{a_1} \ldots p_{t-1}^{a_{t-1}}p_t^2, \ldots, (p_t - 1) \cdot p_1^{a_1} \ldots p_{t-1}^{a_{t-1}}p_t^2\},$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$X_2^{t,a_t-1} := \{1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, \dots, (p_t-1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}\},$$

$$X_3^1 := \{b_{1,1}, \dots, b_{1,p_1-2}\},$$

$$\dots\dots\dots\dots\dots\dots$$

$$X_3^t := \{b_{t,1}, \dots, b_{t,p_t-2}\},$$

$$X_4 := \{c_1, \dots, c_t\},$$

$$Y := (p_1^{a_1} \dots p_t^{a_t} - 2, p_1^{a_1} \dots p_t^{a_t}) \cup (p_1^{a_1} \dots p_t^{a_t}, p_1^{a_1} \dots p_t^{a_t}),$$

где

$$b_{i,j} \equiv j \mod p_i^{a_i}, \quad b_{i,j} \equiv 0 \mod \frac{n}{p_i^{a_i}},$$

$$c_i \equiv -1 \mod p_i^{a_i}, \quad c_i \equiv 0 \mod \frac{n}{p_i^{a_i}}.$$

Покажем, что множество

$$X := X_1^{1,1} \cup \dots \cup X_1^{t,a_t-1} \cup X_2^{1,1} \cup \dots \cup X_2^{t,a_t-1} \cup X_3^1 \cup \dots \cup X_3^t \cup X_4$$

будет опорным семейством для множества Y. Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (n-2, n) \neq \emptyset, \tag{13}$$

$$(x_1, x_2 - x_1) \cap (n, n) \neq \emptyset. \tag{14}$$

Возможны случаи:

Случай 1.

$x_1 \in X_1^{i,j_1}, x_2 \in X_1^{i,j_2}$, $j_1 \leqslant j_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_1}$ и по лемме 1 верно (13).

Случай 2.

$x_1 \in X_1^{i,j_1}, x_2 \in X_1^{i,j_2}$, $j_1 > j_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_2}$ и по лемме 1 верно (13).

Случай 3.

$x_1 \in X_1^{i_1,j_1}, x_2 \in X_1^{i_2,j_2}$, $i_1 \neq i_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_{i_1}^{a_{i_1}} p_{i_2}^{a_{i_2}}} p_{i_1}^{j_1} p_{i_2}^{j_2}$ и по лемме 1 верно (13).

Случай 4.

$x_1 \in X_1^{i_1,j_1}, x_2 \in X_2^{i_2,j_2}$. Тогда НОД$(x_2 - x_1, n) = 1$ и по лемме 1 получаем, что верно (13).

Случай 5.
$x_1 \in X_1^{i,j}, x_2 \in X_3^k$ или $x_2 \in X_1^{i,j}, x_1 \in X_3^k$. Случай аналогичен случаю 4.
Случай 6.
$x_1 \in X_1^{i,j}, x_2 = c_i$ или $x_2 \in X_1^{i,j}, x_1 = c_i$. Тогда НОД$(x_2 - x_1, n) = p_i^j$ и по лемме 1 верно (13).
Случай 7.
$x_1 \in X_1^{i,j}, x_2 = c_k$, $k \neq i$ или $x_2 \in X_1^{i,j}, x_1 = c_k$, $k \neq i$. Тогда верно, что НОД$(x_2 - x_1, n) = p_i^{a_i}$ и по лемме 1 получаем (13).
Случай 8.
$x_1 \in X_2^{i,j_1}, x_2 \in X_2^{i,j_2}$, $j_1 \leqslant j_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_1}$ и по лемме 1 верно (14).
Случай 9.
$x_1 \in X_2^{i,j_1}, x_2 \in X_2^{i,j_2}$, $j_1 > j_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_2}$ и по лемме 1 верно (14).
Случай 10.
$x_1 \in X_2^{i_1,j_1}, x_2 \in X_2^{i_2,j_2}$, $i_1 \neq i_2$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_{i_1}^{a_{i_1}} p_{i_2}^{a_{i_2}}} p_{i_1}^{j_1} p_{i_2}^{j_2}$ и по лемме 1 верно (14).
Случай 11.
$x_1 \in X_2^{i,j}, x_2 \in X_3^i$ или $x_2 \in X_1^{i,j}, x_1 \in X_3^i$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i}}$ и по лемме 1 верно (14).
Случай 12.
$x_1 \in X_2^{i,j}, x_2 \in X_3^k, i \neq k$ или $x_2 \in X_2^{i,j}, x_1 \in X_3^k, i \neq k$. Тогда верно, что НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_k^{a_k}} p_i^j$ и по лемме 1 получаем (14).
Случай 13.
$x_1 \in X_2^{i,j}, x_2 = c_i$ или $x_2 \in X_2^{i,j}, x_1 = c_i$. Случай аналогичен случаю 11.
Случай 14.
$x_1 \in X_2^{i,j}, x_2 = c_k$, $k \neq i$ или $x_2 \in X_2^{i,j}, x_1 = c_k$, $k \neq i$. Случай аналогичен случаю 12.
Случай 15.
$x_1 \in X_3^i, x_2 \in X_3^i$. Случай аналогичен случаю 11.
Случай 16.
$x_1 \in X_3^i, x_2 \in X_3^j$, $i \neq j$. Тогда НОД$(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_j^{a_j}}$ и по лемме 1 верно (14).
Случай 17.
$x_1 \in X_3^i, x_2 = c_i$ или $x_1 \in X_3^i, x_2 = c_i$. Случай аналогичен случаю 11.
Случай 18.

$x_1 \in X_3^i, x_2 = c_j, i \neq j$ или $x_2 \in X_3^i, x_1 = c_j, i \neq j$. Случай аналогичен случаю 16.

Случай 19.

$x_1 = c_i, x_2 = c_j$. Случай аналогичен случаю 16.

Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y. Но в множестве X всего

$$|X_1^{1,1}| + \ldots + |X_1^{t,a_t-1}| + |X_2^{1,1}| + \ldots + |X_2^{t,a_t-1}| + |X_3^1| + \ldots + |X_3^t| + |X_4| =$$

$$= 2(p_1 - 1)(a_1 - 1) + \ldots + 2(p_t - 1)(a_t - 1) + (p_1 - 2) + \ldots + (p_t - 2) + t =$$

$$= (2a_1 - 1)(p_1 - 1) + \ldots + (2a_t - 1)(p_t - 1)$$

элементов. Поэтому по лемме 2 получаем

$$L(p_1^{a_1} \ldots p_t^{a_t}) \geqslant (2a_1 - 1)(p_1 - 1) + \ldots + (2a_t - 1)(p_t - 1).$$

В случае, когда $p_1 > 2, t > 1$, утверждение теоремы доказано. ■

Список литературы

[1] П. С. Дергач, Э. С. Айрапетов. *О прогрессивном разбиении некоторых подмножеств натурального ряда.* Интеллектуальные системы, 2015. Т.19, вып. 3, М., Сс. 79-86.

[2] П. С. Дергач. *О каноническом регулярном представлении S-тонких языков.* Интеллектуальные системы, 2014. Т.18, вып. 1, М., Сс. 211-242.системы, 2014. Т.18, вып. 1, М., Сс. 211-242.

[3] П. С. Дергач. *О проблеме вложения допустимых классов.* Интеллектуальные системы, 2015. Т.19, вып. 2, М., Сс. 143-174.

[4] П. С. Дергач. *О двух размерностях спектров тонких языков.* Интеллектуальные системы, 2015. Т.19, вып. 3, М., Сс. 155-174.

[5] П. С. Дергач, Э. С. Айрапетов. *О прогрессивном разбиении последовательности натуральных чисел, имеющей пропуск длины 2.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 67-86. Д. Е. Александров. *Эффективные методы реализации проверки содержания сетевых пакетов регулярными выражениями.* Интеллектуальные системы, 2014. Т.18, вып. 1, М., Сс. 37-60.

[6] Д. Н. Бабин. *Частотные регулярные языки.* Интеллектуальные системы, 2014. Т.18, вып. 1, М., Сс. 205-210.

[7] Д. Е. Александров. *Об оценках автоматной сложности распознавания классов регулярных языков.* Интеллектуальные системы, 2014. Т.18, вып. 4, М., Сс. 161-190.

[8] В. М. Дементьев. *О звездной высоте регулярного языка и циклической сложности минимального автомата.* Интеллектуальные системы, 2014. Т.18, вып. 4, М., Сс. 215-222.

[9] И. Е. Иванов. *О сохранении периодических последовательностей автоматами с магазинной памятью с однобуквенным магазином.* Интеллектуальные системы, 2015. Т.19, вып. 1, М., Сс. 145-160.

[10] А. А. Петюшко. *О контекстно-свободных биграмных языках.* Интеллектуальные системы, 2015. Т.19, вып. 2, М., Сс. 187-208.

[11] И. Е. Иванов. *Нижняя оценка на максимальную длину периода выходной последовательности автономного автомата с магазинной памятью.* Интеллектуальные системы, 2015. Т.19, вып. 3, М., Сс. 175-194.

[12] В. А. Орлов. *О конечных автоматах с максимальной степенью различимости состояний.* Интеллектуальные системы, 2016. Т.20, вып. 1, М., Сс. 213-222.

[13] П. С. Дергач. *О проблеме проверки однозначности алфавитного декодирования в классе регулярных языков с полиномиальной функцией роста.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 147-202.

[14] А. М. Миронов. *Основные понятия теории вероятностных автоматов.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 283-330.

[15] А. А. Петюшко, Д. Н. Бабин. *Классификация Хомского для матриц биграммных языков.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 331-336.

[16] С. Б. Родин. *О связи линейно реализуемых автоматов и автоматов с максимальной вариативностью относительно кодирования состояний.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 337-348.

Нейросетевое распознавание рукописных символов на изображениях низкого качества

С. А. Комков (МГУ имени М. В. Ломоносова, Москва)

В данной работе решена задача построения сверточной нейронной сети, способной распознавать рукописные символы на сильно зашумленных изображениях с точностью, сопоставимой с человеческой. При этом обучение классификатора происходит по размеченной базе сильно зашумленных изображений, в которой 5% обучающих примеров размечено неправильно.

Ключевые слова: сверточные нейронные сети, распознавание изображений, машинное обучение, обучение с учителем.

Введение.

Стандартная искусственная нейронная сеть прямого распространения — это система, состоящая из нескольких слоев взаимосвязанных искусственных нейронов. Каждый нейрон принимает вектор выходных сигналов всех нейронов предшествующего слоя и скалярно умножает его на собственный вектор весов. К полученному числу в нейроне применяется функция активации, после чего результат поступает на входы ко всем нейронам следующего слоя. Таким образом, входной слой сети обнаруживает набор примитивных шаблонов поступающих данных, второй слой обнаруживает закономерности шаблонов и т.д.

Сверточная нейронная сеть — это особый вид искусственных нейронных сетей. Она состоит из одного или нескольких сверточных слоев (иногда со слоями подвыборки), за которыми следуют полносвязные слои как в обычной нейронной сети. Архитектура сверточных нейронных сетей мотивирована открытием механизма работы визуальной коры головного мозга. В коре содержится много клеток-рецепторов, которые

отвечают за детектирование света в маленьких перекрывающихся областях визуального поля, а более сложные клетки обрабатывают сигналы, поступающие с этих рецепторов.

Сверточные нейронные сети показывают отличные результаты при обработке данных с пространственной структурой по нескольким причинам:

- устойчивость к сдвигам и поворотам объекта на изображении, а так же устойчивость к шумам;
- учет пространственной структуры входных признаков;
- меньшее количество оптимизируемых параметров относительно классических полносвязных сетей;
- более быстрое и качественное обучение относительно обучения полносвязных сетей.

Наиболее известной классической сверточной нейронной сетью является LeNet-5 французского информатика Яна ЛеКуна [7]. Данная сеть обучалась и тестировалась по базе качественных рукописных изображений MNIST [8]. На тестовой выборке сеть верно классифицировала более 99% символов, что сравнимо с человеческой точностью.

Слои сверточной нейронной сети.

Сверточный слой. Входом слоя являются D матриц размера $N \times M$. Сверточный слой может быть как входным слоем сети, так и скрытым слоем. В случае, если сверточный слой является входным, то $N \times M$ — размер изображения, а D — количество цветовых каналов изображения. Входные импульсы сворачиваются T ядрами размера $k \times k \times D$ каждое. Свертка слоя одним ядром производит один выходной признак. Начиная с левого верхнего угла, ядро перемещается по изображению, пока не дойдет до правой границы. Тогда начальное положение ядра смещается вниз, и ядро снова начинает движение вправо. Таким образом, на выходе слоя образуются T матриц размера $(N - k + 1) \times (M - k + 1)$, где значение на месте с координатой (i, j) матрицы под номером k — это результат свертки k-го ядра с входным изображением в ситуации, когда левый верхний угол ядра имеет координаты (i, j). Полученные значения могут быть поданы на вход следующего сверточного слоя.

Слой подвыборки. На слое подвыборки каждый канал входа разбивается на непересекающиеся квадраты размера r на r. Из всех значений каждого квадрата на следующий слой подается только максимальное значение. Таким образом, если вход слоя подвыборки состоит из D матриц $N \times M$, то на выходе будет D матриц размера $(N/r) \times (M/r)$. Данный слой делает сеть более устойчивой к шуму и уменьшает количество весовых коэффициентов для оптимизации. Использование слоя подвыборки мотивировано тем, что для сети важно само наличие признака, а не его точное положение.

Нелинейный слой активации. На данных слоях внутри сети ко всем значениям входа применяется нелинейная функция активации, и результат подается на выход. Таким образом, слой активации не меняет размер входа. Наиболее популярной нелинейной функцией активации является ReLU функция: $\mathrm{ReLU}(x) = \max(0, x)$. В качестве функции активации в работе использовалась модернизированная ReLU функция: $\mathrm{PReLU}(x) = \max(a, x)$, где параметр a автоматически подбирается при обучении модели. Данный подход позволяет улучшить результаты сети за счет подбора оптимальной функции активации для каждого нейрона [3].

Выходной слой построенной сети состоит из 67 нейронов, по количеству возможных классов. На этом слое применяется функция активации Softmax. Данная функция преобразовывает выход j-го нейрона равный z_j по формуле $\sigma_j(z) = \frac{e^{z_j}}{\sum\limits_{k=1}^{67} e^{z_k}}$. Таким образом, на выходе сети получаются оценки вероятности того, что был подан соответствующий класс.

Полносвязный слой. В полносвязном слое на вход каждому нейрону подаются все выходы предшествующего слоя. Соответствующие веса для входов в каждом нейроне, величина сдвига и параметр a в функции активации PReLU подбираются автоматически при обучении сети.

Дропаут слой. Дропаут слой задается параметром p, который равен вероятности, с которой каждый вход не будет передан на выход в течение одной итерации обучения сети. Таким образом, при обучении на каждой итерации часть нейронов выключается из процесса, и веса меняются только у оставшихся нейронов. При распознавании с помощью сети в работе участвуют уже все нейроны. Так как выход слоя при обучении имел меньший размер, то при распознавании все значения входа

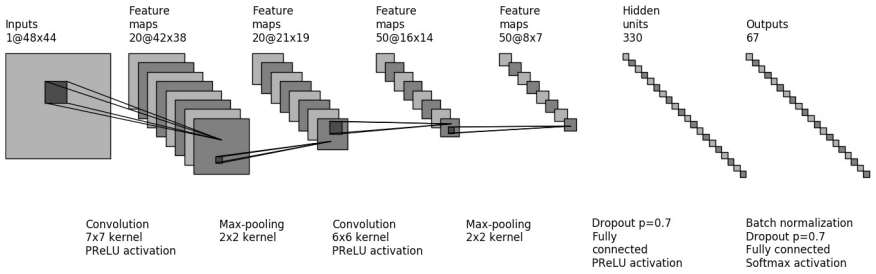


Рис. 1: Архитектура сети.

дропаут слоя умножаются на число $(1 - p)$ и переходят на выход. Данный слой уменьшает время одной эпохи обучения в связи с меньшим число оптимизируемых параметров, а также позволяет лучше бороться с переобучением сети относительно стандартных методов регуляризации [10].

Нормализующий слой. На данном слое от всех входов отнимается выборочное среднее значений на входах, и результат делится на корень выборочной дисперсии. Выборочные величины вычисляются с учетом значений на входах данного слоя на предыдущих итерациях обучения. Данный подход позволяет увеличить скорость обучения сети и улучшить итоговый результат [4].

Архитектура сети.

Архитектура построенной сети представлена на рис. 1.

Исходное монохромное изображение имеет размеры 48 на 44. Первым слоем идет свертка изображения 20 ядрами размера $7\times7\times1$ и применение функции PReLU к получившимся значениям. Получаем 20 изображений 42 на 38.

Далее слой подвыборки разбивает каждое из 20 изображений на непересекающиеся квадраты 2 на 2 и оставляет только максимальное значение из каждого квадрата. Таким образом, на выходе первого слоя подвыборки получаются 20 изображений 21 на 19.

Затем идет свертка полученных изображений 50 ядрами размера $6 \times 6 \times 20$ и применение к полученным значениям функции PReLU. На выходе получается 50 изображений 16 на 14.

Второй слой подвыборки аналогично первому возвращает 50 изображений 8 на 7.

После, значения подаются на дропаут слой с параметром $p = 0.7$. После дропаут слоя идет полносвязный слой из 330 нейронов с функцией активацией PReLU.

Все выходы первого полносвязного слоя подаются на нормализующий слой, а после него на дропаут слой с параметром $p = 0.7$. В конце идет полносвязный слой с 67 нейронами, по количеству возможных классов, каждый из которых распознает определенный класс. К выходам последнего полносвязного слоя применяется функция активации Softmax. Итоговым классом для изображения предсказывается тот класс, у которого оценка вероятности наибольшая.

База изображений.

Имеется размеченная база сильно зашумленных монохромных изображений рукописных символов [5] со следующими свойствами:

- размер изображений — 48 на 44 пикселей;
- символы на изображениях принадлежат одному из 67 классов: 33 класса, соответствующие символам кириллицы (прописные и строчные буквы определяются в один класс), 30 классов, соответствующие числам с 1 по 30, 4 класса, соответствующие запятым, точкам, пробелам и символам процента;
- тренировочная подвыборка состоит из 3600 изображений;
- тестирование построенной модели проводится по 900 изображениям, не участвовавшим в обучении;
- изображения различных классов равномерно распределены по тренировочной и тестовой подвыборкам;
- 5% изображений тренировочной подвыборки размечены неправильно;
- на изображениях присутствуют артефакты в виде границ ячеек, клякс или утерянной части изображения, часть символов выходит за пределы изображения;

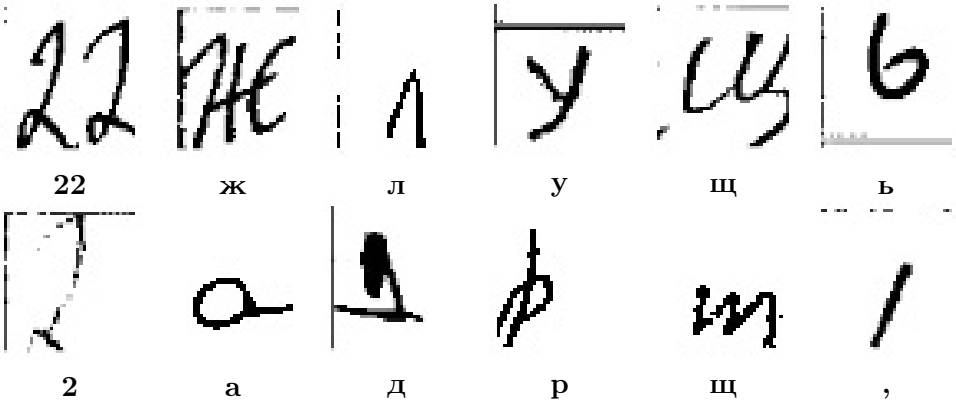


Рис. 2: Изображения тренировочной подвыборки и их классы.

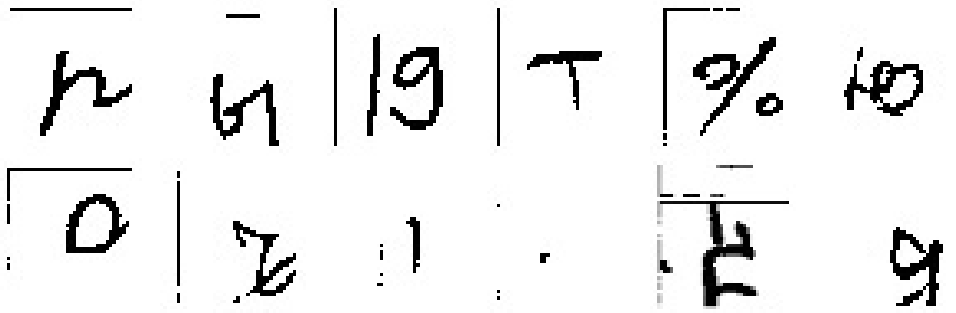


Рис. 3: Изображения тестовой подвыборки.

- примеры изображений из тренировочной и тестовой подвыборок представлены на рис. 2 и рис. 3.

Таким образом, исследуется способность сверточных нейронных сетей обобщать образы классов при обучении по выборке низкого качества с выбросами.

Обучение нейронной сети.

Современные методы обучения нейронных сетей базируются на классическом методе обратного распространения ошибки (параграф 4.3 из [1]). Основная идея этого метода состоит в распространении сигналов ошибки от выходов сети к её входам, в направлении, обратном прямому распространению сигналов в обычном режиме работы. Для этого вво-

дится функция потерь, зависящая, в частности, от всех весов нейронной сети. Таким образом, на каждом слое вычисляется градиент функции потерь, и веса данного слоя меняются в направлении противоположным градиенту.

Для мультиклассовой классификации при обучении сети в качестве функции потерь в методе обратного распространения ошибки используется категориальная кросс-энтропия. В работе веса представленной нейронной сети при обучении меняются каждый раз после обработки 30 изображений. В качестве метода обучения в работе используется адаптивный метод Nadam [2], полученный добавлением ускоренного градиента Нестерова [9] в адаптивный метод обучения Adam [6].

Ускоренный градиент Нестерова вычисляет по следующей формуле:

$$g_t := \gamma g_{t-1} + \alpha \bigtriangledown_\theta f(\theta - \gamma g_{t-1}),$$

где g_t — градиент Нестерова в момент времени t, θ — вектор весов нейронной сети, α — скорость обучения, γ — импульс обучения, а $f(\cdot)$ — функция потерь. Данный прием придает импульс процессу обучения нейронной сети, что позволяет меньше застревать в точках локального минимума.

Идея адаптивных методов заключается в понижении скорости обучения только тех весов нейронной сети, которые обучаются интенсивнее всего. Для этого для каждого параметра нейронной сети вычисляет некоторое число, характеризующее интенсивность обучения этого параметра. Преимущество метода Adam перед другими адаптивными методами заключается в универсальной начальной инициализации параметров этого метода, которая показывает отличные результаты на нейронных сетях различных архитектур. Прочие методы обучения требуют большего количества экспериментов и более чувствительны к изменениям архитектуры сети. Изменение весов методом Adam при рекомендуемой инициализации задается следующими формулами:

$$g_t := \bigtriangledown_\theta f(\theta_{t-1}),$$

$$m_t := 0.9 m_{t-1} + 0.1 g_t,$$

$$v_t^i := 0.999 v_{t-1}^i + 0.001 {g_t^i}^2,$$

$$\hat{m_t} := m_t / (1 - 0.9^t),$$

$$\hat{v_t} := v_t / (1 - 0.999^t),$$

$$\theta_t^i := \theta_{t-1}^i - \alpha \hat{m_t}^i / (\sqrt{\hat{v_t}^i} + 10^{-8}),$$

где $f(\cdot)$ — функция потерь, θ_t — вектор весов нейронной сети в момент времени t, g_t — градиент функции потерь в момент времени t, m_t — импульс движения в момент времени t, v_t — вектор интенсивности обучения весов нейронной сети в момент времени t, а α — скорость обучения. Таким образом, для весов нейронной сети, для которых на предшествующих итерациях соответствующее значение градиента было велико, будет уменьшаться скорость обучения.

Результаты и выводы.

Результаты тестирования построенной нейронной сети представлены в табл. 1. Так же по описанной базе изображений была обучена и протестирована сверточная нейронная сеть LeNet-5, о которой говорилось в введении, и LeNet-5 с функцией активации ReLU вместо сигмоиды. Дополнительно, тестовая подвыборка была полностью размечена человеком.

Классификатор	**Процент совпадений**
LeNet-5	61.667
LeNet-5 + ReLU activation	67.556
Представленная сверточная нейронная сеть	80.556
Человек	84.889

Таблица 1: Результаты тестирования классификаторов.

Таким образом, построенная сверточная нейронная сеть показывает значительно лучшие результаты по сравнению с каноничной архитектурой сверточных нейронных сетей. При этом результаты классификации сравнимы с человеческой классификацией символов на изображениях. Видно, что предложенные методы по улучшению качества нейросетевого распознавания вносят ощутимый вклад в способность нейронной сети предсказывать верные значения.

Список литературы

[1] Хайкин С. Нейронные сети: полный курс, 2-е издание. – Издательский дом Вильямс, 2008.

[2] Dozat T. Incorporating Nesterov momentum into Adam. – Stanford University, Tech. Rep., 2015.[Online]. Available: http://cs229. stanford. edu/proj2015/054 report. pdf, 2015.

[3] He K. et al. Delving deep into rectifiers: Surpassing human-level performance on imagenet classification //Proceedings of the IEEE international conference on computer vision. – 2015. – С. 1026-1034.

[4] Ioffe S., Szegedy C. Batch normalization: Accelerating deep network training by reducing internal covariate shift //arXiv preprint arXiv:1502.03167. – 2015.

[5] Kaggle in Class [Электронный ресурс] : Handwritten symbols recognition (CMF). — Электрон. дан. (4 файла). — San Francisco : 2010 — Режим доступа: https://inclass.kaggle.com/c/handwritten-symbols-recognition-cmf, свободный. — Загл. с экрана

[6] Kingma D., Ba J. Adam: A method for stochastic optimization //arXiv preprint arXiv:1412.6980. – 2014.

[7] LeCun Y. et al. Gradient-based learning applied to document recognition //Proceedings of the IEEE. – 1998. – Т. 86. – №. 11. – С. 2278-2324.

[8] LeCun Y., Cortes C., Burges C. J. C. The MNIST database of handwritten digits. – 1998.

[9] Nesterov Y. A method of solving a convex programming problem with convergence rate O (1/k2) //Soviet Mathematics Doklady. – 1983. – Т. 27. – №. 2. – С. 372-376.

[10] Srivastava N. et al. Dropout: a simple way to prevent neural networks from overfitting //Journal of Machine Learning Research. – 2014. – Т. 15. – №. 1. – С. 1929-1958.

TABLE OF CONTENTS