

Московский Государственный Университет
имени М.В. Ломоносова
Российская Академия Наук
Международная Академия Технологических Наук

Интеллектуальные Системы.

Теория и приложения

ТОМ 27 ВЫПУСК 1 * 2023

МОСКВА

Главный редактор: д.ф.-м.н., профессор Э.Э. Гасанов

Редакционная коллегия:

д.ф.-м.н., проф. А. Е. Андреев	(зам. главного редактора)
к.ф.-м.н., с.н.с. А.В. Галащенко	(зам. главного редактора)
к.ф.-м.н., доц. А. С. Строгалов	(зам. главного редактора)
к.ф.-м.н., м.н.с. В. В. Осокин	(ответственный секретарь)

д.ф.-м.н, проф. В.В.Александров, д.ф.-м.н, проф. С.В.Алешин, д.ф.-м.н, проф. Д.Н.Бабин, проф. К.Вашик, проф. Я.Деметрович, академик РАН, д.ф.-м.н, проф. Ю.Л.Ершов, проф. Г.Килибарда, д.ф.-м.н, проф. В.Н.Козлов, д.ф.-м.н, проф. А.В.Михалев, к.ф.-м.н, в.н.с. В.А.Носов, д.ф.-м.н, проф. А.С.Подколзин, д.ф.-м.н, проф. Ю.П.Пытьев, д.т.н, проф. А.П.Рыжов, академик РАН, д.т.н, проф. А.С.Сигов, проф. Б.Тальхайм, проф. Ш.Ушчумлич, д.ф.-м.н, доц. А.А.Часовских, д.ф.-м.н, проф. А.В.Чечкин, к.ф.-м.н. Р.Шчепанович.

Секретарь редакции: И. О. Бергер, Е. В. Кузнецова

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 имени М. В. Ломоносова, Научного Совета по комплексной проблеме «Кибернетика» РАН, Отделения «Математическое моделирование технологических процессов» МАТН.

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: 119991, Москва, ГСП-1, Ленинские Горы, д. 1, 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».

© ООО «Интеллектуальные системы», 2023.

ОГЛАВЛЕНИЕ

Часть 1. Общие проблемы теории интеллектуальных систем

Дроздов И.Ю., Парфенов Д.В. Влияние распределения спектра матрицы на точность сингулярного разложения 5

Часть 2. Специальные вопросы теории интеллектуальных систем

Соколов А.П., Прохоренкова Л.А. О выразительных возможностях ансамблей решающих деревьев 18

Стырт О.Г. Графы ортогональности матриц над коммутативными кольцами
24

Шишляков В.Г. Выразимость CPL-функций нейронными схемами над ReLU-базисами 35

Часть 3. Математические модели

Валинуров Д.Ю. Вычислительная сложность определения локальности кода 80

Ефимов А.А. Нижняя оценка энергопотребления для класса объемных схем 91

Трифорова Е.Е. О числе p -сократимых индуцированных вероятностных функций 134

Часть 4. Семинары кафедры МатИС

Доклады семинара «Теория автоматов» 144

Доклады семинара «Вопросы сложности алгоритмов поиска» 154

Часть 1.
Общие проблемы теории
интеллектуальных систем

Влияние распределения спектра матрицы на точность сингулярного разложения

И. Ю. Дроздов¹ Д. В. Парфенов²

С помощью численных экспериментов подтверждена гипотеза о зависимости точности нахождения индивидуальных сингулярных значений с помощью численных алгоритмов от особенностей распределения сингулярных значений матрицы при фиксированном числе обусловленности. Продемонстрирована недостаточность применения относительной погрешности по Евклидовой норме вектора результатов и предложена альтернативная метрика в виде среднеквадратичной относительной погрешности.

Ключевые слова: сингулярное разложение, число обусловленности, спектр матрицы, численная устойчивость

1. Введение

Сингулярное разложение (SVD) является одним из наиболее часто применяемых представлений матриц общего вида для решения множества практических задач. Немало и реализаций алгоритмов сингулярного разложения в различных программных библиотеках. Как и для многих других численных методов, здесь важна численная устойчивость. Некоторые аспекты этого вопроса достаточно исследованы [1], обычно в качестве метрики точности разложения используется L_2 -норма относительной погрешности вектора сингулярных значений $\|\sigma - \hat{\sigma}\|/\|\sigma\|$. Общепринятым показателем “качества” матрицы при решении задач является число обусловленности, определяемое как отношение максимального и минимального сингулярных значений $\sigma_{\max}/\sigma_{\min}$. Считается, что устойчивость сингулярного разложения зависит от числа обусловленности матрицы $\sigma_{\max}/\sigma_{\min}$ [2]. Целью данного исследования является проверка гипотезы о зависимости устойчивости сингулярного разложения не только от числа обусловленности, но и от особенностей распределения сингулярных значений в спектре матрицы. Также мы предлагаем и

¹ Дроздов Игорь Юрьевич — аспирант каф. высшей математики Института искусственного интеллекта РТУ МИРЭА, e-mail: drozdov_i@mirea.ru.

Drozдов Igor Yurievich — Ph.D. student, Russian Technological University (MIREA), Institute of Artificial Intelligence, Department of Higher Mathematics.

² Парфенов Денис Васильевич — к.т.н., доцент каф. высшей математики Института искусственного интеллекта РТУ МИРЭА, e-mail: parfenov@mirea.ru.

Parfenov Denis Vasilevich, Ph.D. — associate professor, Russian Technological University (MIREA), Institute of Artificial Intelligence, Department of Higher Mathematics.

обосновываем использование альтернативной метрики для оценки точности нахождения сингулярных значений.

2. Применения сингулярного разложения

Сингулярное разложение определяется как

$$A = U\Sigma V^T, \quad (1)$$

где A – исходная матрица размером $m \times n$, U и V – унитарные матрицы размерами $m \times m$ и $n \times n$ соответственно, Σ – диагональная матрица размером $\min(m, n) \times \min(m, n)$ с сингулярными значениями на главной диагонали. У матрицы A размером $m \times n$ существует $\min(m, n)$ сингулярных значений. Это разложение широко применяется в численной математике, статистике и инженерных дисциплинах. Далее кратко рассмотрим типичные применения с целью подчеркнуть важность точности отыскания сингулярных значений.

Сингулярное разложение – стандартный способ вычисления псевдообратной матрицы Мура-Пенроуза [3]. Псевдообратная матрица A^+ – обобщение обратной матрицы, определенное и для прямоугольных и вырожденных матриц и позволяющее решать пере- или недоопределенные системы линейных уравнений. Имея систему уравнений $Ax = b$, ее решение с помощью псевдообратной матрицы $x = A^+b$ идейно аналогично случаю с обратной матрицей. Если система несовместна, такое решение является наилучшим в смысле наименьшей квадратической ошибки (проекция вектора b на пространство столбцов A), т.е. $\forall x \in \text{im}A \quad \|Ax - b\|_2 \geq \|A\hat{x} - b\|_2$, где $\hat{x} = A^+b$, $\text{im}A$ – образ матрицы A (линейная оболочка ее столбцов). Если у системы бесконечное множество решений, псевдообратная матрица позволяет найти решение с наименьшей евклидовой нормой, т.е. $\forall x : Ax = b \quad \|\hat{x}\|_2 \leq \|x\|_2$. Зная сингулярное разложение $A = U\Sigma V^T$, очень просто получить псевдообратную матрицу как $A^+ = U\Sigma^+V^T$, где псевдообращение диагональной матрицы Σ^+ получается заменой всех ненулевых элементов в Σ на обратные к ним и транспонированием получившейся матрицы.

Целое семейство вычислительных методов, в основе которых лежит сингулярное разложение, может быть охарактеризовано как “приближения меньшего ранга” [5]. В общем случае задача приближения меньшего ранга заключается в нахождении матрицы, максимально “близкой” к исходной, но имеющей при этом заданный меньший ранг r . Иными словами, это задача минимизации нормы Фробениуса:

$$\min_{\hat{A}} \|\hat{A} - A\|_F \quad \text{s.t.} \quad \text{rank}(A) < r, \quad A \in \mathbb{R}^{m \times n}. \quad (2)$$

У этой задачи есть аналитическое решение с использованием сингулярного разложения (теорема Экарта-Юнга-Мирского, [6, 7]). Если $A = U\Sigma V^T \in \mathbb{R}^{m \times n}$, $m \geq n$, то его можно представить в блочном виде:

$$U = [U_1 \quad U_2], \quad \Sigma = \begin{bmatrix} \Sigma_1 & 0 \\ 0 & \Sigma_2 \end{bmatrix}, \quad V = [V_1 \quad V_2],$$

где $U_1 - m \times r$, $\Sigma_1 - r \times r$ и $V_1 - n \times r$. Тогда матрица \hat{A} , удовлетворяющая (2), находится как $\hat{A} = U_1 \Sigma V_1^T$, при этом

$$\|\hat{A} - A\|_F = \sqrt{\sigma_{r+1}^2 + \sigma_{r+2}^2 + \dots + \sigma_m^2}.$$

Один из важных практических методов, использующих приближение меньшего ранга, – это метод главных компонент (МГК), современный обзор которого приведен в [8]. Формально, МГК является техникой уменьшения размерности данных путем линейного преобразования в новую ортогональную систему координат, где данные могут быть описаны в меньшей размерности при минимальной потере информации. Применение сингулярного разложения к матрице данных позволяет выделить “главные компоненты”: сингулярные пары вектор-значение, где сингулярное значение ассоциируется со значением дисперсии данных в направлении соответствующего сингулярного вектора. МГК может быть использован в разведочном анализе данных, с целью визуализации многомерных данных [9] или уменьшения размерности для упрощения модели [10]. Также приближение меньшего ранга используется для идентификации систем (построения математической модели динамической системы на основе статистических наблюдений) [11] и лежит в основе латентного семантического анализа (метода обработки естественных языков, позволяющего анализировать зависимости между документами с содержащимися в них терминами) [12]. Подробный обзор техник и приложений аппроксимации меньшего ранга приведен в [13].

3. Цели и методы исследования

Целью исследования является выявление зависимости точности нахождения сингулярных значений от их распределения при фиксированном числе обусловленности. Чаще всего в численной линейной алгебре используются следующие виды погрешностей [4], позволяющие оценить точность нахождения векторной величины \hat{x} , зная истинное значение x :

- Абсолютная погрешность $E_{\text{абс}}(\hat{x}) = \|\hat{x} - x\|$;
- Относительная погрешность $E_{\text{отн}}(\hat{x}) = \|\hat{x} - x\|/\|x\|$;

- Поэлементная относительная погрешность $\max_i \|\hat{x}_i - x_i\| / \|x_i\|$.

Однако, как видно из наших экспериментов, данные метрики не всегда дают корректное представление о точности алгоритма сингулярного разложения. Для матриц значительного размера, у которых $\sigma_{\min} \ll \sigma_{\max}$, абсолютная и относительная погрешности могут скрывать ошибки в нахождении большого количества малых сингулярных значений при достаточно точном отыскании нескольких больших. Наоборот, поэлементная относительная погрешность дает повышенную надежность, подчеркивая наихудший случай определения отдельного сингулярного значения, в то время как большая часть сингулярных значений может быть вычислена вполне корректно. В связи с этим, для оценки точности нахождения сингулярных значений введем следующий показатель:

$$\text{RMSRE} = \sqrt{\frac{1}{N} \sum_{i=1}^N \left(\frac{\sigma_i - \hat{\sigma}_i}{\sigma_i} \right)^2},$$

где N – количество сингулярных значений матрицы, σ_i – “истинное” i -е сингулярное значение, $\hat{\sigma}_i$ – i -е сингулярное значение, полученное с помощью численного алгоритма сингулярного разложения. Этот показатель является, по сути, среднеквадратичной относительной погрешностью нахождения сингулярных значений и позволяет оценивать точность нахождения как малых, так и больших сингулярных значений при значительном числе обусловленности матрицы, ослабляя описанные проблемы.

3.1. Конструирование матрицы с заданным спектром

Для исследования точности нахождения сингулярных значений, очевидно, необходимо знать “истинные” их значения для исходной матрицы. Для этого исходная тестовая матрица синтетически создается согласно уравнению (1) по следующему алгоритму [3]:

- 1) Задаются размерности матрицы m и n ;
- 2) Генерируются матрицы $T_L(m \times m)$ и $T_R(n \times n)$, в них каждый элемент t_{ij} – псевдослучайное число от -1 до 1, полученное из равномерного распределения генератора псевдослучайных чисел. Задание начального состояния генератора обеспечивает воспроизводимость экспериментов;
- 3) Матрицы T_L и T_R ортогонализуются с помощью преобразования Хаусхолдера [3], которое превращает их в ортогональные матрицы Q_L и Q_R соответственно;

- 4) Заданный спектр σ присваивается главной диагонали нулевой матрицы Σ , превращая ее в диагональную;
- 5) Тестовая матрица с заданным спектром получается как $A = Q_L \Sigma Q_R$.

3.2. Задание распределения сингулярных значений

Для задания распределения сингулярных значений в спектре используется плотность распределения $f_\sigma(x)$. Понятие плотности распределения здесь схоже с аналогичным из теории вероятности. Установим следующие требования для $f_\sigma(x)$ на интервале $[0, 1]$: $f_\sigma : [0, 1] \rightarrow \mathbb{R}^+$ и $\int_0^1 f_\sigma(x) dx = 1$. Спектр матрицы, соответствующий заданной плотности распределения, определяется следующим образом:

- 1) Из плотности распределения $f_\sigma(x)$ получаем функцию распределения: $F_\sigma(x) = \int_0^x f_\sigma(t) dt$;
- 2) Генерируем N равноотстоящих точек u_i на интервале $[0, 1]$, где N – требуемое количество сингулярных значений;
- 3) Получаем сингулярные значения с требуемым распределением с помощью метода обратного преобразования [14]:

$$\sigma_i = F_\sigma^{-1}(u_i).$$

Следует отметить, что, несмотря на использование аналогий из области теории вероятности, описанный процесс полностью детерминирован: при одинаковых исходных плотностях распределения $f_\sigma(x)$ всегда будет получен один и тот же набор сингулярных значений σ .

В качестве модели плотности распределения мы используем нормализованную бета-функцию [15]:

$$f_\sigma(x; \alpha, \beta) = \frac{1}{B(\alpha, \beta)} x^{\alpha-1} (1-x)^{\beta-1}, \quad B(\alpha, \beta) = \int_0^1 t^{\alpha-1} (1-t)^{\beta-1} dt. \quad (3)$$

Этот выбор связан с простотой параметризации и возможностью задавать различные интересующие нас распределения сингулярных значений, сгруппированные с разной плотностью в различных частях интервала $[0, 1]$. Полученные сингулярные значения на этом интервале проецируются на логарифмическую шкалу с заданными границами $[\sigma_{\min}, \sigma_{\max}]$, для получения выбранного числа обусловленности.

3.3. Библиотеки и алгоритмы сингулярного разложения

Вследствие широкой востребованности, реализации алгоритмов сингулярного разложения встречаются во многих пакетах численных методов. В классическом пакете LAPACK [16] имеются две процедуры для вычисления сингулярного разложения. По проведенному авторами анализу, многие другие широко используемые библиотеки численных методов (например, numpy [17], стандартные библиотеки языков Julia [18], R [19], Octave [20]) используют в своих имплементациях сингулярного разложения обращения к соответствующим функциям LAPACK. Одной из немногих широко распространенных библиотек с независимой от LAPACK реализацией SVD является Eigen для C++ [21]. Таким образом, для дальнейших экспериментов мы выделили три по нашему мнению наиболее часто используемых варианта метода сингулярного разложения: BDCSVD из Eigen, dgesvd и dgesdd из LAPACK.

4. Эксперименты

Пользуясь удобством параметризации бета-функции (3), задаем сетку параметров (α, β) в виде декартового произведения множеств выбранных значений для каждого из параметров: $\{0.5, 1, 2, 5\} \times \{0.5, 1, 2, 5\}$. Далее, используя эти функции, по методу, описанному в разделе 3.2, генерируются наборы сингулярных значений, распределение которых соответствуют заданным бета-функциям. Рассматриваются матрицы размером 3000×2000 с числом обусловленности 10^{20} , такие, что $\sigma_{\min} = 10^{-10}$, $\sigma_{\max} = 10^{10}$. Используемые бета-функции и соответствующие им гистограммы распределений сгенерированных наборов сингулярных значений приведены на рисунке 1. Для каждого из этих наборов создаются матрицы с заданным спектром, согласно методу из раздела 3.1. Далее к этим матрицам применяем три алгоритма сингулярного разложения, перечисленные в разделе 3.3, и вычисляем метрики: RMSRE и $E_{\text{отн}}$. Результаты, представленные в виде шести тепловых карт, приведены на рисунке 2. Каждая тепловая карта соответствует комбинации метрики погрешности и алгоритма сингулярного разложения. Каждая ячейка на тепловой карте отражает значение метрики погрешности, при этом положение ячейки соответствует положению спектра на рисунке 1.

5. Выводы

Во-первых, очевидна недостаточная информативность относительной погрешности $E_{\text{отн}}$: во всех случаях $E_{\text{отн}}$ пренебрежимо мала, исходя из чего можно было бы сделать вывод о точном нахождении сингулярных

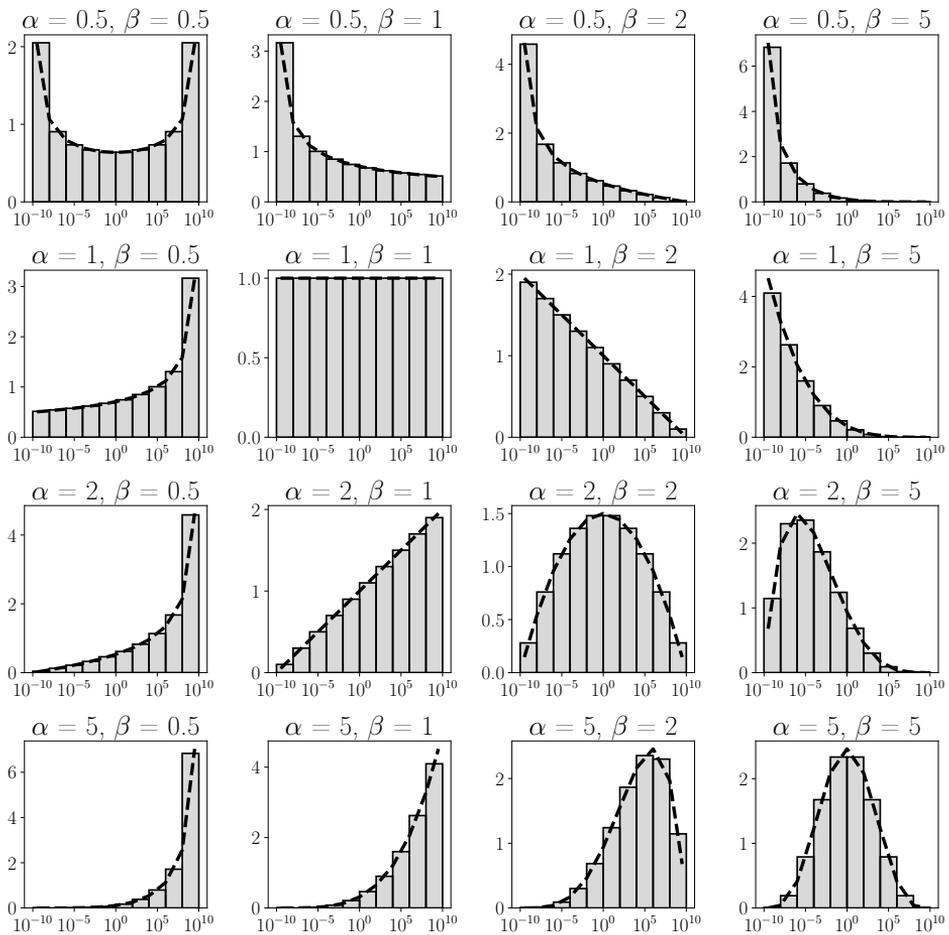


Рисунок 1. Распределение сингулярных значений для каждого из исследуемых случаев

значений. Однако, в метрике RMSRE видно, что точность нахождения сингулярных значений значительно различается. Во-вторых, имеется зависимость точности вычисления сингулярных значений от их распределения при фиксированных σ_{\min} и σ_{\max} . Метод BDCSVD, основанный на подходе “разделяй и властвуй” (который рекурсивно диагонализует матрицу и применяет метод Якоби для достаточно маленьких блоков), лучше всего показывает себя, если большинство сингулярных значений близки к σ_{\max} . Схожие результаты дает и dgesdd, также использующий принцип “разделяй и властвуй”. Методу dgesvd в метрике RMSRE соответствуют лучшие результаты при множестве сингулярных значений,

близких к σ_{\min} . Отличающиеся на порядок результаты в алгоритмах Eigen и LAPACK объясняются тем, что реализация Eigen принимает достаточно маленькие собственные значения за 0, что дает в итоге лучшую RMSRE. В целом, среди рассмотренных алгоритмов отметим следующую закономерность: собственные значения, близкие к σ_{\max} , находятся лучше, чем близкие к σ_{\min} . Также видно, что введенная нами метрика погрешности, хотя и дает более точное представление в сравнении с $E_{\text{отн}}$, несовершенна: например, при $(\alpha = 5, \beta = 0.5)$ и использовании метода dgesdd она сравнима по порядку с случаем $(\alpha = 0.5, \beta = 5)$. Однако, большинство значений для $(\alpha = 5, \beta = 0.5)$ находятся верно; лишь несколько малых сингулярных значений имеют очень большую относительную погрешность. Тем не менее, вклад ошибок нахождения этих малых значений в метрику RMSRE достаточен, чтобы сделать ее сопоставимой со случаем $(\alpha = 0.5, \beta = 5)$, в котором большая часть собственных значений находится неверно, но с меньшей относительной погрешностью.

Список литературы

- [1] Demmel J. et al., “Computing the Singular Value Decomposition with High Relative Accuracy”, *Linear Algebra and its Applications*, 1997, № 299, 21–80.
- [2] Cheney E.W., Kincaid D.R., *Numerical Mathematics and Computing*, Cengage Learning, 2012.
- [3] Golub G.H., Van Loan C.F., *Matrix Computations*, Johns Hopkins University Press, 2013.
- [4] Higham N.J., *Matrix Computations*, SIAM, 2002.
- [5] Markovsky I., *Low Rank Approximation: Algorithms, Implementation, Applications*, Springer-Verlag London Limited, 2012.
- [6] Eckart C., Young J.M., “The approximation of one matrix by another of lower rank”, *Psychometrika*, **1**, 211–218.
- [7] Mirsky L., “Symmetric gauge functions and unitarily invariant norms”, *Quarterly Journal of Mathematics*, **11** (1960), 50–59.
- [8] Jolliffe I. T., Cadima J., “Principal component analysis: a review and recent developments”, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, **374**:2065 (2016), 20150202.

- [9] Alakkari S., Dingliana J., “Principal Component Analysis Techniques for Visualization of Volumetric Data”, *Advances in Principal Component Analysis: Research and Development*, Springer Singapore, 2018, 99–120.
- [10] Navarrete P., Javier R., “Analysis and Comparison of Eigenspace-Based Face Recognition Approaches”, *Int. J. Pattern Recognit. Artif. Intell.*, **16** (2002), 817–830.
- [11] Markovsky I., Willems J.C., Huffel S., De Moor B., Pintelon R., “Application of structured total least squares for system identification and model reduction”, *IEEE Transactions on Automatic Control*, **50** (2005), 1490-1500.
- [12] Landauer T. K., Dumais S.T., “Latent semantic analysis”, *Scholarpedia*, **3** (2004), = 4356.
- [13] Kumar N.K., Shneider J., “Literature survey on low rank approximation of matrices”, 2016, arXiv: <https://arxiv.org/abs/1606.06511>.
- [14] Бусленко Н.П., Голенко Д.И., Соболев И.М., Срагович В.Г., Шрейдер Ю.А., *Метод статистических испытаний (Метод Монте-Карло)*, Физматгиз, М., 1962.
- [15] Abramowitz, M. and Stegun, I.A., *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*, Dover Publications, 1965.
- [16] Anderson E. et al., *LAPACK Users' Guide*, SIAM, 1999.
- [17] Harris C.R., Millman K.J. et al., “Array programming with NumPy”, **585:7825** (2020), 357–362.
- [18] Bezanson J., Edelman A., Karpinski S., Shah V.B., “Julia: A fresh approach to numerical computing”, **59:1** (2020), 65–98.
- [19] R Core Team, *R: A Language and Environment for Statistical Computing*, <https://www.R-project.org/>, 2020.
- [20] Eaton J.W., Bateman D., Hauberg S., Wehbring R., *GNU Octave version 5.2.0 manual: a high-level interactive language for numerical computations*, <https://www.gnu.org/software/octave/doc/v5.2.0/>, 2020.
- [21] Guennebaud G., Jacob B. et al., *Eigen v3*, <http://eigen.tuxfamily.org>, 2010.

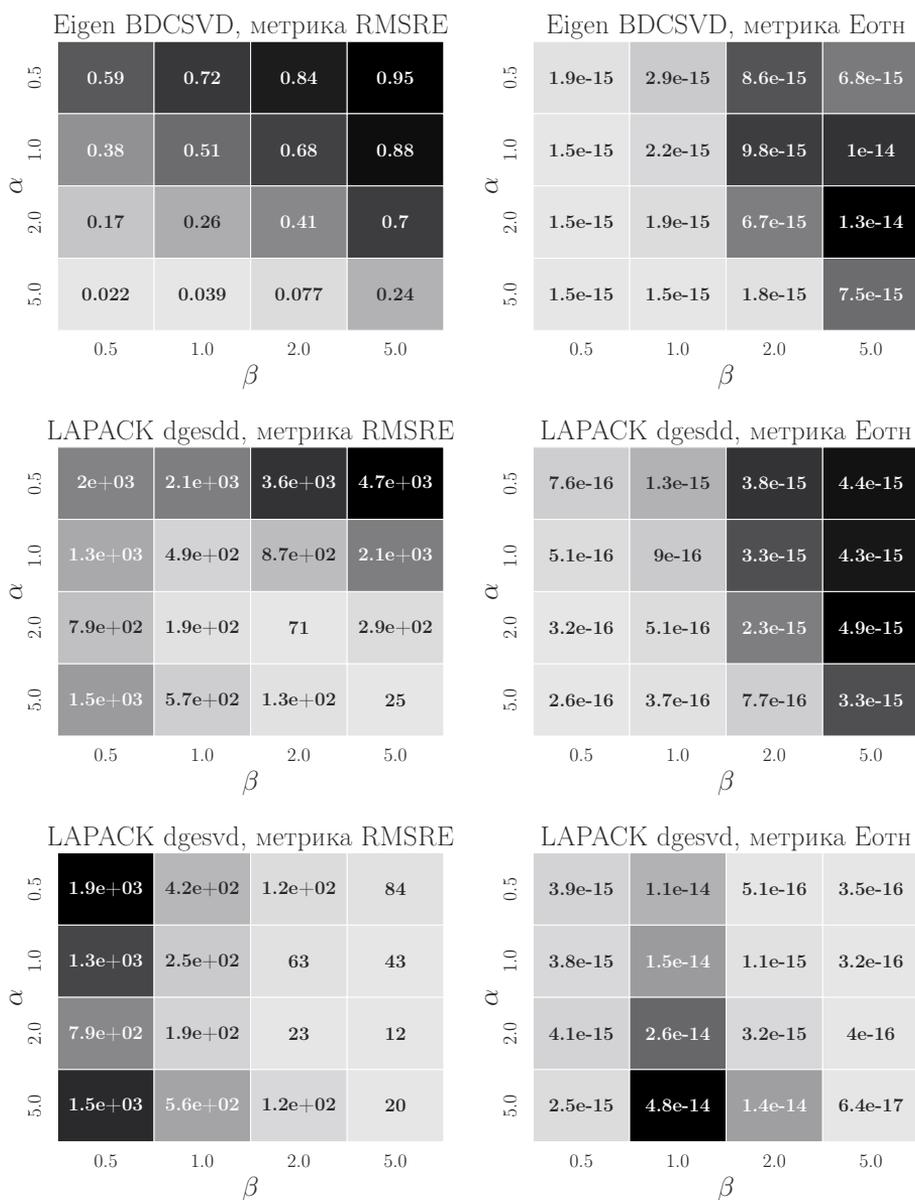


Рисунок 2. Распределение сингулярных значений для каждого из исследуемых случаев

Relationship between accuracy of singular value decomposition and distribution of singular values

Drozdov I.Yu., Parfenov D.V.

Using numerical experiments we demonstrated that accuracy of numerical singular value decomposition (SVD) is affected not only by condition number of the matrix, but also by distribution of singular values in the matrix spectrum. We note that widely used relative norm error of SVD result might be insufficient and propose an alternative metric based on root-mean-squared relative error.

Keywords: singular value decomposition, SVD, condition number, matrix spectrum, numerical stability

Список литературы

- [1] Demmel J. et al., “Computing the Singular Value Decomposition with High Relative Accuracy”, *Linear Algebra and its Applications*, 1997, № 299, 21–80.
- [2] Cheney E.W., Kincaid D.R., *Numerical Mathematics and Computing*, Cengage Learning, 2012.
- [3] Golub G.H., Van Loan C.F., *Matrix Computations*, Johns Hopkins University Press, 2013.
- [4] Higham N.J., *Matrix Computations*, SIAM, 2002.
- [5] Markovsky I., *Low Rank Approximation: Algorithms, Implementation, Applications*, Springer-Verlag London Limited, 2012.
- [6] Eckart C., Young J.M., “The approximation of one matrix by another of lower rank”, *Psychometrika*, **1**, 211–218.
- [7] Mirsky L., “Symmetric gauge functions and unitarily invariant norms”, *Quarterly Journal of Mathematics*, **11** (1960), 50–59.
- [8] Jolliffe I. T., Cadima J., “Principal component analysis: a review and recent developments”, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, **374**:2065 (2016), 20150202.
- [9] Alakkari S., Dingliana J., “Principal Component Analysis Techniques for Visualization of Volumetric Data”, *Advances in Principal Component Analysis: Research and Development*, Springer Singapore, 2018, 99–120.

- [10] Navarrete P., Javier R., “Analysis and Comparison of Eigenspace-Based Face Recognition Approaches”, *Int. J. Pattern Recognit. Artif. Intell.*, **16** (2002), 817–830.
- [11] Markovsky I., Willems J.C., Huffel S., De Moor B., Pintelon R., “Application of structured total least squares for system identification and model reduction”, *IEEE Transactions on Automatic Control*, **50** (2005), 1490-1500.
- [12] Landauer T. K., Dumais S.T., “Latent semantic analysis”, *Scholarpedia*, **3** (2004), = 4356.
- [13] Kumar N.K., Shneider J., “Literature survey on low rank approximation of matrices”, 2016, arXiv: <https://arxiv.org/abs/1606.06511>.
- [14] Buslenko N.P, Golenko D.I., Sobol I.M, Sragovich V.G., Shreider Yu.A., *Method of statistical trials (Monte-Carlo method)*, Fizmatgiz, Moscow, 1962 (In Russian).
- [15] Abramowitz, M. and Stegun, I.A., *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*, Dover Publications, 1965.
- [16] Anderson E. et al., *LAPACK Users’ Guide*, SIAM, 1999.
- [17] Harris C.R., Millman K.J. et al., “Array programming with NumPy”, **585**:7825 (2020), 357–362.
- [18] Bezanson J., Edelman A., Karpinski S., Shah V.B., “Julia: A fresh approach to numerical computing”, **59**:1 (2020), 65–98.
- [19] R Core Team, *R: A Language and Environment for Statistical Computing*, <https://www.R-project.org/>, 2020.
- [20] Eaton J.W., Bateman D., Hauberg S., Wehbring R., *GNU Octave version 5.2.0 manual: a high-level interactive language for numerical computations*, <https://www.gnu.org/software/octave/doc/v5.2.0/>, 2020.
- [21] Guennebaud G., Jacob B. et al., *Eigen v3*, <http://eigen.tuxfamily.org>, 2010.

Часть 2.
Специальные вопросы теории
интеллектуальных систем

О выразительных возможностях ансамблей решающих деревьев

А. П. Соколов¹, Л. А. Прохоренкова²

Решающие деревья широко применяются в машинном обучении, статистике и анализе данных. Предиктивные модели, основанные на решающих деревьях, показывают отличные результаты в терминах точности и времени обучения, особенно на гетерогенных табличных датасетах. Производительность, простота и надежность делают это семейство алгоритмов одним из наиболее популярных в машинном обучении и науке о данных.

Одним из важных гиперпараметров алгоритмов, основанных на решающих деревьях, является максимальная глубина.

В данной работе получен теоретический результат, который показывает как ограничение на максимальную глубину решающих деревьев влияет на выразительные возможности всего ансамбля. Этот результат применим к таким алгоритмам, как одиночное решающее дерево (Decision Tree), случайный лес (Random Forest), градиентный бустинг (GBDT) и другие.

Ключевые слова: машинное обучение, наука о данных, решающее дерево, случайный лес, градиентный бустинг.

1. Введение

Решающие деревья широко применяются в машинном обучении, статистике и анализе данных. Предиктивные модели, основанные на решающих деревьях, показывают отличные результаты в терминах точности и времени обучения, особенно на гетерогенных табличных датасетах ([1]). Производительность, простота и надежность делают это семейство алгоритмов одним из наиболее популярных в машинном обучении и науке о данных ([2]).

Одним из важных гиперпараметров алгоритмов, основанных на решающих деревьях, является максимальная глубина.

В данной работе получен теоретический результат, который показывает как ограничение на максимальную глубину решающих деревьев

¹ *Соколов Андрей Павлович* — к.ф.-м.н., м.н.с. каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: sokolov@intsys.msu.ru

Sokolov Andrey Pavlovich — junior scientific researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

² *Прохоренкова Людмила Александровна* — д.ф.-м.н., исследователь, Яндекс, e-mail: ostroumova-la@yandex.ru

Prokhorenkova Liudmila Alexandrovna — researcher, Yandex.

влияет на выразительные возможности всего ансамбля. Этот результат применим к таким алгоритмам, как одиночное решающее дерево (Decision Tree), случайный лес (Random Forest), градиентный бустинг (GBDT) и другие.

2. Определения и основной результат

Предположим задан датасет из n примеров по m признаков.

$$D = \{(X_i, y_i) \mid i \in \{1, \dots, n\}, X_i \in \mathbb{R}^m, y_i \in \mathbb{R}\}.$$

В задачах машинного обучения обычно X_i называется *вектором признаков*, а y_i – *значением*.

Будем использовать обозначение $D(X) = y$, где $(X, y) \in D$.

Задача регрессии в машинном обучении обычно ставится следующим образом: необходимо найти такую функцию $\Phi : \mathbb{R}^m \rightarrow \mathbb{R}$, которая бы минимизировала некоторую функцию потерь \mathcal{L} на датасете D . Функция Φ называется *моделью*.

В данной работе для простоты мы намеренно не рассматриваем вопросы, связанные с обобщающей способностью модели. Поэтому мы не разбиваем датасет на обучающую и валидационную выборки, как это принято при решении прикладных задач машинного обучения. Единственный вопрос, который мы поднимаем, – насколько точно может описывать датасет модель, основанная на ансамбле решающих деревьев.

Обычно функция потерь (лосс-функция) \mathcal{L} может быть представлена как сумма элементарных функций потерь на отдельных примерах $\mathcal{L}(D, \Phi) = \sum_{i=1}^n l(D(X_i), \Phi(X_i))$, где $l : \mathbb{R}^2 \rightarrow \mathbb{R}$ – элементарная функция потерь. В данной работе мы рассматриваем только такие лосс-функции, которые могут быть представлены как сумма элементарных функций потерь на индивидуальных примерах.

Различные элементарные функции потерь используются на практике: L_1 , L_2 и другие. В данной статье мы будем рассматривать только такие элементарные функции потерь l , для которых $l(a, b) = 0 \iff a = b$. Для таких функций потерь $\mathcal{L}(D, \Phi) = 0$ тогда и только тогда, когда $D(X_i) = \Phi(X_i)$ для всех $i \in \{1, \dots, n\}$, и $\mathcal{L}(D, \Phi) > 0$ если существует такое $i \in \{1, \dots, n\}$, что $D(X_i) \neq \Phi(X_i)$.

Будем говорить, что модель Φ *идеально аппроксимирует* датасет D , тогда и только тогда, когда $\mathcal{L}(\Phi, D) = 0$. Идеальная аппроксимация означает, что выход модели $\Phi(X_i)$ равен истинному значению y_i на всех примерах X_i из датасета.

Ансамбль Φ из k деревьев имеет вид $\Phi(X) = \sum_{i=1}^k t_i(X)$, $t_i \in \mathbb{T}$, где t_i – индивидуальные решающие деревья из множества всех возможных решающих деревьев – \mathbb{T} .

Решающее дерево t работает следующим образом. Входной вектор подается на корневую вершину дерева. Каждая внутренняя вершина s содержит предикат вида $p_s(X) = (x_{i_s} \geq r_s)$, где x_{i_s} – компонента вектора признаков с индексом i_s , а r_s – некоторое пороговое значение, ассоциированное с вершиной. Предикаты внутренних вершин дерева последовательно решают, куда должен спускаться вектор признаков X . В конце концов X спускается до листа дерева с индексом q и весом w_q . Этот вес определяет выходное значение дерева на данном векторе признаков, то есть $t(X) = w_q$.

Максимальная глубина дерева d определяет максимальную длину пути (число внутренних вершин с предикатами), который ведет от корневой вершины к листу. Заметим, что максимальное число листьев N решающего дерева и максимальная глубина d связаны соотношением $N \leq 2^d$.

Видно, что каждое решающее дерево t максимальной глубины d задает кусочно-константную функцию, которая отображает \mathbb{R}^m в \mathbb{R} . При этом число константных областей в пространстве признаков ограничено сверху как 2^d . Следовательно, каждое решающее дерево t может быть представлено следующим образом $t(X) = \sum_{q=1}^{N_t} I_q(X) \cdot w_q$, где q пробегает N_t листьев дерева t , $I_q(X)$ – индикаторная функция листа с индексом q

$$I_q(X) = \begin{cases} 1, & \text{если } X \text{ принадлежит листу } q; \\ 0, & \text{иначе;} \end{cases}$$

$w_q \in \mathbb{R}$ – вещественные веса, ассоциированные с листьями дерева.

Каждая индикаторная функция $I_q(X)$ принимает значение 1 в области пространства признаков, которая определена набором не более, чем из d ограничений вида $a_i \leq x_i \leq b_i$, где $a_i, b_i \in \mathbb{R} \cup \{-\infty, +\infty\}$. Обозначим множество таких индикаторных функций как \mathbb{I}_d .

Имеет место следующее утверждение.

Теорема. *Для всякого $d > 1$ существует датасет D_d такой, что:*

- 1) *он не может быть идеально аппроксимирован никаким ансамблем решающих деревьев Φ с максимальной глубиной $(d - 1)$;*
- 2) *он может быть идеально аппроксимирован одним решающим деревом t глубины d .*

Доказательство. Для начала рассмотрим представление решающего дерева t с помощью его индикаторных функций $t(X) = \sum_{q=1}^{N_t} I_q(X) \cdot w_q$.

Следовательно, всякий ансамбль Φ может быть представлен следующим образом $\Phi(X) = \sum_{q=1}^{N_\Phi} I_q(X) \cdot w_q$, где N_Φ – общее число листьев в ансамбле Φ . Обозначим $\Phi(X) = \sum_{q=1}^{N_\Phi} \Phi_q(X)$, где $\Phi_q(X) = I_q(X) \cdot w_q$ – элементарная предиктивная функция, реализуемая листом q одного из деревьев ансамбля.

Заметим, что каждая индикаторная функция решающего дерева с максимальной глубиной $(d-1)$ может быть представлена следующим образом $I_q(X) = \bigwedge_{i=1}^{d-1} p_{s_i}^{\sigma_{s_i}}(X)$, где $\&$ – операция конъюнкции (логическое «И»), вершины s_1, \dots, s_{d-1} соответствуют пути в дереве от корня до листа q и

$$p_{s_i}^{\sigma_{s_i}} = \begin{cases} p_{s_i}, & \sigma_{s_i} = 1; \\ \bar{p}_{s_i}, & \text{иначе.} \end{cases}$$

Здесь \bar{p}_{s_i} означает логическое отрицание p_{s_i} . Также $\sigma_{s_i} = 1$ если соответствующий предикат в вершине s_i равен 1 и $\sigma_{s_i} = 0$ иначе.

Теперь мы можем построить датасет, который не может быть аппроксимирован никаким ансамблем с деревьями максимальной глубины $(d-1)$. Рассмотрим булеву функцию $f(x_1, \dots, x_d) = \sum_{i=1}^d x_i$, где используется сложение по модулю 2. Положим

$$D_d = \left\{ (x_1, \dots, x_d, -1) \mid (x_1, \dots, x_d) \in \{0, 1\}^d, f(x_1, \dots, x_d) = 0 \right\} \cup \\ \left\{ (x_1, \dots, x_d, +1) \mid (x_1, \dots, x_d) \in \{0, 1\}^d, f(x_1, \dots, x_d) = 1 \right\}.$$

Запишем все значения в датасете D_d в единый вектор Y длины 2^d . Обозначим $Y(x_1, \dots, x_d) = y$ для всякого вектора $(x_1, \dots, x_d, y) \in D_d$. Далее выпишем в таком же порядке значения, предсказанные ансамблем Φ на примерах из датасета, и получим вектор Φ . Аналогичным образом введем в рассмотрение Φ_q – вектор предсказаний q -го листа ансамбля на всех примерах датасета D . Заметим, что D_d содержит элементы для всех возможных наборов признаков (x_1, \dots, x_d) и, таким образом, его размер равен 2^d . Далее, $Y(x_1, \dots, x_j, \dots, x_d) = -Y(x_1, \dots, \bar{x}_j, \dots, x_d)$ для всякого $j \in \{1, \dots, d\}$. Заметим, что мы можем применить логическое отрицание к признакам, потому что они принадлежат множеству $\{0, 1\}$. Рассмотрим скалярное произведение $\langle Y, \Phi \rangle$ в евклидовом пространстве размерности 2^d . Если ансамбль Φ идеально аппроксимирует D_d , тогда $\langle Y, \Phi \rangle = \|Y\|^2$. Следовательно, если $\langle Y, \Phi \rangle \neq \|Y\|^2$,

то Φ аппроксимирует D_d не идеальным образом. Обратим внимание, что $\Phi = \sum_{q=1}^{N_\Phi} \Phi_q$, где Φ_q соответствует вектору длины 2^d , который равен w_q на тех позициях, где индикаторная функция I_q принимает значение 1. На других позициях вектор Φ_q равен нулю. Следовательно, $\langle Y, \Phi \rangle = \sum_{q=1}^{N_\Phi} \langle Y, \Phi_q \rangle$. Заметим, что индикаторная функция $I_q \in \mathbb{I}_{d-1}$ может быть представлена как конъюнкция предикатов размера $(d-1)$, следовательно, она существенно зависит не более, чем от $(d-1)$ признака. Таким образом, для каждой индикаторной функции I_q найдется хотя бы одна переменная x_i такая, что I_q не зависит от нее существенным образом. То есть $I_q(x_1, \dots, x_j, \dots, x_d) = I_q(x_1, \dots, \bar{x}_j, \dots, x_d)$. Следовательно, для каждого листа $q \in \{1, \dots, N_\Phi\}$ найдется такое $j \in \{1, \dots, d\}$, что $\Phi_q(x_1, \dots, x_j, \dots, x_d) = \Phi_q(x_1, \dots, \bar{x}_j, \dots, x_d)$. В то же время, как было показано ранее, $Y(x_1, \dots, x_j, \dots, x_d) = -Y(x_1, \dots, \bar{x}_j, \dots, x_d)$. Из этого наблюдения следует, что $\langle Y, \Phi_q \rangle = 0$ для всякого листа ансамбля q . Следовательно $\langle Y, \Phi \rangle = 0$ для каждого ансамбля максимальной глубины $(d-1)$.

Теперь построим одно решающее дерево глубины d , которое будет идеально аппроксимировать D_d . В корневую вершину s_1 поместим предикат $p_{s_1}(X) = (x_1 \geq 0.5)$. Во всех вершинах, находящихся на глубине i в дереве, разместим предикаты $p_i(X) = (x_i \geq 0.5)$. Очевидно, что 2^d листьев построенного таким образом решающего дерева будут содержать все 2^d примеров датасета D_d . Теперь осталось лишь присвоить веса листьям в соответствии со значениями из датасета D_d . Таким образом построенное решающее дерево идеально аппроксимирует датасет D_d . Теорема доказана.

3. Заключение

В данной работе мы доказали, что произвольный ансамбль решающих деревьев максимальной глубины $(d-1)$ имеет меньшие выразительные возможности, чем одно решающее дерево глубины d .

Одним из следствий этого результата, которое имеет важное значение для прикладных задач машинного обучения, является то, что мы не можем компенсировать недостаток глубины решающих деревьев увеличением их количества в ансамбле.

4. Благодарности

Авторы выражают благодарность Сергею Иванову, Леониду Литовченко и Станиславу Моисееву за ряд ценных замечаний по данной работе.

Список литературы

- [1] Vadim Borisov and Tobias Leemann and Kathrin Seßler and Johannes Haug and Martin Pawelczyk and Gjergji Kasneci, “Deep Neural Networks and Tabular Data: A Survey”, *CoRR*, **abs/2110.01889** (2021), <https://arxiv.org/abs/2110.01889>.
- [2] Iqbal H Sarker, “Machine Learning: Algorithms, Real-World Applications and Research Directions”, *SN Comput Sci.*, **2(3)** (2021), 10.1007/s42979-021-00592-x.

On The Expressive Power of Decision Tree Ensembles Sokolov A.P., Prokhorenkova L.A.

Decision trees are widely used in machine learning, statistics and data mining.

Predictive models based on decision trees show outstanding results in terms of accuracy and training time. Especially on heterogeneous tabular datasets. Performance, simplicity and integrity make this family of algorithms one of the most popular in data science.

One important hyper-parameter of decision tree training algorithms is maximum depth of the trees.

This paper proves theoretical result that shows how maximum depth of decision trees limits the expressive power of ensemble. This result is applicable to such tree based algorithms as plain Decision Tree, Random Forest, GBDT and others.

Keywords: machine learning, data science, decision tree, random forest, gradient boosting.

References

- [1] Vadim Borisov and Tobias Leemann and Kathrin Seßler and Johannes Haug and Martin Pawelczyk and Gjergji Kasneci, “Deep Neural Networks and Tabular Data: A Survey”, *CoRR*, **abs/2110.01889** (2021), <https://arxiv.org/abs/2110.01889>.
- [2] Iqbal H Sarker, “Machine Learning: Algorithms, Real-World Applications and Research Directions”, *SN Comput Sci.*, **2(3)** (2021), 10.1007/s42979-021-00592-x.

Графы ортогональности матриц над коммутативными кольцами

О. Г. Стырт^{1 2}

Работа посвящена исследованию графа ортогональности кольца матриц над коммутативным кольцом. Доказано, что граф ортогональности кольца матриц размера более 1 над коммутативным нецелостным кольцом связан и имеет диаметр 3 либо 4; получен критерий для каждого из значений. Также доказано, что любая его вершина удалена от некоторой скалярной матрицы не более, чем на 2.

Ключевые слова: ассоциативное кольцо с единицей, коммутативное кольцо, делитель нуля, кольцо матриц, граф делителей нуля, граф ортогональности.

1. Введение

В современной математике важное место занимает изучение свойств ассоциативных колец в терминах графов некоторых алгебраических бинарных отношений, возникающих естественным образом. Так, *граф делителей нуля* был впервые определён в 1986 г. И. Беком [1] для коммутативного кольца. Его вершинами были все делители нуля, а рёбра проводились в точности между всеми парами различных элементов с нулевым произведением. Однако с 1999 г. используется более удобная его интерпретация, которую ввели Д. Андерсон и Ф. Ливингстон в работе [2], исключив нулевой элемент кольца из множества его вершин. Также в ней доказано, что граф делителей нуля коммутативного кольца связан и имеет диаметр не более трёх; в прежней трактовке графа данные утверждения были бы бессодержательными. В ряде дальнейших работ также изучаются различные характеристики графа делителей нуля: центр и радиус [8], вопросы планарности [4] и однозначности восстановления кольца по графу

¹ *Стырт Олег Григорьевич* — доцент каф. дискретной математики Физтех-школы прикладной математики и информатики МФТИ, e-mail: oleg_styrt@mail.ru.

Styrt Oleg Grigoryevich — associate professor, MIPT, The Phystech School of Applied Mathematics and Computer Science, Chair of Discrete Mathematics.

² *Исследование выполнено при поддержке Министерства науки и высшего образования Российской Федерации (госзадание) №075-00337-20-03, номер проекта 0714-2020-0005.*

The research is supported by the Ministry of Science and Higher Education of the Russian Federation (Goszadaniye) 075-00337-20-03, project No. 0714-2020-0005.

с точностью до изоморфизма [3, 5]. Для некоммутативных колец имеется несколько разновидностей графов, определённых делителями нуля:

Название	Ориентация рёбер	Вершины	Ребро из x в y	См.
Ор. граф делителей нуля	есть	1- и 2-стор. делители нуля	$xy = 0$	[6, 7]
(Неор.) граф делителей нуля	нет	Ненулевые 1- и 2-стор. делители нуля	$(xy = 0) \vee (yx = 0)$	[7]
Граф ортогональности	нет	Ненулевые двустор. делители нуля	$(xy = 0) \wedge (yx = 0)$	[9, 10]

Основные имеющиеся к текущему моменту результаты для графов ортогональности некоммутативных колец относятся прежде всего к матричным кольцам. Так, в случае, если основное кольцо является телом, получены следующие свойства графа ортогональности кольца $(n \times n)$ -матриц: при $n = 2$ он несвязен, и все его связные компоненты имеют диаметры не более 2, а при $n \geq 3$ он связан и имеет диаметр 4. Эти утверждения доказаны в 2014 г. для поля [9], а позднее, в 2017 г. — для произвольного тела [10]; их также легко обобщить на целостные кольца (путём перехода к полю частных).

В данной же работе изучен граф ортогональности кольца матриц над коммутативным нецелостным кольцом и доказаны следующие основные результаты.

Теорема 1. Пусть R — коммутативное кольцо с множеством делителей нуля $Z_R \neq \{0\}$. Тогда для любого $n > 1$ граф ортогональности кольца $(n \times n)$ -матриц над R связан и имеет диаметр 3 либо 4, причём значение 3 равносильно соотношению

$$\forall a_0 \in Z_R \quad \exists a_1, a_2 \in R \setminus \{0\} \quad \forall i, j \in \{0, 1, 2\}, i \neq j: \quad a_i a_j = 0, \quad (1)$$

а каждая его вершина удалена от некоторой скалярной матрицы не более, чем на 2.

Теорема 2. Пусть r — радиус графа в условиях теоремы 1. Тогда

- 1) $2 \leq r \leq 4$;
- 2) если выполнено (1), то $r \in \{2; 3\}$;

3) $r = 2$, если и только если найдётся элемент $c \in R \setminus \{0\}$, такой что

$$\forall a \in Z_R \quad \text{Ann}(c) \cap \text{Ann}(a) \neq 0. \quad (2)$$

2. Вспомогательные соглашения

В работе будут использованы следующие обозначения и соглашения.

1) Теоретико-множественные:

- При перечислении элементов неупорядоченного набора (или множества) используются фигурные скобки. Элементы же упорядоченного набора перечисляются в круглых скобках и могут повторяться.
- $D^n := \underbrace{D \times \dots \times D}_n$ — n -я декартова степень множества D .

2) Общие алгебраические:

- Все рассматриваемые кольца предполагаются ассоциативными и с единицей.
- R — произвольное кольцо.
- Для произвольного подмножества $D \subset R$ положим $D^* := D \setminus \{0\}$. В частности, через R^* обозначается подмножество всех ненулевых (необязательно обратимых, как в общепринятой интерпретации) элементов R .
- Идеал в R *собственный*, если он не равен R .
- $M_{m \times n}(R)$ — R -модуль $(m \times n)$ -матриц над R ; $M_n(R)$ — кольцо $M_{n \times n}(R)$. Если в скобках вместо кольца указывается некоторое его подмножество D , то такая запись означает подмножество всех матриц с элементами из D .
- 0_n^m — нулевая $(m \times n)$ -матрица; $0_n := 0_n^n$; E_n — единичная $(n \times n)$ -матрица; J_r — жорданова клетка размера r с собственным значением 0. Если размеры матрицы ясны из контекста, то индексы могут опускаться.
- E_{kl} — матричная единица (a_{ij}) , $a_{ij} := \delta_{ki}\delta_{lj}$.
- Для квадратной матрицы A над коммутативным кольцом: \tilde{A} — матрица её алгебраических дополнений; $\hat{A} := (\tilde{A})^T$.
- Если $A = (a_{k_1, k_2}) \in M_{n_1 \times n_2}(R)$, $P_i \in \{1, \dots, n_i\}^{m_i}$ ($i = 1, 2$), то $A_{P_2}^{P_1}$ — матрица $(b_{l_1, l_2}) \in M_{m_1 \times m_2}(R)$, $b_{l_1, l_2} := a_{k_1(l_1), k_2(l_2)}$, где

$k_i(l_i)$ — l_i -й элемент P_i . Если ни в P_1 , ни в P_2 числа не повторяются, то $A_{P_2}^{P_1}$ есть подматрица A с номерами строк и столбцов из P_1 и P_2 соответственно.

3) По видам делителей нуля:

- Элемент $a \in R$ называется
 - *левым* (соотв. *правым*) *делителем нуля*, если найдётся элемент $b \in R^*$, такой что $ab = 0$ (соотв. $ba = 0$);
 - *делителем нуля*, если он является левым либо правым делителем нуля;
 - *двусторонним делителем нуля*, если он является одновременно левым и правым делителем нуля.

При этом

- в коммутативном кольце понятия всех видов делителей нуля равносильны;
- нуль есть двусторонний делитель нуля; если других делителей нуля нет, то R называют *кольцом без делителей нуля*.
- *Целостное кольцо* — коммутативное кольцо без делителей нуля.

4) Из общей теории графов:

- Все рассматриваемые графы предполагаются неориентированными.
- $\Gamma = (V, E)$ — произвольный граф; V и E — множества его вершин и рёбер соответственно. При этом можно (и зачастую удобно) задавать E при помощи симметричного бинарного отношения на V .
- Две вершины *смежны*, если они соединены ребром.
- *Подграф* — граф с множеством вершин $V' \subset V$ и, если не оговорено противное, с прежним бинарным отношением, ограниченным на V' .
- *Путь* — последовательность вершин, из которых любые две соседних вершины смежны.
- *Длина пути* — число его рёбер.
- *Расстояние* между вершинами v и w (обозн. $d(v, w)$) — наименьшая длина соединяющего их пути; при его отсутствии полагаем $d(v, w) := +\infty$; знак в данном контексте очевиден и поэтому будет опускаться. Ясно, что $(d(v, w) = 0) \Leftrightarrow (v = w)$.

- *Расстояние* от вершины v до подмножества $W \subset V$ (обозн. $d(v, W)$) — число $\min\{d(v, w) : w \in W\}$.
- $d(v) := \sup\{d(v, w) : w \in V\}$ ($v \in V$).
- *Диаметр* Γ — число $\text{diam}(\Gamma) := \sup\{d(v, w) : v, w \in V\} = \max\{d(v) : v \in V\}$.
- *Радиус* Γ — число $\text{rad}(\Gamma) := \min\{d(v) : v \in V\}$. Ясно, что

$$\text{rad}(\Gamma) \leq \text{diam}(\Gamma) \leq 2 \cdot \text{rad}(\Gamma). \quad (3)$$

- Граф *связен*, если любые две его вершины можно соединить путём.

Замечание 1. Легко видеть, что граф с конечным диаметром *связен*. Обратное неверно; пример — множество натуральных чисел с отношением соседства.

5) По специальным графам в алгебраических структурах:

- $O(R)$ — граф ортогональности кольца R (для коммутативного кольца это не что иное как граф делителей нуля).
- Вершинами $O(R)$ служат все ненулевые двусторонние делители нуля кольца R ; соотношение ортогональности ($xy = yx = 0$) записывается как $(x \perp y)$; $O_R(x)$ — множество всех вершин, ортогональных x .

3. Доказательства результатов

Рассмотрим произвольное коммутативное кольцо R . Через $\text{Ann}(a)$ ($a \in R$) обозначим идеал $\{x \in R : ax = 0\}$, через Z_R — множество $\{a \in R : \text{Ann}(a) \neq 0\}$ всех делителей нуля. Пусть, далее, S — кольцо $M_n(R)$ ($n > 1$). Посредством естественного вложения колец $R \hookrightarrow S$, $a \rightarrow aE$ отождествим R с подкольцом $RE \subset S$ (и, таким образом, $O(R)$ — с подграфом графа $O(S)$). Для $A \in S$ положим $I_A := \text{Ann}(\det A) \triangleleft R$.

Граф $O(R)$ *связен* и имеет диаметр не более 3 (см. теорему 2.3 в [2, § 2]). Кроме того, если R — тело, то

- 1) при $n = 2$ граф $O(S)$ *несвязен*, и все его *связные* компоненты имеют диаметры ≤ 2 ;
- 2) при $n \geq 3$ граф $O(S)$ *связен* и имеет диаметр 4.

Эти результаты получены в [9, § 4] для полей (лемма 4.1 и теорема 4.5 соответственно), а в [10, § 2] обобщены на произвольные тела (лемма 2.2 и теорема 2.1 соответственно). Переносятся они и на целостные кольца (путём перехода к полю частных).

Теорема 3. Для любых матрицы $A \in S$ и собственного идеала $I \triangleleft R$, содержащего $\det A$, найдётся матрица $B \in S \setminus (M_n(I))$, такая что $AB, BA \in M_n(I)$.

Доказательство. Положим $Q_m := \{1, \dots, m\}$ и $P_m := (1, \dots, m) \in \mathbb{N}^m$ ($m \in \mathbb{N}$).

Рассмотрим всевозможные тройки (k, P', P'') ($k \geq 0$, $P', P'' \in (Q_n)^k$), удовлетворяющие соотношению $\det(A_{P''}^{P'}) \notin I$. Для любой из них ни в P' , ни в P'' нет повторяющихся чисел и, согласно условию, $k < n$. Кроме того, по крайней мере одна такая тройка существует: для $k := 0$ и пустых наборов P', P'' соответствующая (0×0) -матрица имеет определитель $1 \notin I$. Значит, мы можем фиксировать одну из этих троек с наибольшим возможным k , и тогда $0 \leq k < n$, $m := k + 1 \in Q_n$.

Случай 1). $P' = P'' = P_k$.

По построению $\det(A_{P_k}^{P_k}) \notin I$. Далее, положим $C := A_{P_m}^{P_m} \in M_m(R)$,

$$B := \begin{pmatrix} \widehat{C} & 0_{n-m}^m \\ 0_m^{n-m} & 0_{n-m} \end{pmatrix} \in S.$$

Тогда $b_{m,m} = \det(A_{P_k}^{P_k}) \notin I$, откуда $B \notin M_n(I)$. Покажем, что $AB, A^T B^T \in M_n(I)$, т. е. что для любых $p, q \in Q_n$ матричные элементы $(AB)_{p,q}$ и $(A^T B^T)_{p,q}$ лежат в I . Будем считать, что $p \in Q_n$ и $q \in Q_m$ (иначе $(AB)_{p,q} = (A^T B^T)_{p,q} = 0$). Пусть $P \in (Q_n)^m$ — набор, полученный из P_m заменой q -го элемента на p . Ввиду максимальной k , а также неравенства $m > k$, имеем $\det(A_{P_m}^P), \det(A_{P^m}^P) \in I$,

$$\begin{aligned} (AB)_{p,q} &= \sum_{i \in Q_n} (a_{p,i} b_{i,q}) = \sum_{i \in Q_m} (a_{p,i} (\widehat{C})_{i,q}) = \sum_{i \in Q_m} (a_{p,i} (\widetilde{C})_{q,i}) = \det(A_{P_m}^P) \in I; \\ (A^T B^T)_{p,q} &= \sum_{i \in Q_n} ((A^T)_{p,i} (B^T)_{i,q}) = \sum_{i \in Q_m} (a_{i,p} (\widetilde{C})_{i,q}) = \det(A_{P^m}^P) \in I. \end{aligned}$$

Тем самым установлено, что $AB, (BA)^T = A^T B^T \in M_n(I)$, откуда $BA \in M_n(I)$.

Случай 2). $P', P'' \in (Q_n)^k$ — произвольные наборы.

В каждом из наборов P' и P'' все числа попарно различны. Значит, надлежащими перестановками строк и столбцов можно из A получить матрицу A_0 , попадающую под случай 1) с тем же k . По уже доказанному, существует матрица $B_0 \in S \setminus (M_n(I))$, для которой $A_0 B_0, B_0 A_0 \in M_n(I)$. При этом найдутся мономиальные (стало быть, обратимые) матрицы $C_1, C_2 \in S$, такие что $A = C_1 A_0 C_2^{-1}$. Умножение матрицы слева (соотв. справа) на мономиальную переставляет её строки (соотв. столбцы), и,

следовательно, $B := C_2 B_0 C_1^{-1} \in S \setminus (M_n(I))$, $AB = C_1(A_0 B_0)C_1^{-1}$, $BA = C_2(B_0 A_0)C_2^{-1} \in M_n(I)$. \square

Следствие 1. Если $A \in S$ и $c \in I_A^*$, то в подмножестве $(cS)^* \subset S$ существует элемент, ортогональный A .

Доказательство. По условию $I := \text{Ann}(c) \triangleleft R$ — собственный идеал, содержащий $\det A$. Согласно теореме 3, найдётся матрица $B \in S \setminus (M_n(I))$, для которой $AB, BA \in M_n(I)$. В таком случае $C := cB \neq 0$ и $c(AB) = c(BA) = 0$, т. е. $C \in (cS)^*$ и $AC = CA = 0$. \square

Лемма 1. Для произвольного $A \in S$ следующие условия эквивалентны:

- 1) $\det A \in Z_R$;
- 2) $I_A \neq 0$;
- 3) в S^* существует элемент, ортогональный A ;
- 4) A — двусторонний делитель нуля;
- 5) A — делитель нуля.

Доказательство. Импликации 1) \Leftrightarrow 2) и 3) \Rightarrow 4) \Rightarrow 5) очевидным образом вытекают из определений, а импликация 2) \Rightarrow 3) — из следствия 1.

Докажем импликацию 5) \Rightarrow 1). Предположим, что, не умаляя общности, A — левый делитель нуля, т. е. что $AB = 0$ для некоторого $B \in S^*$. Тогда $\widehat{A}A = (\det A)E$, откуда $(\det A)B = \widehat{A}AB = 0$. Осталось воспользоваться нетривиальностью B . \square

Следствие 2. Все делители нуля в S двусторонние.

Пусть $Z_S \subset S$ — подмножество всех элементов $A \in S$, удовлетворяющих каждому из эквивалентных условий 1)–5) леммы 1, т. е. множество всех делителей нуля кольца S . Тогда множество вершин графа $O(S)$ есть Z_S^* .

Далее будем считать, что $Z_R^* \neq \emptyset$.

Утверждение 1. Если $I \triangleleft R$ и $I \neq 0$, то $Z_R \cap I \neq \{0\}$.

Доказательство. Предположим, что $Z_R \cap I = \{0\}$. Существуют элементы $b \in I^*$ и $c \in Z_R^*$; тогда $bc \in Z_R \cap I = \{0\}$. Итак, $bc = 0 \neq c$, откуда $b \in Z_R \cap I^* = \emptyset$. Получили противоречие. \square

Лемма 2. Если для подмножества $D \subset S$ идеал $I := \bigcap_{A \in D} I_A \triangleleft R$ ненулевой, то существуют элементы $b \in Z_R^*$ и $C_A \in S^*$, $A \in D$, такие что $bE \perp C_A \perp A$ ($A \in D$).

Доказательство. Согласно утверждению 1, идеал I содержит элемент $c \in Z_R^*$. Тогда $bc = 0$, где $b \in Z_R^*$. Далее, для произвольного $A \in D$ имеем $c \in I_A^*$ и, ввиду следствия 1, найдётся элемент $C_A \in (cS)^*$, ортогональный A ; при этом $bC_A \in bcS = 0$, $bE \perp C_A$. \square

Следствие 3.

1) Для любого $A \in Z_S^*$ имеем $d(A, O(R)) \leq 2$.

2) Если $A_1, A_2 \in Z_S^*$ и $I_{A_1} \cap I_{A_2} \neq 0$, то $d(A_1, A_2) \leq 4$.

Доказательство. Достаточно применить лемму 2 к подмножествам $\{A\}$ и $\{A_1, A_2\}$ множества S . \square

Лемма 3. Если $A_i \in Z_S^*$, $c_i \in I_{A_i}^*$ ($i = 1, 2$) и $c_1c_2 = 0$, то $d(A_1, A_2) \leq 3$.

Доказательство. В силу следствия 1, для любого $i = 1, 2$ найдётся элемент $C_i \in (c_iS)^*$, такой что $C_i \perp A_i$. При этом $C_1C_2, C_2C_1 \in c_1c_2S = 0$, $C_1 \perp C_2$. \square

Определение. Будем говорить, что идеал $I \triangleleft R$ не имеет делителей нуля, если $I^*I^* \not\cong 0$, т. е. если кольцо (вообще говоря, без единицы) I не имеет делителей нуля.

Лемма 4. Если $A_1, A_2 \in Z_S^*$ и $d(A_1, A_2) > 3$, то I_{A_i} ($i = 1, 2$) — один и тот же идеал без делителей нуля.

Доказательство. Согласно лемме 3, $I_{A_1}^*I_{A_2}^* \not\cong 0$. Осталось доказать, что $I_{A_1} = I_{A_2}$.

Допустим, что $I_{A_1} \neq I_{A_2}$. Не умаляя общности, будем считать, что найдётся элемент $c \in I_{A_1} \setminus I_{A_2}$. Полагая $a := \det A_2$, имеем $I_{A_2} = \text{Ann}(a)$, $b := ca \in I_{A_1}^*$ и $bI_{A_2} = caI_{A_2} = 0$, откуда $bI_{A_2}^* \subset \{0\} \cap (I_{A_1}^*I_{A_2}^*) = \emptyset$, $I_{A_2}^* = \emptyset$, $I_{A_2} = 0$, что невозможно. \square

Теорема 4. Граф $O(S)$ связан и имеет диаметр не более 4.

Доказательство. Предположим, что существуют элементы $A_1, A_2 \in Z_S^*$, такие что $d(A_1, A_2) > 4$. По лемме 4 $0 \neq I_{A_1} = I_{A_2} = I_{A_1} \cap I_{A_2}$, что противоречит следствию 3. \square

Теорема 5. Имеем $\text{diam}(O(S)) \geq 3$, причём строгое неравенство эквивалентно существованию идеала вида $\text{Ann}(a) \triangleleft R$ ($a \in Z_R$) без делителей нуля.

Доказательство. Наподобие примеров из [9, 10], дающих нижние оценки диаметра, для произвольного $a \in Z_R$ положим $I := \text{Ann}(a) \triangleleft R$ и $A := J_n + aE_{n1} \in S$. Заметим, что

- $A, A^T \in Z_S^*$, $O_S(A) = I^*E_{1n}$, $O_S(A^T) = I^*E_{n1}$;
- $a_{12} = 1 \neq a_{21}$, $(AA^T)_{11} = 1$ и $O_S(A) \cap O_S(A^T) = \emptyset$, откуда $d(A, A^T) \geq 3$;
- если $I^*I^* \neq 0$, то $(O_S(A))(O_S(A^T)) = (I^*I^*)E_{11} \neq 0$ и, значит, $d(A, A^T) \geq 4$.

Ввиду вышесказанного, $\text{diam}(O(S)) \geq 3$, причём для строгого неравенства достаточно существования идеала вида $\text{Ann}(a) \triangleleft R$ ($a \in Z_R$) без делителей нуля. Обратно, в случае строгого неравенства по лемме 4 для некоторых элементов $A \in Z_S$ и $a := \det A \in Z_R$ идеал $I_A = \text{Ann}(a) \triangleleft R$ не имеет делителей нуля. \square

Теперь основная теорема 1 вытекает из теорем 4 и 5, а также следствия 3. Из неё, а также из неравенств (3) следуют утверждения 1) и 2) теоремы 2. Докажем 3).

Предположим, что $\text{rad}(O(S)) = 2$. Найдутся элементы $C \in Z_S^*$, $c \in R^*$ и $k, l \in Q_n$, такие что $d(C, A) \leq 2$ ($A \in Z_S^*$) и $c_{kl} = c$. Далее, существует подстановка $\sigma \in S_n$, для которой $m := \sigma(k) \neq l$.

Пусть $a \in Z_R$ — произвольный элемент.

Положим $I := \text{Ann}(a) \triangleleft R$ и $A := \left(\sum_{i \neq k} E_{i, \sigma(i)} \right) + aE_{km} \in S$. Заметим, что

- $A \in Z_S^*$, $O_S(A) = I^*E_{mk}$;
- $A \neq C$ (иначе $a_{kl} = c \neq 0$, $m = l$);
- $(m, k) \neq (k, l)$ (иначе $m = k = l$), откуда $C \notin O_S(A)$.

Таким образом, $d(C, A) = 2$, и тогда найдётся элемент $B \in Z_S^*$, ортогональный C и A . Имеем $B = bE_{mk}$, где $b \in I^*$. При этом $BC = 0$, $0 = (BC)_{ml} = bc$, $b \in \text{Ann}(c) \cap I^*$.

Ввиду произвольности $a \in Z_R$, элемент $c \in R^*$ удовлетворяет (2).

Обратно, предположим, что для некоторого $c \in R^*$ выполнено (2). Покажем, что элемент $C := cE \in S^*$ удовлетворяет для каждого $A \in Z_S^*$ неравенству $d(C, A) \leq 2$.

Пусть $A \in Z_S^*$ — произвольный элемент. Тогда $\det A \in Z_R$, и, ввиду (2), существует элемент $b \in I_A^*$, такой что $cb = 0$. Далее, согласно следствию 1, найдётся элемент $B \in (bS)^*$, ортогональный A ; при этом $cB \in cbS = 0$, $C \in Z_S^*$, $C \perp B \perp A$, $d(C, A) \leq 2$.

Тем самым теорема 2 полностью доказана.

Благодарности

Автор благодарит д. ф.-м. н. проф. Э. Б. Винберга за привитый интерес к алгебре.

Автор посвящает статью заместителю директора департамента министерства сельского хозяйства РФ Е. Н. Трошиной.

Список литературы

- [1] Beck I., “Coloring of commutative rings”, *J. Algebra*, **116** (1988), 208–226.
- [2] Anderson D.F., Livingston P.S., “The zero-divisor graph of a commutative ring”, *J. Algebra*, **217** (1999), 434–447.
- [3] Anderson D.F., Frazier A., Lauve A., Livingston P.S., “The zero-divisor graph of a commutative ring, II”, *Lect. Notes Pure Appl. Math., Marcel Dekker, New York*, **220** (2001), 61–72.
- [4] Akbari S., Maimani H.R., Yassemi S., “When zero-divisor graph is planar or a complete r -partite graph”, *J. Algebra*, **270** (2003), 169–180.
- [5] Akbari S., Mohammadian A., “On the zero-divisor graph of a commutative ring”, *J. Algebra*, **274** (2004), 847–855.
- [6] Akbari S., Mohammadian A., “Zero-divisor graphs of non-commutative rings”, *J. Algebra*, **296** (2006), 462–479.
- [7] Akbari S., Mohammadian A., “On zero-divisor graphs of finite rings”, *J. Algebra*, **314** (2007), 168–184.
- [8] Redmond S.P., “Central sets and radii of the zero-divisor graphs of commutative rings”, *Comm. in Algebra*, **34**:7 (2006), 2389–2401.
- [9] Бахадлы Б. Р., Гутерман А. Э., Маркова О. В., “Графы, определённые ортогональностью”, *Зап. научн. семин. ПОМИ*, **428** (2014), 49–80.
- [10] Гутерман А. Э., Маркова О. В., “Графы ортогональности матриц над телами”, *Зап. научн. семин. ПОМИ*, **463** (2017), 81–93.

Orthogonality graphs of matrices over commutative rings
Styrt O.G.

The paper is devoted to studying the orthogonality graph of the matrix ring over a commutative ring. It is proved that the orthogonality graph of the ring of matrices with size greater than 1 over a commutative ring with zero-divisors is connected and has diameter 3 or 4; a criterion for each value is obtained. It is also shown that each of its vertices has distance at most 2 from some scalar matrix.

Keywords: associative ring with identity, commutative ring, zero-divisor, matrix ring, zero-divisor graph, orthogonality graph.

Список литературы

- [1] Beck I., “Coloring of commutative rings”, *J. Algebra*, **116** (1988), 208–226.
- [2] Anderson D.F., Livingston P.S., “The zero-divisor graph of a commutative ring”, *J. Algebra*, **217** (1999), 434–447.
- [3] Anderson D.F., Frazier A., Lauve A., Livingston P.S., “The zero-divisor graph of a commutative ring, II”, *Lect. Notes Pure Appl. Math., Marcel Dekker, New York*, **220** (2001), 61–72.
- [4] Akbari S., Maimani H.R., Yassemi S., “When zero-divisor graph is planar or a complete r -partite graph”, *J. Algebra*, **270** (2003), 169–180.
- [5] Akbari S., Mohammadian A., “On the zero-divisor graph of a commutative ring”, *J. Algebra*, **274** (2004), 847–855.
- [6] Akbari S., Mohammadian A., “Zero-divisor graphs of non-commutative rings”, *J. Algebra*, **296** (2006), 462–479.
- [7] Akbari S., Mohammadian A., “On zero-divisor graphs of finite rings”, *J. Algebra*, **314** (2007), 168–184.
- [8] Redmond S.P., “Central sets and radii of the zero-divisor graphs of commutative rings”, *Comm. in Algebra*, **34**:7 (2006), 2389–2401.
- [9] Bakhadly B.R., Guterman A.E., Markova O.V., “Graphs defined by orthogonality”, *Computational methods and algorithms. Part XXVII, Zap. Nauchn. Sem. POMI, St. Petersburg*, **428** (2014), 49–80 (In Russian).
- [10] Guterman A.E., Markova O.V., “Orthogonality graphs of matrices over skew fields”, *Computational methods and algorithms. Part XXX, Zap. Nauchn. Sem. POMI, St. Petersburg*, **463** (2017), 81–93 (In Russian).

Выразимость CPL-функций нейронными схемами над ReLU-базисами

В. Г. Шишляков¹

В работе рассматривается вопрос выразимости любой кусочно-линейной непрерывной функции многих переменных в виде нейронной схемы над базисом с нелинейностями типа \max . Затем результат переносится на нейронные схемы, построенные над базисом с единственной нелинейной функцией ReLU .

Перед доказательством результата формулируются и доказываются несколько вспомогательных, технических лемм, расширяющих имеющиеся знания о свойствах кусочно-линейных функций и классов эквивалентности, порожденных некоторым набором гиперплоскостей.

Также в работе даются оценки нелинейной сложности и глубины для построенных нейронных схем в двух данных базисах.

Наконец, в работе доказывается равенство класса кусочно-линейных непрерывных функций, класса функций, представимых нейронными схемами над базисом первого типа и класса функций, представимых нейронными схемами над базисом второго типа.

Ключевые слова: Нейронные схемы, архитектура, восстановление функций, выразимость функций, выпуклые функции, кусочно-линейные непрерывные функции, ReLU -функции, функция максимума

1. Введение

В данной работе продолжается изучение вопросов выразимости функций, которые впервые подробно были исследованы в работе [1]. В работе [1] был заложен фундамент в виде определений, связывающих понятия нейронных сетей с классическими понятиями дискретной математики, такими, как схемы функциональных элементов и автоматные функции [2], а также рассмотрены некоторые проблемы, с которыми часто приходится сталкиваться при построении нейросетевой архитектуры.

А именно, в исследовании [1] было предложено рассмотрение нейронных сетей с точки зрения схем функциональных элементов над определенным заранее фиксированным набором функциональных элементов

¹*Шишляков Владимир Геннадьевич* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: bolotmaks@yandex.ru.

Shishlyakov Vladimir Gennad'evich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

(базисом) и сравнение (с теоретико-множественной точки зрения) множества функций, соответствующих всем таким схемам, с классом функций, обладающих определенными свойствами.

Упомянутые выше схемы, согласно [1], будем называть нейронными схемами. Данные схемы, по сути, являются синонимами термина нейронная сеть, так как нейронную сеть можно получить из нейронной схемы, группируя определенные комбинации функциональных элементов в нейроны, что подробно описано в работах [3] и [4].

Также в работе [1] было решено множество задач, давших сильную базу в виде самих результатов, а также методов и идей их доказательств, для решения дальнейших подобных задач. В частности, в работе [1] было показано, что класс функций, реализуемых классическими нейронными сетями Мак-Каллока и Питтса (с функциями активации Хевисайда) [5] в точности совпадает с классом кусочно-параллельных функций. Однако, данный класс функций является достаточно узким классом, при помощи которого невозможно полноценно решать, например, задачи регрессии.

Подобные вопросы выразимости исследовались также в работах [6], [7], [8], [9], [10], [11]. В работах [6], [7], [8] и [9] был доказан ряд интересных результатов, связанных с выразимостью различных классов функций, обладающих определенными свойствами, над базисами, состоящими из функций, обладающих определенными характеристиками, во многом схожими с базисами из работы [1]. В работах [10] и [11] доказаны результаты, являющиеся частными случаями результата, доказанного в данном исследовании. О полученных в работах [10] и [11] результатах будет подробнее рассказано ниже.

Стоит отметить, что помимо классических нейронных сетей с функцией активации Хевисайда есть нейронные сети с другими функциями активации. В частности, большое распространение в современных архитектурах получила ставшая классической функция активации RELU. Возникает теоретический интерес - выяснить, какой класс функций выражается при помощи нейронных сетей с указанной функцией активации.

В силу того, что базис для построения нейронных сетей с RELU функциями активации содержит лишь кусочно-линейные непрерывные функции, а классы кусочно-линейных и непрерывных функций замкнуты по операции суперпозиции [1],[6], то возникает гипотеза, что, класс функций, представимых нейронными сетями над базисами с функциями активации RELU, совпадает с классом кусочно-линейных непрерывных функций.

Данная гипотеза частично была исследована в работах [7], [10] и [11]. В работе [10] было доказано, что нейронные схемы, построенные над базисом, состоящим из линейных функций и функции модуля, могут вос-

становливать произвольную кусочно-линейную непрерывную функцию одной и двух переменных.

В работе [7] было доказано, что нейронные схемы над базисом, состоящим из линейных функций и функции RELU, могут восстанавливать произвольную кусочно-линейную непрерывную функцию от одной и двух переменных.

Отметим, что вопрос исследования функций с бóльшим числом переменных в работах [7] и [10] затронут не был.

В работе [11] было доказано, что любую выпуклую кусочно-линейную непрерывную функцию можно выразить в виде нейронной схемы над любым из двух базисов, один из которых содержит все линейные функции и нелинейности $\max(x_1, \dots, x_n)$ от любого числа аргументов, а второй содержит все линейные функции и функцию RELU.

Текущее исследование является продолжением серии публикаций, начатой в работе [11]. В текущей статье доказывается основная теорема о том, что произвольную кусочно-линейную непрерывную функцию можно представить нейронной схемой над базисом из линейных функций и функций $\max(x_1, \dots, x_n)$ от любого числа аргументов, а затем доказывается аналогичное утверждение для базисов с единственной нелинейностью — функцией RELU, которая может использоваться, как функция активации получаемых из данных схем нейронных сетей.

Доказательство упомянутой теоремы идейно базируется на результатах работы [11], однако текущая работа является полноценным и скорее основным исследованием, в силу того, что при развертывании идеи доказательства на математический язык потребовалось доказать гораздо больший объем вспомогательных утверждений, чем было доказано в работе [11].

Таким образом, в данной работе устанавливается связь в виде равенства между классом кусочно-линейных непрерывных функций и функциями, получаемыми из схем в упомянутых выше базисах и, помимо сказанного, доказывается множество замечательных свойств классов эквивалентности и кусочно-линейных непрерывных функций, которые в дальнейшем используются при доказательстве основного результата.

Также в данной работе даются оценки сверху нелинейной сложности и нелинейной глубины полученных нейронных схем.

2. Основные понятия и формулировка результатов

Определим основные понятия, которые используются в данной статье. Для начала введем понятие базиса нейронной схемы и связанные с ним понятия, следуя работам [1], [2] и [3].

Базисом будем называть некоторый набор функциональных элементов, где каждый функциональный элемент представляет из себя пару $(S, f(x_1, \dots, x_n))$, в которой $f(x_1, \dots, x_n) : \mathbb{R}^n \rightarrow \mathbb{R}$, а S – сопоставленный ей графический объект с n входными стрелками и одной выходной стрелкой (кратко – входы и выход объекта S). Входам объекта S приписаны слева направо переменные x_1, \dots, x_n , являющиеся аргументами функции f , выходу приписан выход функции f .

В данной работе будем рассматривать два базиса (1) и (2), приведенных ниже.

$$B_1 = \{c, \gamma \cdot x, \sum_n(x_1, \dots, x_n), \max(x_1, \dots, x_n)\} \quad (1)$$

$$B_2 = \{c, \gamma \cdot x, \sum_n(x_1, \dots, x_n), RELU(x)\} \quad (2)$$

Подробное описание функций из базисов (1) и (2) и их графические обозначения можно найти в работе [11].

Функциональные элементы \max и $RELU$ из базисов (1) и (2) будем называть нелинейными. Все остальные элементы данных базисов будем называть линейными.

Подробнее о том, как строятся схемы функциональных элементов из элементов любого из рассматриваемых в данной работе базисов, описано в [1]. Получаемые схемы называются нейронными схемами. Множество нейронных схем, получаемых из элементов некоторого базиса B , будем обозначать $[B]$.

Будем говорить, что функция $f : \mathbb{R}^n \rightarrow \mathbb{R}$ представима (выражается, восстанавливается) нейронной схемой над некоторым базисом B , если $\exists g \in [B] : \forall \bar{x} \in \mathbb{R}^n f(\bar{x}) = g(\bar{x})$.

Путем в нейронной схеме назовем последовательность функциональных элементов $(S_1, f_1), \dots, (S_k, f_k)$ схемы, таких, что:

- Один из входов элемента (S_1, f_1) является входом схемы
- Выход элемента (S_k, f_k) является выходом схемы
- Один из входов элемента (S_i, f_i) является выходом элемента (S_{i-1}, f_{i-1}) при $i \in \{2, \dots, k\}$

Длиной пути называется число нелинейных элементов, содержащихся в нем.

Нелинейной глубиной схемы называется длина самого длинного пути в данной схеме. Нелинейной сложностью схемы называется число всех нелинейных элементов в схеме.

Далее введем важнейшие понятия для данной работы — это понятия гиперплоскости, класса эквивалентности, кусочно-линейной функции, функции класса CPL, а также связанные с ними понятия.

Пусть дано пространство \mathbb{R}^n . Гиперплоскостью (плоскостью размерности $n-1$) будем называть геометрическое место точек $l = \{(x_1, \dots, x_n) \in \mathbb{R}^n | a_1x_1 + \dots + a_nx_n + c = 0\}$ (где a_1, \dots, a_n, c — константы, причем a_1, \dots, a_n не равны нулю одновременно).

Пусть $\bar{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$. Тогда под значением $l(\bar{x})$ будем понимать значение $a_1x_1 + \dots + a_nx_n + c$.

Будем говорить, что точка \bar{x} лежит на гиперплоскости l , если $l(\bar{x}) = 0$. Таким образом, гиперплоскость — это множество решений уравнения $l(\bar{x}) = 0$.

Так как по уравнению вида $a_1x_1 + \dots + a_nx_n = 0$ можно в точности восстановить гиперплоскость, то в дальнейшем будем иногда определять гиперплоскость через ее уравнение, а само уравнение будем называть уравнением, определяющим гиперплоскость.

Вместе с гиперплоскостью $l = \{(x_1, \dots, x_n) \in \mathbb{R}^n | a_1x_1 + \dots + a_nx_n + c = 0\}$ естественным образом определяются два полупространства $l^+ = \{(x_1, \dots, x_n) \in \mathbb{R}^n | a_1x_1 + \dots + a_nx_n + c > 0\}$ и $l^- = \{(x_1, \dots, x_n) \in \mathbb{R}^n | a_1x_1 + \dots + a_nx_n + c < 0\}$. Очевидно, что $l^+ \cup l^- \cup l = \mathbb{R}^n$ для любой гиперплоскости l .

В дальнейшем под некоторым набором гиперплоскостей всегда будем подразумевать именно множество гиперплоскостей, то есть множество геометрических мест точек, отличных друг от друга, если не оговорено иное. Следует отметить, что все дальнейшие определения и большинство доказанных утверждений остаются верными и для случая, если в наборах гиперплоскостей разрешить повторения. Однако в данном случае оказывается неверной лемма 13, рассмотренная далее, а также все утверждения, в доказательствах которых явно или неявно используется данная лемма. Именно поэтому в данной работе используется указанное ограничение.

Гиперплоскостью размерности $n - k$ будем называть геометрическое место точек, полученное, как пересечение k гиперплоскостей размерности $n - 1$.

Пусть $\bar{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$, а l_1, \dots, l_k — некоторые гиперплоскости, определяемые выражениями $l_i = \{(x_1, \dots, x_n) \in \mathbb{R}^n | a_{i1}x_1 + \dots + a_{in}x_n + c_i = 0\}$, $i = 1, \dots, k$.

Рассмотрим вектор-функцию $\sigma(\bar{x}) = (\text{sgn}(a_{11}x_1 + \dots + a_{1n}x_n + c_1), \dots, \text{sgn}(a_{k1}x_1 + \dots + a_{kn}x_n + c_k))$, которая называется сигнатурой вектора \bar{x} [1]. Каждая ее компонента показывает расположение точки \bar{x} относительно каждой из гиперплоскостей l_1, \dots, l_k .

Будем считать точки $\bar{x}, \bar{y} \in \mathbb{R}^n$ эквивалентными относительно гиперплоскостей l_1, \dots, l_k и обозначать это $\bar{x} \sim \bar{y}$, если $\sigma(\bar{x}) = \sigma(\bar{y})$.

Очевидно, что отношение $\bar{x} \sim \bar{y}$ является отношением эквивалентности [1]. Следовательно, гиперплоскости разбивают \mathbb{R}^n на множество непустых, непересекающихся классов R^1, \dots, R^s , дающих в объединении все множество \mathbb{R}^n .

Сигнатурой всякого класса $R^i \in \{R^1, \dots, R^s\}$ назовем значение $\sigma(R^i) = \sigma(\bar{x})$, где \bar{x} – произвольный элемент класса R^i . Отметим, что определение корректно, так как по построению $\forall \bar{x}, \bar{y} \in R^i \sigma(\bar{x}) = \sigma(\bar{y})$ [1].

Так как в доказательствах иногда удобно обращаться к компонентам вектора сигнатуры, то обозначим $\sigma_u(R^i)$ и $\sigma_u(\bar{x})$ – значения компоненты с номером u сигнатур класса R^i и вектора $\bar{x} \in \mathbb{R}^n$, соответственно.

В дальнейшем мы хотим оперировать не самими классами эквивалентности, а их сигнатурами. Однако бывают случаи, когда всевозможных сигнатур больше, чем классов эквивалентности в разбиении пространства рассматриваемым набором гиперплоскостей.

Если рассмотреть системы равенств и неравенств, соответствующие сигнатурам, для которых не нашлось классов эквивалентности, можно легко убедиться, что данные системы будут иметь пустые множества решений. Поставим в соответствие таким сигнатурам пустые множества и назовем их пустыми (мнимыми) классами эквивалентности.

Таким образом, сигнатурами пустых классов являются все оставшиеся комбинации векторов из $\{-1, 0, 1\}^k$, которые не соответствуют ни одному классу эквивалентности из классического разбиения пространства, порожденного отношением эквивалентности $\sigma(\bar{x}) = \sigma(\bar{y})$. Так как пустые классы в некотором смысле неотличимы, то не имеет значения – какая сигнатура из данных оставшихся комбинаций присваивается выбираемому пустому классу (главное, чтобы у всех пустых классов были различные сигнатуры).

Здесь и далее под множеством классов эквивалентности, полученных в результате разбиения пространства \mathbb{R}^n некоторым набором гиперплоскостей, всегда будем понимать это расширенное множество классов, среди которых есть пустые множества, если не оговорено иное.

Данное допущение никоим образом не портит картину, так как добавленные пустые классы не пересекаются по определению, и новое расширенное множество классов будет давать в объединении все множество \mathbb{R}^n . Непустота же классов будет в дальнейшем каждый раз оговариваться.

Однако, при этом, любой сигнатуре теперь будет соответствовать некоторый класс из полученного разбиения.

Множество классов эквивалентности $\{R^1, \dots, R^s\}$, полученное объединением разбиения пространства \mathbb{R}^n некоторым набором гиперплоскостей $\{l_1, \dots, l_k\}$ при помощи введенного выше отношения эквивалентности $\bar{x} \sim \bar{y}$ и пустых классов, соответствующих сигнатурам, которым изначально никакие классы не соответствовали, будем называть разбиением пространства \mathbb{R}^n или просто разбиением.

Класс эквивалентности R^i назовем плоским, если $\exists l_j \in \{l_1, \dots, l_k\} : R^i \subset l_j$.

Класс эквивалентности R^i назовем объемным, если он не является плоским.

Очевидно, что если R^i – непустой и объемный, то он имеет сигнатуру $\sigma = (\sigma_1, \dots, \sigma_k) : \sigma_j \neq 0 \forall j \in \{1, \dots, k\}$. Если же класс R^i – непустой и плоский, то он имеет сигнатуру $\sigma = (\sigma_1, \dots, \sigma_k)$, в которой $\exists j \in \{1, \dots, k\} : \sigma_j = 0$.

Пусть дан объемный класс эквивалентности $R^i \subset \mathbb{R}^n$, имеющий сигнатуру $\sigma = (\sigma_1, \dots, \sigma_k)$. Тогда контуром размерности $n - l, l \in \{1, \dots, n\}$ данного класса назовем объединение всех классов эквивалентности, имеющих сигнатуры σ' , содержащиеся во множестве векторов, полученных из сигнатуры $\sigma = (\sigma_1, \dots, \sigma_k)$ занулением всех возможных комбинаций из l компонент вектора σ .

Контуром будем называть объединение контуров размерностей $n - 1, n - 2, \dots, 0$. Контур класса R^i обозначим $\partial_{lin} R^i$. Контур класса R^i размерности k будем обозначать $\partial_{lin}^k R^i, k \in \{0, \dots, n - 1\}$.

Если требуется посмотреть на контур не как на объединение классов эквивалентности, а как на множество классов эквивалентности, будем обозначать это $\partial_{set lin} R^i$ и $\partial_{set lin}^k R^i, k \in \{0, \dots, n - 1\}$. Другими словами, $\partial_{lin} R^i = \bigcup_{R \in \partial_{set lin} R^i} R$ и $\partial_{lin}^k R^i = \bigcup_{R \in \partial_{set lin}^k R^i} R$.

Размерностью непустого класса R^i назовем число $n - l, l \in \{0, \dots, n\}$, где l – число нулевых компонент вектора сигнатуры класса R^i .

Отметим, что, число нулевых компонент вектора сигнатуры всякого класса R^i лежит во множестве $\{0, \dots, k\}$, где, вообще говоря, $k \neq n$. В случае, когда $k < n$, могут получаться лишь классы размерности, не меньшей $n - k$. Если же $k > n$, то при занулении более, чем n компонент вектора сигнатуры будут получаться всегда пустые классы эквивалентности. Случай же $k = n$ является самым сбалансированным – в данном случае могут существовать непустые классы любой размерности, при этом классы даже с полностью нулевыми сигнатурами могут оказаться непустыми.

Для пустых классов эквивалентности не будем вводить никакого понятия размерности, так как такие классы в дальнейшем нас не интересуют.

Пусть $L_N = \{l_1, \dots, l_N\}$ – множество гиперплоскостей. Тогда обозначим $R(L_N)$ – множество всех непустых классов, получаемых при разбиении пространства \mathbb{R}^n данными гиперплоскостями (то есть классическое разбиение пространства \mathbb{R}^n отношением эквивалентности, заданным равенством сигнатур). Также обозначим $V(L_N)$ – множество всех непустых объемных классов, полученных при разбиении пространства \mathbb{R}^n гиперплоскостями L_N . Очевидно, что $V(L_N) \subset R(L_N)$.

Под выражениями $R(\emptyset)$ и $V(\emptyset)$ будем понимать множество из одного класса эквивалентности, совпадающего с \mathbb{R}^n .

Отметим, что множества $R(L_N)$ и $V(L_N)$ могут тоже иногда называться разбиениями пространства \mathbb{R}^n гиперплоскостями L_N или просто разбиениями. Однако, когда речь будет идти только о непустых или непустых объемных классах эквивалентности, в предложении будет всегда указываться обозначение $R(L_N)$ или $V(L_N)$, соответственно.

Два непустых объемных класса R^+, R^- из некоторого разбиения, таких, что $R^+ \neq R^-$, будем называть смежными, если существует непустой $(n-1)$ -мерный класс R^0 из данного разбиения, такой, что $R^0 \subset \overline{R^+} \cap \overline{R^-}$. Обозначать это соотношение будем, как $R^+|R^-$ или $R^-|R^+$, так как очевидно, что отношение смежности является симметричным.

Класс R^0 будем называть пограничным классом.

Классы $R^1, R^2 \in V(L) : R^1 \neq R^2$ будем называть связанными по смежности, если для них выполняется, что $R^1|R^2$ или $\exists R^{(1)}, \dots, R^{(r)} \in R(L) : R^1|R^{(1)}|\dots|R^{(r)}|R^2$.

Пусть $L = \{l_1, \dots, l_k\}$ и дано множество $R(L) = \{R^1, \dots, R^s\}$ непустых классов, порождаемых разбиением пространства \mathbb{R}^n гиперплоскостями $L = \{l_1, \dots, l_k\}$. Тогда укрупнением разбиения $R(L)$ называется всякое разбиение $R(L')$, где $L' \subset L$.

Другими словами, укрупнением разбиения называется разбиение, полученное из исходного разбиения удалением одной или нескольких гиперплоскостей.

По определению будем считать, что всякое укрупнение $R(\emptyset)$ – это снова $R(\emptyset)$.

Очевидно, что если $R(L)$ – некоторое разбиение, а $R(L')$ – его укрупнение, то $\forall R \in R(L) \exists R' \in R(L') : R \subset R'$.

Будем говорить, что функция $f(\bar{x})$ является кусочно-линейной [1] и обозначать это $f(\bar{x}) \in PL$, если существует разбиение некоторым множеством гиперплоскостей L , такое что $\forall R^i \in R(L) \subset \{R^1, \dots, R^s\}$ выполняется $\forall \bar{x} \in R^i f(\bar{x}) = \bar{b}_i \cdot \bar{x} + d_i$, где \bar{b}_i, d_i – константы.

Другими словами, кусочно-линейной будем называть всякую функцию, для которой существует разбиение, над каждым непустым классом которого ее поведение можно описать некоторой линейной функцией.

Всякую функцию $f_{R^i}(\bar{x}) = \bar{b}_i \cdot \bar{x} + d_i$ будем называть линейной частью функции $f(\bar{x})$ на классе R^i .

Иногда, чтобы сразу ввести кусочно-линейную функцию и зафиксировать валидирующее (проверяющее) ее разбиение, будем говорить, что функция $f(\bar{x})$ – кусочно-линейная функция, заданная над (разбиением, классами) $\{R^1, \dots, R^s\}$, где в качестве разбиения будет использоваться либо классическое разбиение с непустыми классами эквивалентности, либо расширенное разбиение, в котором к непустым классам добавлены мнимые классы эквивалентности.

Также иногда будем говорить, что функция $f(\bar{x})$ – кусочно-линейная функция, заданная над набором гиперплоскостей $\{l_1, \dots, l_k\}$. В этом случае будем подразумевать, что $f(\bar{x})$ задана над разбиением $\{R^1, \dots, R^s\}$, которое порождается гиперплоскостями $\{l_1, \dots, l_k\}$.

CPL -функцией назовем всякую кусочно-линейную непрерывную функцию. Множество всех непрерывных кусочно-линейных функций обозначим CPL .

Пусть дана некоторая функция $f(\bar{x}) : \mathbb{R}^n \rightarrow \mathbb{R}$. Сечением функции $f(\bar{x})$ прямой $l = (\bar{x}_1; \bar{x}_2)$ назовем функцию $f_{\bar{x}_1, \bar{x}_2}(t) = f((1-t) \cdot \bar{x}_1 + t \cdot \bar{x}_2)$ одного аргумента $t \in \mathbb{R}$.

Отметим, что иногда для краткости удобно опускать или сокращать обозначение прямой, по которой производится сечение, и писать $f_l(t)$ или просто $f(t)$.

Сечение всякой функции $f(\bar{x})$ произвольной прямой $(\bar{x}_1; \bar{x}_2)$ обладает следующими очевидными свойствами:

- 1) $f(0) = f(\bar{x}_1)$, $f(1) = f(\bar{x}_2)$.
- 2) $\forall \bar{\xi} \in (\bar{x}_1; \bar{x}_2) \exists t_{\bar{\xi}} \in (0; 1) : f(t_{\bar{\xi}}) = f(\bar{\xi})$.
- 3) Если $f(\bar{x})$ – непрерывная функция, то $f(t)$ – тоже непрерывная функция.
- 4) Если $f(\bar{x})$ – линейная функция, то $f(t)$ – линейная функция одного аргумента.
- 5) Если $f(\bar{x})$ – выпуклая функция, то $f(t)$ – тоже выпуклая функция, как сужение выпуклой функции на выпуклое множество.
- 6) Вообще говоря, сечения функции $f(\bar{x})$ прямыми $(\bar{x}_1; \bar{x}_2)$ и $(\bar{x}_2; \bar{x}_1)$ – это два разных сечения из-за разницы в параметризации прямых.

Пусть $f_{R^i}(t), f_{R^j}(t)$ – сечения линейных частей функции $f(\bar{x})$ некоторой прямой $(\bar{x}_1; \bar{x}_2)$. Тогда разницей сечений линейных частей (дельтой линейных частей) назовем функцию $A(t) = f_{R^i}(t) - f_{R^j}(t)$.

Функция $A(t)$ обладает следующими очевидными замечательными свойствами:

- 1) Если $\exists \bar{\xi} \in (\bar{x}_1; \bar{x}_2) : f_{R^i}(\bar{\xi}) = f_{R^j}(\bar{\xi})$, то $A(t_{\bar{\xi}}) = 0$ и наоборот. А также, в частности, $f_{R^i}(\bar{x}_1) = f_{R^j}(\bar{x}_1)$ эквивалентно тому, что $A(0) = 0$, а $f_{R^i}(\bar{x}_2) = f_{R^j}(\bar{x}_2)$ эквивалентно тому, что $A(1) = 0$.
- 2) $A(t)$ является линейной функцией одного аргумента, как разность двух линейных одноместных функций.

Пусть $f(\bar{x})$ – CPL-функция, заданная над разбиением $\{R^1, \dots, R^s\}$, порожденным гиперплоскостями $\{l_1, \dots, l_k\}$ и пусть R^+, R^- – два смежных класса эквивалентности по пограничному классу R^0 . Тогда склейкой классов R^+, R^- назовем функцию $g(\bar{x})$, для которой выполняется два свойства:

- 1) $g(\bar{x}) = \max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$ или $g(\bar{x}) = \min(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$;
- 2) $g(\bar{x}) = f(\bar{x}) \forall \bar{x} \in R^+ \cup R^- \cup R^0$.

Очевидно, что любая склейка — это CPL-функция, которую можно задать над разбиением пространства единственной прямой $l \in \{l_1, \dots, l_k\} : R^0 \subset l$.

Ниже будет показано (лемма 11), что для любой CPL-функции склейки существуют для всех пар смежных классов R^+, R^- разбиения, задающего рассматриваемую CPL-функцию.

Склейку классов R^+, R^- для функции $f(\bar{x})$ назовем *вогнутой*, если ее можно представить в виде функции $g(\bar{x}) = \min(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$. Выпуклой склейкой классов R^+, R^- назовем склейку, представимую функцией $g(\bar{x}) = \max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$.

Как далее станет известно, склейки могут быть одновременно выпуклыми и вогнутыми. Чтобы задать класс склеек, которые являются выпуклыми, но не являются вогнутыми и наоборот, введем следующие понятия.

Склейку классов R^+, R^- для функции $f(\bar{x})$ назовем *строго вогнутой*, если она является вогнутой, но не является выпуклой. Строго выпуклой склейкой классов R^+, R^- назовем склейку, которая является выпуклой, но не является вогнутой.

Пусть $R \subset V(L)$ – некоторое подмножество множества объемных классов, полученных при разбиении пространства \mathbb{R}^n некоторым набором гиперплоскостей L .

Тогда обозначим $\partial_S(R) = \{R^i \in V(L) : \exists R^j \in R : R^i | R^j\} \cup R$, что в переводе на русский означает множество исходных классов R , расширенное на множество всех классов, смежных с классами данного множества R . Если же R – это некоторый класс (а не множество классов), то будем считать, что $\partial_S(R) = \partial_S(\{R\})$.

Пусть $R^{(1)} \in V(L)$, где L – некоторый набор гиперплоскостей. Цепью (цепью расширений) $\partial_S^i(R^{(1)})$, $i \in \mathbb{N}$ будем называть последовательность множеств $\partial_S^i(R^{(1)}) = \underbrace{\partial_S(\dots\partial_S(R^{(1)}))}_{i \text{ раз}}$. Будем говорить, что цепь

$\partial_S^i(R^{(1)})$, $i \in \mathbb{N}$ стабилизируется (на некотором индексе $i_{stab} \in \mathbb{N}$), если $\partial_S^{i_{stab}+1}(R^{(1)}) = \partial_S^{i_{stab}}(R^{(1)})$.

Обозначим также $\partial_{add}^{i-1}(R^{(1)}) = \partial_S^i(R^{(1)}) \setminus \partial_S^{i-1}(R^{(1)})$.

Наконец, напомним несколько определений и свойств из топологии и выпуклого анализа, которые будут активно использоваться в дальнейшем.

Отрезком, соединяющим две произвольные точки $\bar{x}, \bar{y} \in \mathbb{R}^n$ назовем множество $[\bar{x}; \bar{y}] = \{\bar{\xi} = (1 - \alpha) \cdot \bar{x} + \alpha \cdot \bar{y} | \alpha \in [0; 1]\}$. Аналогично вводится понятие интервала: $(\bar{x}; \bar{y}) = \{\bar{\xi} = (1 - \alpha) \cdot \bar{x} + \alpha \cdot \bar{y} | \alpha \in (0; 1)\}$. Под прямой, соединяющей точки $\bar{x}, \bar{y} \in \mathbb{R}^n$, будем понимать множество $(\bar{x}; \bar{y})_\infty = \{\bar{\xi} = (1 - \alpha) \cdot \bar{x} + \alpha \cdot \bar{y} | \alpha \in \mathbb{R}\}$.

Отметим, что если дана некоторая точка $\bar{\xi}$ из отрезка, интервала или прямой, соединяющих точки \bar{x}, \bar{y} , то ей соответствует единственное значение параметра $t \in \mathbb{R}$, задающего точку $\bar{\xi}$ в данном промежутке. Будем обозначать это значение параметра, как $t_{\bar{\xi}}$.

Множество $M \subset \mathbb{R}^n$ называется выпуклым, если $\forall \bar{x}, \bar{y} \in M$ выполняется, что $[\bar{x}; \bar{y}] \subset M$.

Функция $f : U \rightarrow \mathbb{R}$ называется выпуклой, если $U \subset \mathbb{R}^n$ – выпуклое множество и $\forall \bar{x}_1, \bar{x}_2 \in U \forall \alpha \in (0; 1)$ выполняется, что $f((1 - \alpha) \cdot \bar{x}_1 + \alpha \cdot \bar{x}_2) \leq (1 - \alpha) \cdot f(\bar{x}_1) + \alpha \cdot f(\bar{x}_2)$.

ε -окрестностью точки $\bar{x} \in \mathbb{R}^n$ ($\varepsilon > 0$) будем называть шар $O_\varepsilon(\bar{x}) = \{\bar{x}' \in \mathbb{R}^n : \|\bar{x} - \bar{x}'\| < \varepsilon\}$. Иногда удобно рассуждать в терминах окрестностей вида $O(\bar{x})$. Под такой окрестностью понимается окрестность какого-то радиуса $\varepsilon > 0$, без уточнения конкретного значения ε . Обычно такая запись употребляется вместе с кванторами всеобщности или существования, когда конкретное значение ε становится избыточным.

Точка $\bar{x} \in M \subset \mathbb{R}^n$ называется внутренней точкой множества M , если $\exists O(\bar{x}) \subset M$. Множество всех внутренних точек множества M называется внутренностью множества M и обозначается $\text{int } M$.

Множество $M \subset \mathbb{R}^n$ называется открытым, если $\forall \bar{x} \in M \exists O(\bar{x}) : O(\bar{x}) \subset M$. Или, другими словами, если любая точка данного множества – внутренняя.

Точкой прикосновения множества $M \subset \mathbb{R}^n$ называется всякая точка $\bar{x}' \in \mathbb{R}^n$ для которой выполняется, что $\exists \{\bar{x}_n\}_{n \in \mathbb{N}} \subset M : \lim_{n \rightarrow +\infty} \bar{x}_n = \bar{x}'$.

Замыканием множества M назовем множество \bar{M} всех точек прикосновения множества M .

Граничной точкой множества $M \subset \mathbb{R}^n$ называется всякая точка $\bar{x} \in \mathbb{R}^n$, для которой выполняется, что $\forall O(\bar{x}) \exists \bar{x}', \bar{x}'' \in O(\bar{x}) : \bar{x}' \notin M \ \& \ \bar{x}'' \in M$. Множество всех граничных точек множества M называется границей множества M и обозначается ∂M .

Из курса общей топологии [12], [13] известно, что если множество M – открыто, то это эквивалентно тому, что $M = \text{int } M$, а также, что $\bar{M} = \text{int } M \cup \partial M$ и для любых множеств A_1, \dots, A_n верно, что $\overline{A_1 \cap \dots \cap A_n} \subset \bar{A}_1 \cap \dots \cap \bar{A}_n$.

Далее представлены основные результаты данной работы. Их формулировки и доказательства для удобства разбиты на несколько разделов.

В первом, вспомогательном, разделе (фактически, это раздел 4) описывается общая схема доказательства основной теоремы со ссылками на соответствующие леммы, в которых описываемые идеи превращаются из гипотез в доказанные суждения. В данном разделе все утверждения формулируются в виде неформализованных гипотез.

Во втором разделе (фактически, это раздел 5) описываются технические леммы, которые требуются для доказательства основных лемм (основных идей из описываемой в первом разделе схемы доказательства).

В третьем разделе (фактически, это раздел 6) строго формулируются и доказываются основные идеи, описанные в первом разделе.

В четвертом разделе (фактически, это раздел 7) доказывается основное утверждение о выразимости произвольной n -местной CPL-функции в виде нейронной схемы над базисом B_1 и несколько следствий из него.

3. Схема доказательства основного результата

Доказательство выразимости CPL-функций над базисом B_1 идейно опирается на результаты о выразимости выпуклых CPL-функций, полученные в работе [11], к которым добавлены новые гипотезы о поведении CPL-функций:

- 1) Сложение и умножение на константу любой CPL-функции снова дает CPL-функцию, при этом множество гиперплоскостей, над которыми можно задать результат сложения, можно взять равным объединению множеств гиперплоскостей исходных функций. А умножение на константу вообще не меняет число порождающих гиперплоскостей. Данная гипотеза формализована и доказана в лемме 18.

Гипотеза 1, формально, не используется в процессе доказательства основного утверждения, т.к. скрыта в доказательстве гипотезы 2, однако идейно она включается в основные гипотезы, т.к. при помощи нее осуществляется контроль неизменности числа склеек при упомянутых преобразованиях.

- 2) Добавление вогнутой функции к CPL-функции уменьшает число строго выпуклых склеек CPL-функции (при определенных предположениях, связанных с гипотезой 1). Частный случай данной гипотезы (когда вогнутая функция — это вогнутая склейка), достаточный для доказательства основного результата, доказан в лемме 19.
- 3) Если CPL-функция не имеет строго выпуклых склеек, то она вогнута (лемма 21).

Ниже, для упрощения понимания, представлена схема доказательства утверждения о выразимости CPL-функций над базисом B_1 . Пусть f — CPL-функция. Тогда:

- 1) Если f не имеет строго выпуклых склеек, то она вогнута (гипотеза 3) и ее можно представить нейронной схемой [11].
- 2) Если f имеет строго выпуклые склейки, то смоделируем (выразим) одну из таких склеек нейронной схемой g_1 и вычтем ее из f . Получим функцию $f_1 = f - g_1$, заданную над теми же гиперплоскостями, что и функция f (гипотеза 1), поэтому число склеек в f_1 не увеличилось. При этом у функции f_1 уменьшилось число строго выпуклых склеек (гипотеза 2).
- 3) Прodelывая пункты 3.1. и 3.2. для получаемых в пункте 3.2 функций $f_j, j \in \mathbb{N}$, получаем в некоторый момент времени функцию $f_N = f - \sum_{i \in \{1, \dots, N\}} g_i$ без строго выпуклых склеек.
- 4) Если у функции f_N нет строго выпуклых склеек, то она — вогнутая (гипотеза 3), поэтому ее можно восстановить некоторой нейронной схемой [11].
- 5) Но $f_N + \sum_{i \in \{1, \dots, N\}} g_i$ по построению в точности совпадает с f , а функции $g_i, i \in \{1, \dots, N\}$, f_N выразимы нейронными схемами. Но тогда и f выразима нейронной схемой, как суперпозиция суммы и схем $g_i, i \in \{1, \dots, N\}$, f_N .

- 6) Далее производится оценка числа N для оценки нелинейной сложности полученной схемы. Нелинейная глубина полученной схемы оценивается исходя из оценки нелинейных глубин схем g_i , $i \in \{1, \dots, N\}$, f_N .

4. Вспомогательные леммы

Далее формулируются и доказываются вспомогательные леммы, которые не являются основными гипотезами, сформулированными в разделе 3, однако активно используются как при доказательстве данных гипотез, так и при доказательстве основного утверждения. Доказательства лемм 1, 2, 3 и 4 можно найти в работе [11].

Лемма 1. Пусть $f(\bar{x}) = a_1 \cdot x_1 + \dots + a_n \cdot x_n + d$ – линейная функция и имеются две точки $\bar{x}, \bar{y} \in \mathbb{R}^n$. Тогда $\forall \alpha \in [0; 1] f((1 - \alpha) \cdot \bar{x} + \alpha \cdot \bar{y}) = (1 - \alpha) \cdot f(\bar{x}) + \alpha \cdot f(\bar{y})$.

Лемма 2. Пусть l – гиперплоскость, определяемая уравнением $a_1 \cdot x_1 + \dots + a_n \cdot x_n + d = 0$, а также l^+ и l^- – соответствующие полупространства, определяемые данной гиперплоскостью. Тогда верны следующие утверждения:

- 1) $l = \partial l^+, l = \partial l^-$.
- 2) l^+, l^- – открытые множества.
- 3) $\bar{l}^+ = l^+ \cup l$.
- 4) $l^+, l^-, \bar{l}^+, \bar{l}^-, l$ – выпуклые множества.

Лемма 3. Для всякого разбиения $\{R^1, \dots, R^s\}$ пространства \mathbb{R}^n выполнены следующие свойства:

- 1) Любой непустой объемный класс R^i является выпуклым открытым множеством.
- 2) Для любого непустого объемного класса R^i верно, что $\bar{R}^i = R^i \cup \partial_{in} R^i$.
- 3) Любой непустой плоский класс содержится в пересечении замыканий как минимум двух непустых объемных классов эквивалентности.

Лемма 4. Пусть $f : \mathbb{R}^n \rightarrow \mathbb{R}$ – выпуклая непрерывная кусочно-линейная функция, заданная над разбиением $\{R^1, \dots, R^s\}$ пространства

\mathbb{R}^n , а R^i, R^j – два произвольных непустых объемных класса из данного разбиения.

Тогда верно, что $\forall \bar{x} \in R^j \ f(\bar{x}) \geq f_{R^i}(\bar{x})$.

Лемма 5. Пусть даны два различных непустых объемных класса R^+, R^- из одного разбиения. Тогда они смежные по $(n-1)$ -мерному классу $R^0 \iff R^0 \neq \emptyset$ и $\sigma(R^+) = (\sigma_1, \dots, \sigma_{u-1}, 1, \sigma_{u+1}, \dots, \sigma_k)$, $\sigma(R^-) = (\sigma_1, \dots, \sigma_{u-1}, -1, \sigma_{u+1}, \dots, \sigma_k)$, $\sigma(R^0) = (\sigma_1, \dots, \sigma_{u-1}, 0, \sigma_{u+1}, \dots, \sigma_k)$, где $\sigma_1, \dots, \sigma_{u-1}, \sigma_{u+1}, \dots, \sigma_k \in \{-1, 1\}$.

Доказательство. (\Leftarrow) : Пусть $R^0 \neq \emptyset$ – $(n-1)$ -мерный класс. Тогда по лемме 3 найдутся непустые объемные классы R^+, R^- такие, что $R^+ \neq R^-$ и $R^0 \subset \overline{R^+} \cap \overline{R^-}$. По определению, они являются смежными по R^0 .

Причем, так как $\sigma(R^0) = (\sigma_1, \dots, \sigma_{u-1}, 0, \sigma_{u+1}, \dots, \sigma_k)$, то из доказательства [11] леммы 3 видно, что $\sigma(R^+) = (\sigma_1, \dots, \sigma_{u-1}, 1, \sigma_{u+1}, \dots, \sigma_k)$, $\sigma(R^-) = (\sigma_1, \dots, \sigma_{u-1}, -1, \sigma_{u+1}, \dots, \sigma_k)$.

В силу единственности класса, обладающего заданной сигнатурой, получаем, что классы R^+, R^- с требуемыми сигнатурами существуют, непусты, объемны и смежны по R^0 .

(\Rightarrow) : Пусть R^+, R^- – смежные по классу R^0 . По определению это означает, что $R^0 \neq \emptyset$, а также, что верно следующее:

$$R^0 \subset \overline{R^+} \cap \overline{R^-} \quad (3)$$

Отметим также, что так как R^0 – $(n-1)$ -мерный, то $\sigma(R^0) = (\sigma_1, \dots, \sigma_{u-1}, 0, \sigma_{u+1}, \dots, \sigma_k)$, где $\sigma_1, \dots, \sigma_{u-1}, \sigma_{u+1}, \dots, \sigma_k \in \{-1, 1\}$.

Далее, по лемме 3 для любого непустого объемного класса R^j верно (4).

$$\overline{R^j} = R^j \cup \partial_{lin} R^j \quad (4)$$

Но тогда, из (3), (4) и таких очевидных фактов, как $R^+ \cap R^- = \emptyset$, $R^- \cap \partial_{lin} R^+ = \emptyset$ и $R^+ \cap \partial_{lin} R^- = \emptyset$, следует (5).

$$R^0 \in \partial_{set \ lin} R^+ \cap \partial_{set \ lin} R^- \quad (5)$$

Но в $\partial_{set \ lin} R^+$ содержатся только классы, полученные занулениями компонент сигнатуры R^+ . Следовательно, $\forall R \in \partial_{set \ lin} R^+$ верно, что $\sigma_i(R) = \sigma_i(R^+)$, если $\sigma_i(R^+) \neq 0$.

Учитывая сказанное и тот факт, что $R^0 \in \partial_{set \ lin} R^+$ (следует из (5)), получаем, что $\sigma_i(R^0) = \sigma_i(R^+) \stackrel{def}{=} \sigma_i \ \forall i \in \{1, \dots, k\} \setminus \{u\}$. Аналогичное верно и для R^- , то есть $\sigma_i(R^0) = \sigma_i(R^-) \stackrel{def}{=} \sigma_i \ \forall i \in \{1, \dots, k\} \setminus \{u\}$.

Таким образом, $\sigma_i(R^+) = \sigma_i(R^-)$ для $\forall i \in \{1, \dots, k\} \setminus \{u\}$.

При этом, по условию, $R^+ \neq R^-$. Следовательно, сигнатуры классов R^+, R^- также различны. А из того, что $\sigma_i(R^+) = \sigma_i(R^-)$ для $\forall i \in \{1, \dots, k\} \setminus \{u\}$, следует, что их сигнатуры могут различаться лишь в u -ой компоненте.

При этом R^+, R^- – объемные, следовательно, в их сигнатурах отсутствуют нули.

Поэтому $\sigma_i(R^+) = \sigma_i(R^-) \in \{-1, 1\} \forall i \in \{1, \dots, k\} \setminus \{u\}$. Без ограничения общности, положим, что $\sigma_u(R^+) = 1$, а $\sigma_u(R^-) = -1$, откуда и следует доказываемое. \square

Лемма 6. Пусть R^+, R^-, R^0 – классы некоторого разбиения $R(L)$, обладающие сигнатурами $\sigma(R^+) = (\sigma_1, \dots, \sigma_{u-1}, 1, \sigma_{u+1}, \dots, \sigma_k)$, $\sigma(R^-) = (\sigma_1, \dots, \sigma_{u-1}, -1, \sigma_{u+1}, \dots, \sigma_k)$ и $\sigma(R^0) = (\sigma_1, \dots, \sigma_{u-1}, 0, \sigma_{u+1}, \dots, \sigma_k)$, причём $R^+, R^- \neq \emptyset$. Тогда:

1. $\overline{R^+} \cup \overline{R^-}$, $\overline{R^+} \cup \overline{R^-}$ и $R^+ \cup R^- \cup R^0$ – выпуклые множества.
2. $\forall \bar{x} \in R^+, \forall \bar{y} \in R^-$ верно, что $\exists \bar{\xi} \in [\bar{x}; \bar{y}] \cap R^0$.

Доказательство. 1. Рассмотрим классы R^+, R^- . По условию, сигнатуры классов R^+, R^- отличаются только в u -ой компоненте и имеют вид $\sigma(R^+) = (\sigma_1, \dots, \sigma_{u-1}, 1, \sigma_{u+1}, \dots, \sigma_k)$, $\sigma(R^-) = (\sigma_1, \dots, \sigma_{u-1}, -1, \sigma_{u+1}, \dots, \sigma_k)$. Это означает, что R^+ и R^- являются решениями систем (6) и (7), соответственно.

$$\left\{ \begin{array}{l} \sigma_1 \cdot l_1(\bar{x}) > 0 \\ \dots \\ \sigma_{u-1} \cdot l_{u-1}(\bar{x}) > 0 \\ l_u(\bar{x}) > 0 \\ \sigma_{u+1} \cdot l_{u+1}(\bar{x}) > 0 \\ \dots \\ \sigma_k \cdot l_k(\bar{x}) > 0 \end{array} \right. \quad (6)$$

$$\left\{ \begin{array}{l} \sigma_1 \cdot l_1(\bar{x}) > 0 \\ \dots \\ \sigma_{u-1} \cdot l_{u-1}(\bar{x}) > 0 \\ l_u(\bar{x}) < 0 \\ \sigma_{u+1} \cdot l_{u+1}(\bar{x}) > 0 \\ \dots \\ \sigma_k \cdot l_k(\bar{x}) > 0 \end{array} \right. \quad (7)$$

Но тогда по пункту 2 леммы 3 верно, что $\overline{R^+}$ и $\overline{R^-}$ являются решениями систем (8) и (9), соответственно.

$$\left\{ \begin{array}{l} \sigma_1 \cdot l_1(\bar{x}) \geq 0 \\ \dots \\ \sigma_{u-1} \cdot l_{u-1}(\bar{x}) \geq 0 \\ l_u(\bar{x}) \geq 0 \\ \sigma_{u+1} \cdot l_{u+1}(\bar{x}) \geq 0 \\ \dots \\ \sigma_k \cdot l_k(\bar{x}) \geq 0 \end{array} \right. \quad (8)$$

$$\left\{ \begin{array}{l} \sigma_1 \cdot l_1(\bar{x}) \geq 0 \\ \dots \\ \sigma_{u-1} \cdot l_{u-1}(\bar{x}) \geq 0 \\ l_u(\bar{x}) \leq 0 \\ \sigma_{u+1} \cdot l_{u+1}(\bar{x}) \geq 0 \\ \dots \\ \sigma_k \cdot l_k(\bar{x}) \geq 0 \end{array} \right. \quad (9)$$

Полученные системы (8) и (9) отличаются только в неравенстве с номером u . Поэтому $\overline{R^+} \cup \overline{R^-}$ можно записать в виде решения системы (10).

$$\left\{ \begin{array}{l} \sigma_1 \cdot l_1(\bar{x}) \geq 0 \\ \dots \\ \sigma_{u-1} \cdot l_{u-1}(\bar{x}) \geq 0 \\ l_u(\bar{x}) \geq 0 \cup l_u(\bar{x}) \leq 0 \\ \sigma_{u+1} \cdot l_{u+1}(\bar{x}) \geq 0 \\ \dots \\ \sigma_k \cdot l_k(\bar{x}) \geq 0 \end{array} \right. \quad (10)$$

Строку с номером u в системе (10) можно, очевидно, поменять с $l_u(\bar{x}) \geq 0 \cup l_u(\bar{x}) \leq 0$ на $l_u(\bar{x}) \in \mathbb{R}$, в результате чего получаем систему (11).

$$\left\{ \begin{array}{l} \sigma_1 \cdot l_1(\bar{x}) \geq 0 \\ \dots \\ \sigma_{u-1} \cdot l_{u-1}(\bar{x}) \geq 0 \\ l_u(\bar{x}) \in \mathbb{R} \\ \sigma_{u+1} \cdot l_{u+1}(\bar{x}) \geq 0 \\ \dots \\ \sigma_k \cdot l_k(\bar{x}) \geq 0 \end{array} \right. \quad (11)$$

Но \mathbb{R} – выпуклое множество, как и множества, задаваемые неравенствами $\sigma_i \cdot l_i(\bar{x}) \geq 0$, $i \in \{1, \dots, u-1, u+1, \dots, k\}$. То есть $\overline{R^+} \cup \overline{R^-}$ задается в виде пересечения конечного числа выпуклых множеств, откуда следует, что множество $\overline{R^+} \cup \overline{R^-}$ – выпукло. Аналогично доказываются и остальные случаи.

2. Возьмем $\forall \bar{x} \in R^+, \forall \bar{y} \in R^-$ и рассмотрим отрезок $[\bar{x}; \bar{y}]$. Очевидно, что $R^+, R^- \subset R^+ \cup R^- \cup R^0$, поэтому верно (12).

$$\bar{x}, \bar{y} \in R^+ \cup R^- \cup R^0 \quad (12)$$

Но $R^+ \cup R^- \cup R^0$ – выпуклое множество, поэтому из (12) следует, что $[\bar{x}; \bar{y}] \subset R^+ \cup R^- \cup R^0$. Последнее означает, что $\forall \bar{\xi} \in [\bar{x}; \bar{y}] \sigma_u(\bar{\xi}) \in \{-1, 0, 1\}$, а $\sigma_i(\bar{\xi}) = \sigma_i(R^+) = \sigma_i(R^-)$ при $i \in \{1, \dots, k\} \setminus \{u\}$.

Далее, так как $\sigma_u(\bar{x}) = 1, \sigma_u(\bar{y}) = -1$, то $l_u(\bar{x}) > 0$ и $l_u(\bar{y}) < 0$. Рассмотрим $t = \frac{l_u(\bar{x})}{l_u(\bar{x}) - l_u(\bar{y})}$. Очевидно, что $t \in (0; 1)$. Тогда t порождает некоторую точку $\bar{\xi} = (1-t) \cdot \bar{x} + t \cdot \bar{y} \in (\bar{x}; \bar{y}) \subset [\bar{x}; \bar{y}]$.

$$\begin{aligned} \text{Причем } l_u(\bar{\xi}) &= l_u((1-t) \cdot \bar{x} + t \cdot \bar{y}) \stackrel{\text{лемма 1}}{=} (1-t) \cdot l_u(\bar{x}) + t \cdot l_u(\bar{y}) = \\ &= \left(1 - \frac{l_u(\bar{x})}{l_u(\bar{x}) - l_u(\bar{y})}\right) \cdot l_u(\bar{x}) + \frac{l_u(\bar{x})}{l_u(\bar{x}) - l_u(\bar{y})} \cdot l_u(\bar{y}) = \frac{l_u(\bar{x}) - l_u(\bar{y}) - l_u(\bar{x})}{l_u(\bar{x}) - l_u(\bar{y})} \cdot l_u(\bar{x}) + \frac{l_u(\bar{x}) \cdot l_u(\bar{y})}{l_u(\bar{x}) - l_u(\bar{y})} = \\ &= \frac{l_u(\bar{x}) \cdot l_u(\bar{y})}{l_u(\bar{x}) - l_u(\bar{y})} - \frac{l_u(\bar{x}) \cdot l_u(\bar{y})}{l_u(\bar{x}) - l_u(\bar{y})} = 0. \end{aligned}$$

Таким образом, $l_u(\bar{\xi}) = 0$, а $\sigma_i(\bar{\xi}) = \sigma_i(R^+) = \sigma_i(R^-) \forall i \in \{1, \dots, k\} \setminus \{u\}$. Следовательно, $\bar{\xi} \in R^0$. При этом, по построению, $\bar{\xi} \in (\bar{x}; \bar{y}) \subset [\bar{x}; \bar{y}]$. То есть нашлась точка $\bar{\xi} \in R^0 \cap [\bar{x}; \bar{y}]$. □

Лемма 7. Если R^+, R^- – смежные классы, а R^0 – пограничный класс, то:

1. $\overline{R^+} \cup \overline{R^-}$, $\overline{R^+ \cup R^-}$ и $R^+ \cup R^0 \cup R^-$ – выпуклые множества.
2. $\forall \bar{x} \in R^+, \forall \bar{y} \in R^-$ верно, что $\exists \bar{\xi} \in [\bar{x}; \bar{y}] \cap R^0$.

Доказательство. Прямое следствие лемм 5 и 6. □

Лемма 5 устанавливает некую взаимосвязь между смежными классами и поведением их сигнатур, что существенно упрощает работу по

определению смежных классов. Однако на практике проверка условия $R^0 \neq \emptyset$ иногда является избыточной, так как часто требуется установить просто факт смежности классов без знания чего-либо о пограничном классе R^0 , по которому данные классы являются смежными.

Поэтому взаимосвязь из леммы 5 можно существенно усилить, убрав условие $R^0 \neq \emptyset$ и сведя проверку смежности реально существующих в пространстве \mathbb{R}^n (то есть непустых) классов к простой проверке поведения их сигнатур. Данная усиленная взаимосвязь формулируется и доказывается в следующей лемме.

Лемма 8. *Два непустых, различных объемных класса R^+, R^- являются смежными $\iff \sigma(R^+) = (\sigma_1, \dots, \sigma_{u-1}, 1, \sigma_{u+1}, \dots, \sigma_k)$, $\sigma(R^-) = (\sigma_1, \dots, \sigma_{u-1}, -1, \sigma_{u+1}, \dots, \sigma_k)$.*

Доказательство. (\Rightarrow) : Если два непустых объемных класса R^+, R^- смежны, то по определению $\exists R^0 \neq \emptyset$, являющийся $(n-1)$ -мерным, такой, что $R^0 \subset \overline{R^+} \cap \overline{R^-}$.

То есть классы R^+, R^- являются смежными по некоторому $(n-1)$ -мерному классу R^0 . Но тогда, по лемме 5, $\sigma(R^+) = (\sigma_1, \dots, \sigma_{u-1}, 1, \sigma_{u+1}, \dots, \sigma_k)$, $\sigma(R^-) = (\sigma_1, \dots, \sigma_{u-1}, -1, \sigma_{u+1}, \dots, \sigma_k)$.

(\Leftarrow) : Пусть $\sigma(R^+) = (\sigma_1, \dots, \sigma_{u-1}, 1, \sigma_{u+1}, \dots, \sigma_k)$, $\sigma(R^-) = (\sigma_1, \dots, \sigma_{u-1}, -1, \sigma_{u+1}, \dots, \sigma_k)$ и при этом R^+, R^- – непустые и объемные. Тогда по пункту 2 леммы 6 $\forall \bar{x} \in R^+, \forall \bar{y} \in R^- \exists \bar{\xi} \in [\bar{x}; \bar{y}] \cap R^0$, где R^0 – класс, обладающий сигнатурой $\sigma(R^0) = (\sigma_1, \dots, \sigma_{u-1}, 0, \sigma_{u+1}, \dots, \sigma_k)$.

Но тогда получаем, что точка $\bar{\xi}$ имеет сигнатуру $\sigma(\bar{\xi}) = (\sigma_1, \dots, \sigma_{u-1}, 0, \sigma_{u+1}, \dots, \sigma_k)$, откуда следует, что $\bar{\xi} \in R^0$. Из последнего следует, что $R^0 \neq \emptyset$. Более того, так как $\sigma(R^0)$ содержит всего один нуль, то данный класс является $(n-1)$ -мерным.

Так как все условия леммы 5 выполнены, то $R^+ | R^-$. \square

Лемма 9. *Пусть $f(\bar{x})$ – CPL-функция, заданная над разбиением $\{R^1, \dots, R^s\}$, порожденным гиперплоскостями $\{l_1, \dots, l_k\}$. И пусть также $R^+, R^- \in \{R^1, \dots, R^s\}$ – смежные классы, а $R^0 \in \{R^1, \dots, R^s\}$ – пограничный класс. Тогда:*

1. $\forall \bar{x} \in R^0 f(\bar{x}) = f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$.
2. Если $\forall \bar{x} \in R^0 f(\bar{x}) = f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$ и $R^0 \subset l$, где l – некоторая гиперплоскость, то $\forall \bar{x} \in l f(\bar{x}) = f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$.

Аналогичное утверждение верно для выражения $n(\bar{x}) = C$, где $n(\bar{x})$ – линейная функция, а C – константа. Другими словами, если $\forall \bar{x} \in R^0 n(\bar{x}) = C$ и $R^0 \subset l$, где l – некоторая гиперплоскость, то $\forall \bar{x} \in l n(\bar{x}) = C$.

3. Если $\exists \bar{x} \in R^+ \cup R^- f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$, то $f_{R^+} = f_{R^-}$ (то есть $\forall \bar{x} \in \mathbb{R}^n f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$).

4. Если $\exists \bar{x} \in R^+ f_{R^+}(\bar{x}) > f_{R^-}(\bar{x})$, то $\forall \bar{x} \in l^+ f_{R^+}(\bar{x}) > f_{R^-}(\bar{x})$ и $\forall \bar{x} \in l^- f_{R^+}(\bar{x}) < f_{R^-}(\bar{x})$.

5. Если $\exists \bar{x} \in R^+ f_{R^+}(\bar{x}) < f_{R^-}(\bar{x})$, то $\forall \bar{x} \in l^+ f_{R^+}(\bar{x}) < f_{R^-}(\bar{x})$ и $\forall \bar{x} \in l^- f_{R^+}(\bar{x}) > f_{R^-}(\bar{x})$.

Доказательство. **1.** Пусть $f(\bar{x})$ – CPL-функция, R^+, R^- – смежные классы, а R^0 – пограничный при них класс. Рассмотрим $\forall \bar{x}^* \in R^0$. В силу того, что $R^0 \subset \overline{R^+} \cap \overline{R^-} \subset \overline{R^+}, \overline{R^-}$, получаем (13).

$$\exists \{\bar{x}_n\}_{n \in \mathbb{N}} \subset R^+, \exists \{\bar{y}_n\}_{n \in \mathbb{N}} \subset R^- : \lim_{n \rightarrow +\infty} \bar{x}_n = \lim_{n \rightarrow +\infty} \bar{y}_n = \bar{x}^* \quad (13)$$

При этом, так как $\forall \bar{x} \in R^+ f(\bar{x}) = f_{R^+}(\bar{x})$, то $\forall n \in \mathbb{N} f(\bar{x}_n) = f_{R^+}(\bar{x}_n)$. Аналогично, $\forall n \in \mathbb{N} f(\bar{y}_n) = f_{R^-}(\bar{y}_n)$. Но тогда верно (14)

$$\lim_{n \rightarrow +\infty} f(\bar{x}_n) = \lim_{n \rightarrow +\infty} f_{R^+}(\bar{x}_n), \lim_{n \rightarrow +\infty} f(\bar{y}_n) = \lim_{n \rightarrow +\infty} f_{R^-}(\bar{y}_n) \quad (14)$$

В силу непрерывности функций f, f_{R^+}, f_{R^-} , можно внести пределы под данные функции, в результате из (14) получим (15).

$$f\left(\lim_{n \rightarrow +\infty} \bar{x}_n\right) = f_{R^+}\left(\lim_{n \rightarrow +\infty} \bar{x}_n\right), f\left(\lim_{n \rightarrow +\infty} \bar{y}_n\right) = f_{R^-}\left(\lim_{n \rightarrow +\infty} \bar{y}_n\right) \quad (15)$$

Переходя к пределу в (15) и учитывая (13), получаем, что $f(\bar{x}^*) = f_{R^+}(\bar{x}^*)$, $f(\bar{x}^*) = f_{R^-}(\bar{x}^*)$. Отсюда и следует, что $f(\bar{x}^*) = f_{R^+}(\bar{x}^*) = f_{R^-}(\bar{x}^*)$.

2. Пусть $\forall \bar{x} \in R^0 f(\bar{x}) = f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$ и $R^0 \subset l$. Отметим, что, по определению, множество R^0 задается системой неравенств (16).

$$\begin{cases} \sigma_1 \cdot l_1(\bar{x}) > 0 \\ \dots \\ \sigma_{i-1} \cdot l_{i-1}(\bar{x}) > 0 \\ \sigma_i \cdot l_i(\bar{x}) = 0 \\ \sigma_{i+1} \cdot l_{i+1}(\bar{x}) > 0 \\ \dots \\ \sigma_k \cdot l_k(\bar{x}) > 0 \end{cases} \quad (16)$$

Отметим, что $\sigma_i \cdot l_i(\bar{x})$ можно представить в виде $a_1 \cdot x_1 + \dots + a_n \cdot x_n + d$, где $a_1, \dots, a_n, d \in \mathbb{R}$ – некоторые константы, причем a_1, \dots, a_n не равны нулю одновременно. Без ограничения общности, будем считать, что $a_n \neq$

0. Но тогда уравнение $\sigma_i \cdot l_i(\bar{x}) = 0$ можно записать в виде выражения (17), в котором $\tilde{a}_i = a_i/a_n, i \in \{1, \dots, n-1\}, \tilde{d} = d/a_n$.

$$x_n = -\tilde{a}_1 \cdot x_1 - \dots - \tilde{a}_{n-1} \cdot x_{n-1} - \tilde{d} \quad (17)$$

Заменяя в (16) переменную x_n на линейную комбинацию значений $x_1, \dots, x_{n-1}, 1$ по уравнению (17), получаем, что систему равенств и неравенств (16) можно переписать в виде эквивалентной системы (18), в которой $l'_j(x_1, \dots, x_{n-1}), j = 1, \dots, k$ – линейные функции, а $l'_i(x_1, \dots, x_{n-1}) = -\tilde{a}_1 \cdot x_1 - \dots - \tilde{a}_{n-1} \cdot x_{n-1} - \tilde{d}$.

$$\begin{cases} l'_1(x_1, \dots, x_{n-1}) > 0 \\ \dots \\ l'_{i-1}(x_1, \dots, x_{n-1}) > 0 \\ x_n = l'_i(x_1, \dots, x_{n-1}) \\ l'_{i+1}(x_1, \dots, x_{n-1}) > 0 \\ \dots \\ l'_k(x_1, \dots, x_{n-1}) > 0 \end{cases} \quad (18)$$

Очевидно, что система (19), полученная из (18) удалением уравнения $x_n = l'_i(x_1, \dots, x_{n-1})$, является системой строгих неравенств, то есть задает некоторый объемный класс в пространстве \mathbb{R}^{n-1} . По лемме 3 данный класс является открытым множеством, поэтому (19) задает открытое множество R_{n-1}^0 в пространстве \mathbb{R}^{n-1} .

$$\begin{cases} l'_1(x_1, \dots, x_{n-1}) > 0 \\ \dots \\ l'_{i-1}(x_1, \dots, x_{n-1}) > 0 \\ l'_{i+1}(x_1, \dots, x_{n-1}) > 0 \\ \dots \\ l'_k(x_1, \dots, x_{n-1}) > 0 \end{cases} \quad (19)$$

Далее введем отображения $\pi : \mathbb{R}^n \rightarrow \mathbb{R}^{n-1}$ и $\pi^{-1} : \mathbb{R}^{n-1} \rightarrow \mathbb{R}^n$, действующие по законам $\pi(x_1, \dots, x_n) = (x_1, \dots, x_{n-1})$ и $\pi^{-1}(x_1, \dots, x_{n-1}) = (x_1, \dots, x_{n-1}, l'_i(x_1, \dots, x_{n-1}))$, соответственно.

Выберем некоторую точку $\bar{x} \in R^0$ и рассмотрим точку $\bar{x}' = (x_1, \dots, x_{n-1}) = \pi(\bar{x}) \in \mathbb{R}^{n-1}$. Из построения множества R_{n-1}^0 и того факта, что $\bar{x} \in R^0$, выполняется $\bar{x}' \in R_{n-1}^0$. И так как R_{n-1}^0 – открыто, то существует некоторая окрестность $O_\varepsilon(\bar{x}')$ такая, что $O_\varepsilon(\bar{x}') \subset R_{n-1}^0 \subset \mathbb{R}^{n-1}$.

Далее возьмем произвольную точку $\bar{y} = (y_1, \dots, y_n) \in l$ и рассмотрим точку $\bar{y}' = (y_1, \dots, y_{n-1}) = \pi(\bar{y}) \in \mathbb{R}^{n-1}$.

Соединим точки $\overline{x'}$ и $\overline{y'}$ отрезком $[\overline{x'}; \overline{y'}]$. Очевидно, что $\exists \overline{\xi'} \in (\overline{x'}; \overline{y'}) \cap O_\varepsilon(\overline{x'})$, где $(\overline{x'}; \overline{y'}) \subset [\overline{x'}; \overline{y'}]$. Рассмотрим точки $\overline{x} = \pi^{-1}(\overline{x'})$, $\overline{\xi} = \pi^{-1}(\overline{\xi'})$. По построению R_{n-1}^0 следует, что $\overline{x}, \overline{\xi} \in R^0$.

Тогда, по условию, для точек $\overline{x}, \overline{\xi}$ верно, что $f_{R^+}(\overline{x}) = f_{R^-}(\overline{x})$ и $f_{R^+}(\overline{\xi}) = f_{R^-}(\overline{\xi})$. Отметим также, что $\overline{\xi} \in (\overline{x}; \overline{y}) \subset [\overline{x}; \overline{y}]$. Действительно, пусть $t_{\overline{\xi'}} \in (0; 1)$ – параметр интервала $(\overline{x'}; \overline{y'})$, задающий точку $\overline{\xi'}$. Это означает, что $\overline{\xi'} = (\xi_1, \dots, \xi_{n-1})$, где ξ_i , $i = 1, \dots, n-1$ определены по формуле (20).

$$\xi_i = (1-t) \cdot x_i + t \cdot y_i, \quad i = 1, \dots, n-1 \quad (20)$$

Но тогда, по определению π^{-1} , $\overline{\xi} = (\xi_1, \dots, \xi_{n-1}, \xi_n)$, где $\xi_n = -\tilde{a}_1 \cdot \xi_1 - \dots - \tilde{a}_{n-1} \cdot \xi_{n-1} - \tilde{d}$. Выражая в последней формуле значения ξ_i , $i = 1, \dots, n-1$, используя выражение (20), получаем, что $\xi_n = -\tilde{a}_1 \cdot ((1-t_{\overline{\xi'}}) \cdot x_1 + t_{\overline{\xi'}} \cdot y_1) - \dots - \tilde{a}_{n-1} \cdot ((1-t_{\overline{\xi'}}) \cdot x_{n-1} + t_{\overline{\xi'}} \cdot y_{n-1}) - \tilde{d} = -\tilde{a}_1 \cdot ((1-t_{\overline{\xi'}}) \cdot x_1 - \tilde{a}_1 \cdot (t_{\overline{\xi'}} \cdot y_1) - \dots - \tilde{a}_{n-1} \cdot ((1-t_{\overline{\xi'}}) \cdot x_{n-1}) - \tilde{a}_{n-1} \cdot (t_{\overline{\xi'}} \cdot y_{n-1}) - \tilde{d} = (1-t_{\overline{\xi'}}) \cdot (-\tilde{a}_1 \cdot x_1 - \dots - \tilde{a}_{n-1} \cdot x_{n-1} - \tilde{d}) + t_{\overline{\xi'}} \cdot (-\tilde{a}_1 \cdot y_1 - \dots - \tilde{a}_{n-1} \cdot y_{n-1} - \tilde{d}) = (1-t_{\overline{\xi'}}) \cdot x_n + t_{\overline{\xi'}} \cdot y_n$.

Таким образом, $\xi_i = (1-t_{\overline{\xi'}}) \cdot x_i + t_{\overline{\xi'}} \cdot y_i$, $i = 1, \dots, n$, где $t_{\overline{\xi'}} \in (0; 1)$, откуда по определению следует, что $\overline{\xi} = (\xi_1, \dots, \xi_{n-1}, \xi_n) \in (\overline{x}; \overline{y}) \subset [\overline{x}; \overline{y}]$. Причем отметим, что точку $\overline{\xi}$ на промежутке $(\overline{x}; \overline{y})$ задает тот же параметр $t_{\overline{\xi'}}$, который использовался при задании точки $\overline{\xi'}$ на промежутке $(\overline{x'}; \overline{y'})$. Другими словами, $t_{\overline{\xi'}} = t_{\overline{\xi}}$, где $t_{\overline{\xi}}$ – параметр, задающий точку $\overline{\xi} \in (\overline{x}; \overline{y}) \subset [\overline{x}; \overline{y}]$.

Рассмотрим разность $A(t) = f_{R^+}(t) - f_{R^-}(t)$ сечений $f_{R^+}(t) = f_{R^+}((1-t) \cdot \overline{x} + t \cdot \overline{y})$, $f_{R^-}(t) = f_{R^-}((1-t) \cdot \overline{x} + t \cdot \overline{y})$ линейных частей $f_{R^+}(\overline{x})$, $f_{R^-}(\overline{x})$ на прямой $(\overline{x}; \overline{y})_\infty$.

По построению $\overline{\xi}$, верно, что $A(t_{\overline{\xi}}) = 0$. Но из того, что $A(0) = 0$, $A(t_{\overline{\xi}}) = 0$, $t_{\overline{\xi}} \neq 0$, а также из того факта, что $A(t)$ – линейная функция одного аргумента, следует, что $\forall t \in \mathbb{R} A(t) = 0$, откуда следует, что $A(1) = 0$. А это означает, по определению, что $f_{R^+}(\overline{y}) = f_{R^-}(\overline{y})$.

Таким образом, $\forall \overline{y} \in l f_{R^+}(\overline{y}) = f_{R^-}(\overline{y})$. Получили доказываемое.

Для доказательства пункта 2 применительно к выражению $n(\overline{x}) = C$ достаточно рассмотреть функции $f_{R^+}(\overline{x}) = n(\overline{x})$, $f_{R^-}(\overline{x}) = C$, абстрагировавшись от того, что $f_{R^+}(\overline{x})$, $f_{R^-}(\overline{x})$ – линейные части некоторой CPL-функции, после чего применить уже доказанную часть данного пункта.

3. Покажем, что, если $\exists \overline{x} \in R^+ \cup R^- : f_{R^+}(\overline{x}) = f_{R^-}(\overline{x})$, то $f_{R^+} = f_{R^-}$. Выберем точку $\overline{x} \in R^+ \cup R^- : f_{R^+}(\overline{x}) = f_{R^-}(\overline{x})$. Без ограничения общности, будем считать, что $\overline{x} \in R^+$.

Рассмотрим R^0 – пограничный класс для смежных классов $R^+ \cup R^-$. Очевидно, что среди гиперплоскостей $\{l_1, \dots, l_k\}$, порождающих разбиение

ние $\{R^1, \dots, R^s\}$, существует такая гиперплоскость l , что $R^0 \subset l$. Тогда по лемме 5, $R^+ \subset l^+$ и $R^- \subset l^-$.

Далее возьмем $\forall \bar{y} \in l^-$. Очевидно, что $\exists \bar{\xi} \in l \cap (\bar{x}; \bar{y})$. Но по пункту 1 данной леммы $\forall \bar{\eta} \in R^0 f_{R^+}(\bar{\eta}) = f_{R^-}(\bar{\eta})$, а тогда по пункту 2 данной леммы $\forall \bar{\eta} \in l f_{R^+}(\bar{\eta}) = f_{R^-}(\bar{\eta})$, в частности $f_{R^+}(\bar{\xi}) = f_{R^-}(\bar{\xi})$.

Рассмотрим функцию $A(t) = f_{R^+}(t) - f_{R^-}(t)$, где $f_{R^+}(t)$, $f_{R^-}(t)$ – сечения функций $f_{R^+}(\bar{x})$, $f_{R^-}(\bar{x})$ прямой $(\bar{x}; \bar{y})_\infty$. По условию для выбранного $\bar{x} \in R^+$ верно, что $f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$, поэтому $A(0) = 0$, а так как $f_{R^+}(\bar{\xi}) = f_{R^-}(\bar{\xi})$, то $A(t_{\bar{\xi}}) = 0$, где $t_{\bar{\xi}} \in (0; 1) : \bar{\xi} = (1 - t_{\bar{\xi}}) \cdot \bar{x} + t_{\bar{\xi}} \cdot \bar{y}$.

Но тогда, в силу того, что $A(t)$ – линейная функция одного аргумента, то из $A(0) = 0$, $A(t_{\bar{\xi}}) = 0$ и того факта, что $t_{\bar{\xi}} \neq 0$, получаем, что $\forall t \in \mathbb{R} A(t) = 0$. Тогда и $A(1) = 0$, откуда следует, что $f_{R^+}(\bar{y}) = f_{R^-}(\bar{y})$.

Но тогда, взяв $\forall \bar{y} \in l^-$, $\forall \bar{x} \in l^+$ и рассуждая аналогично (построив отрезок $[\bar{y}; \bar{x}]$ и рассмотрев на нем поведение функции $A(t)$, построенной на сечениях функций $f_{R^+}(\bar{x})$, $f_{R^-}(\bar{x})$ прямой $(\bar{y}; \bar{x})_\infty$), получаем, что $\forall \bar{x} \in l^+ f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$.

Таким образом, из всего вышесказанного получили, что $\forall \bar{x} \in l^+, l^-, l f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$. Но тогда, в силу того, что $l^+ \cup l \cup l^- = \mathbb{R}^n$, получаем доказываемое.

4. Пусть $\exists \bar{x} \in R^+ : f_{R^+}(\bar{x}) > f_{R^-}(\bar{x})$. Покажем, что тогда $\forall \bar{x} \in l^+ : f_{R^+}(\bar{x}) > f_{R^-}(\bar{x})$ и $\forall \bar{x} \in l^- : f_{R^+}(\bar{x}) < f_{R^-}(\bar{x})$.

Доказывается по той же схеме, что и пункт 3. Возьмем $\bar{x} \in R^+ : f_{R^+}(\bar{x}) > f_{R^-}(\bar{x})$ и выберем $\forall \bar{y} \in l^-$. После чего рассмотрим $A(t) = f_{R^+}(t) - f_{R^-}(t)$, где $f_{R^+}(t)$, $f_{R^-}(t)$ – сечения функций $f_{R^+}(\bar{x})$, $f_{R^-}(\bar{x})$ прямой $(\bar{x}; \bar{y})_\infty$.

Далее, по построению, $\exists \bar{\xi} \in (\bar{x}; \bar{y}) \cap l$. По определению выражение $\bar{\xi} \in (\bar{x}; \bar{y})$ означает, что $\exists t_{\bar{\xi}} \in (0; 1) : \bar{\xi} = (1 - t_{\bar{\xi}}) \cdot \bar{x} + t_{\bar{\xi}} \cdot \bar{y}$.

Но тогда, в силу того, что $\forall \bar{x} \in l f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$, то $A(t_{\bar{\xi}}) = 0$. А так как для выбранного $\bar{x} \in R^+$ верно $f_{R^+}(\bar{x}) > f_{R^-}(\bar{x})$, то $A(0) > 0$.

Таким образом, получили, что $t_{\bar{\xi}} > 0$, $A(0) > 0$, $A(t_{\bar{\xi}}) = 0$. Причем, так как $A(t)$ – линейная функция одного аргумента, то $\forall t > t_{\bar{\xi}} A(t) < 0$ и $\forall t < t_{\bar{\xi}} A(t) > 0$. Но тогда $A(1) < 0$, так как $1 > t_{\bar{\xi}}$. Следовательно, $f_{R^+}(\bar{y}) < f_{R^-}(\bar{y})$.

Но тогда, взяв $\forall \bar{y} \in l^-$, $\forall \bar{x} \in l^+$ и рассуждая аналогично, получаем, что $\forall \bar{x} \in l^+ f_{R^+}(\bar{x}) > f_{R^-}(\bar{x})$.

Итак, получили, что $\forall \bar{x} \in l^+ f_{R^+}(\bar{x}) > f_{R^-}(\bar{x})$, $\forall \bar{x} \in l^- f_{R^+}(\bar{x}) < f_{R^-}(\bar{x})$.

5. Доказывается полностью аналогично пункту 4. □

Лемма 10. Пусть $f(\bar{x}) : \mathbb{R}^n \rightarrow \mathbb{R}$ – кусочно-линейная функция, заданная над гиперплоскостями $\{l_1, \dots, l_k\}$. Тогда можно добавить к гипер-

плоскостям $\{l_1, \dots, l_k\}$ гиперплоскость l_{k+1} и считать, что $f(\bar{x})$ задана над гиперплоскостями $\{l_1, \dots, l_k, l_{k+1}\}$ (то есть разбиение, полученное от нового набора гиперплоскостей, тоже можно считать валидирующим для данной кусочно-линейной функции).

Доказательство. Пусть $f(\bar{x})$ задана над гиперплоскостями $L = \{l_1, \dots, l_k\}$. Это означает, что классы R^i из разбиения $\{R^1, \dots, R^s\}$ пространства \mathbb{R}^n гиперплоскостями L обладают сигнатурами $\sigma(R^i) = (\sigma_1, \dots, \sigma_k)$, где k – число гиперплоскостей, а также выполняется, что $\forall \bar{x} \in R^i \in R(L) f(\bar{x}) = f_{R^i}(\bar{x})$, где $f_{R^i}(\bar{x})$ – линейная функция. Но тогда, добавив новую гиперплоскость l_{k+1} , мы получим набор гиперплоскостей $\{l_1, \dots, l_k, l_{k+1}\}$ и классы $Q_{\sigma_{k+1}}^i$, обладающие сигнатурами $\sigma(Q_{\sigma_{k+1}}^i) = (\sigma_1, \sigma_2, \dots, \sigma_{k+1})$, $i \in \{1, \dots, s\}$, $\sigma_{k+1} \in \{-1, 0, 1\}$ (для удобства сделана двойная индексация получившихся классов).

Причем очевидно, что для получения исходной картины (исходного разбиения пространства \mathbb{R}^n гиперплоскостями $\{l_1, \dots, l_k\}$ на классы), достаточно рассмотреть классы $R^i = Q_1^i \cup Q_0^i \cup Q_{-1}^i$, где $\sigma(Q_q^i) = (\sigma_1, \dots, \sigma_k, q)$, $q \in \{-1, 0, 1\}$. К тому же, также очевидно, что все пустые классы могут разбиться лишь в объединение пустых классов.

Но тогда имеем, что если $\forall \bar{x} \in R^i \in R(L) f(\bar{x}) = f_{R^i}(\bar{x})$, то для тех из классов Q_1^i, Q_0^i, Q_{-1}^i , которые не являются пустыми, верно, что $\forall \bar{x} \in Q_1^i \subset R^i, Q_0^i \subset R^i, Q_{-1}^i \subset R^i f(\bar{x}) = f_{R^i}(\bar{x})$. То есть $f(\bar{x})$ по определению является кусочно-линейной функцией над классами $Q_{\sigma_{k+1}}^i$, $i \in \{1, \dots, s\}$, $\sigma_{k+1} \in \{-1, 0, 1\}$. Но классы $Q_{\sigma_{k+1}}^i$ порождаются гиперплоскостями $\{l_1, \dots, l_k, l_{k+1}\}$, откуда и следует доказываемое. \square

Лемма 11. Пусть $f(\bar{x})$ – CPL-функция. Тогда верно, что:

- 1) Для любых двух смежных классов R^+, R^- существует склейка;
- 2) Для любых двух смежных классов R^+, R^- верно, что их склейку можно представить либо в виде выпуклой склейки, либо в виде вогнутой склейки.

Доказательство. Пусть R^+, R^- – смежные классы, а класс R^0 является пограничным для R^+, R^- . Рассмотрим три случая:

- Пусть $\exists \bar{x} \in R^+ f_{R^+}(\bar{x}) > f_{R^-}(\bar{x})$. Тогда по пункту 4 леммы 9 верно, что $\forall \bar{x} \in R^+ f(\bar{x}) = f_{R^+}(\bar{x}) > f_{R^-}(\bar{x})$ и $\forall \bar{x} \in R^- f_{R^+}(\bar{x}) < f_{R^-}(\bar{x}) = f(\bar{x})$ (так как, очевидно, что $R^+ \subset l^+, R^- \subset l^-$). Отсюда немедленно следует, что $\forall \bar{x} \in R^+ f(\bar{x}) = f_{R^+}(\bar{x}) = \max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$. Полностью аналогично, получаем, что $\forall \bar{x} \in R^- f(\bar{x}) = f_{R^-}(\bar{x}) = \max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$.

А по пункту 1 леммы 9 $\forall \bar{x} \in R^0 f(\bar{x}) = f_{R^+}(\bar{x}) = f_{R^-}(\bar{x}) = \max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$. Таким образом, в данном случае $\forall \bar{x} \in R^0 \cup R^+ \cup R^- f(\bar{x}) = \max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$.

- Пусть $\exists \bar{x} \in R^+ f_{R^+}(\bar{x}) < f_{R^-}(\bar{x})$. Тогда по пункту 5 леммы 9 верно, что $\forall \bar{x} \in R^+ f_{R^+}(\bar{x}) = f(\bar{x}) < f_{R^-}(\bar{x})$ и $\forall \bar{x} \in R^- f_{R^+}(\bar{x}) > f_{R^-}(\bar{x}) = f(\bar{x})$. При этом по пункту 1 леммы 9 $\forall \bar{x} \in R^0$ выполняется, что $f(\bar{x}) = f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$.

Получили, что $\forall \bar{x} \in R^+ \cup R^- \cup R^0 f(\bar{x}) = \min(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$.

- Пусть $\forall \bar{x} \in R^+ f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$. Тогда по пункту 3 леммы 9 получаем, что $\forall \bar{x} \in \mathbb{R}^n f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$.

В частности, $\forall \bar{x} \in R^+ \cup R^- \cup R^0 f_{R^+}(\bar{x}) = f_{R^-}(\bar{x})$. Поэтому $\forall \bar{x} \in R^+ f(\bar{x}) = f_{R^+}(\bar{x}) = \max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x})) = \min(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$ и $\forall \bar{x} \in R^- f(\bar{x}) = f_{R^-}(\bar{x}) = \max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x})) = \min(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$. Учитывая, что $\forall \bar{x} \in R^0 f(\bar{x}) = f_{R^+}(\bar{x}) = f_{R^-}(\bar{x}) = \max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x})) = \min(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$, получаем, что в данном случае выполняется $\forall \bar{x} \in R^+ \cup R^- \cup R^0 f(\bar{x}) = \max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x})) = \min(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$.

Так как всегда, очевидно, верен один из трех рассмотренных случаев, то верен пункт 1 леммы. А так как по определению склейки всегда выражаются функциями $\min(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$ или $\max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$, то любую склейку можно считать выпуклой или вогнутой, поэтому пункт 2 леммы тоже верен. \square

Далее сформулируем и докажем несколько лемм, необходимых для понимания доказательства всего лишь одного, кажущегося на первый взгляд очевидным, факта: если у функции нет чисто выпуклых склеек, то она — вогнутая (сам факт доказывается в следующем разделе).

На деле при доказательстве данного факта возникают дополнительные вопросы о характере поведения классов эквивалентности, такие, как:

- Можно ли связать два произвольных непустых объемных класса цепочкой смежных классов? (то есть, построить такую цепочку классов с началом в первом объемном классе и концом во втором объемном классе, в которой два любых соседних класса являются смежными);

- Точно ли элементы последовательности множеств $\partial_S^i(R^{(1)})$ когда-нибудь станут равными множеству всех непустых объемных классов эквивалентности или же часть непустых объемных классов так никогда и не войдет в последовательность $\partial_S^i(R^{(1)})$;

- Какие элементы добавляются к $\partial_S^i(R^{(1)})$ при переходе от $\partial_S^i(R^{(1)})$ к $\partial_S^{i+1}(R^{(1)})$;

- Стабилизируется ли цепь $\partial_S^i(R^{(1)})$ и есть ли какие-нибудь критерии стабилизируемости данной цепи.

Для доказательства всех вышеописанных фактов в определениях вводились так называемые укрупнения. И рассмотрение сформулированных выше вопросов мы начнем с доказательств некоторых свойств данных укрупнений.

Лемма 12. Пусть $L = \{l_1, \dots, l_k\}$ - набор гиперплоскостей. Тогда при укрупнении $L' = L \setminus \{l_i\}$ любой из объемных классов $U \in V(L')$ либо равен одному из классов в $V(L)$ (равенство множеств), либо образован, как $U = R^+ \cup R^0 \cup R^-$ для некоторых непустых классов $R^+, R^0, R^- \in R(L)$, из которых R^+, R^- - объемные (и не равные друг другу), а R^0 - $(n-1)$ -мерный. Причем классы R^+, R^- являются смежными по классу R^0 (см. рис. 1 и 2).

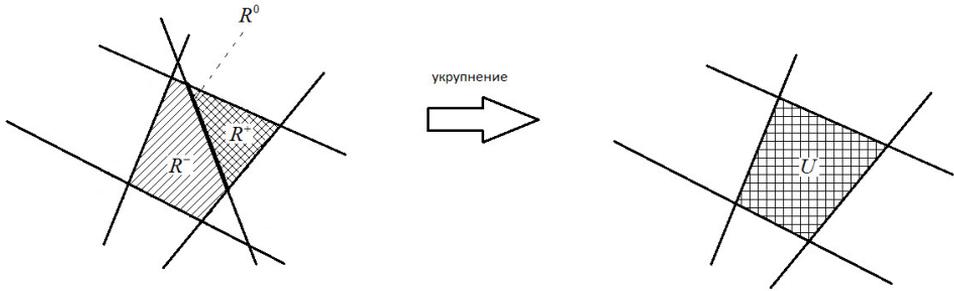


Рис. 1. Иллюстрация основной идеи леммы 2 (первый возможный случай)

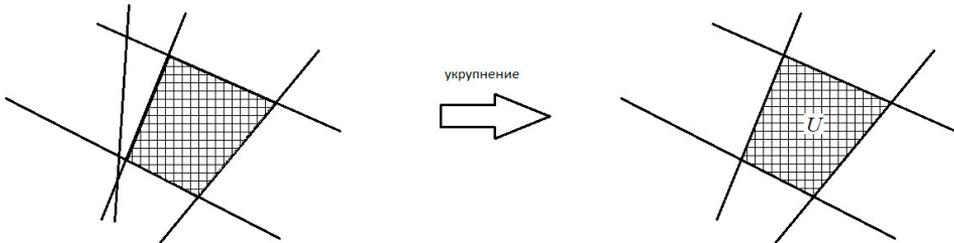


Рис. 2. Иллюстрация основной идеи леммы 2 (второй возможный случай)

Доказательство. Рассмотрим произвольный класс $U \in V(L')$ и проведем гиперплоскость l_i . Без ограничения общности будем считать, что $L' = \{l_1, \dots, l_{k-1}\}$, а $l_i = l_k$. Возможны два случая:

- $U \cap l_k = \emptyset$. Отметим, что $\forall \bar{x}, \bar{y} \in U \sigma(\bar{x}) = \sigma(\bar{y})$ при разбиении $R(L')$. Поэтому $\sigma_i(\bar{x}) = \sigma_i(\bar{y}), i \in \{1, \dots, k-1\}$. Далее рассмотрим $\sigma_k(\bar{x}) = \text{sgn}(l_k(\bar{x}))$ и $\sigma_k(\bar{y}) = \text{sgn}(l_k(\bar{y}))$.

Отметим, что, если $U \cap l_k = \emptyset$, то $\sigma_k(\bar{x}) = \sigma_k(\bar{y})$. В противном случае мы можем соединить точки \bar{x}, \bar{y} отрезком $[\bar{x}; \bar{y}]$. А так как по лемме 3 любой класс эквивалентности при любом разбиении гиперплоскостями — это выпуклое множество, то $[\bar{x}; \bar{y}] \subset U$. И при этом, если $\sigma_k(\bar{x}) \neq \sigma_k(\bar{y})$, то, очевидно, что $\exists \bar{\xi} \in [\bar{x}; \bar{y}] : \sigma_k(\bar{\xi}) = 0$. Но последнее означает, что $\bar{\xi} \in l_k$. Таким образом, $\exists \bar{\xi} \in [\bar{x}; \bar{y}] \cap l_k \subset U \cap l_k$, откуда вытекает, что $U \cap l_k \neq \emptyset$. Получили противоречие.

Следовательно, предположение неверно и $\forall \bar{x}, \bar{y} \in U \sigma_k(\bar{x}) = \sigma_k(\bar{y})$. Но тогда получаем, что $\forall \bar{x}, \bar{y} \in U$ обладают одинаковыми сигнатурами при разбиении $R(L)$.

При этом также очевидно, что если две точки обладали разными сигнатурами при разбиении $R(L')$, то при разбиении $R(L)$ они будут обладать тем более различными сигнатурами (в вектор сигнатур лишь добавились новые компоненты).

Из всего сказанного вытекает, что в новом разбиении класс U сохраняется (является таким же множеством точек, как и в исходном разбиении).

• $U \cap l_k \neq \emptyset$. Пусть $\bar{\xi} = U \cap l_k$. Так как U — объемный класс, то по лемме 3 он является открытым множеством, а поэтому $\exists O_\varepsilon(\bar{\xi}) : O_\varepsilon(\bar{\xi}) \subset U$. При этом очевидно, что найдутся точки $\bar{x}', \bar{x}'' \in O_\varepsilon(\bar{\xi}) : l_k(\bar{x}') > 0, l_k(\bar{x}'') < 0$ (для этого достаточно рассмотреть любую точку в направлении вектора нормали, расстояние от которой до $\bar{\xi}$ будет меньше ε ; это будет искомая точка \bar{x}' ; аналогично для точки \bar{x}'').

Очевидно, что точки \bar{x}', \bar{x}'' будут принадлежать двум разным классам в новом разбиении $R(L)$. Обозначим эти классы R^+, R^- , соответственно. Также рассмотрим сигнатуру $(\sigma(U), 0)$ и рассмотрим класс R^0 , обладающий данной сигнатурой.

Так как сигнатура U не содержит нулей в $R(L')$, а также, $sgn(l_k(\bar{x}')) = 1, sgn(l_k(\bar{x}'')) = -1$, то $\sigma(\bar{x}'), \sigma(\bar{x}'')$ не содержат нулей. Отсюда следует, что R^+, R^- — объемные.

При этом также очевидно, что $R^+ \subset U, R^- \subset U, R^0 \subset U$, так как они являются решением системы, состоящей из уравнений и неравенств, задающих множество U , к которым добавлено дополнительно одно из трех выражений $l_k(\bar{x}) > 0, l_k(\bar{x}) < 0, l_k(\bar{x}) = 0$ в зависимости от задаваемого класса R^+, R^-, R^0 , соответственно.

Таким образом, нашлись два класса R^+, R^- — объемные и непустые такие, что $R^+ \subset U, R^- \subset U$. Более того, так как для любой точки $\bar{x} \in U$ верно, что $sgn(l_k(\bar{x})) > 0$ или $sgn(l_k(\bar{x})) < 0$ или $sgn(l_k(\bar{x})) = 0$, то $R^+ \cup R^- \cup R^0 = U$.

По лемме 6 $R^0 \neq \emptyset$. Учитывая, что, по построению, $\sigma(R^+) = (\sigma_1, \dots, \sigma_{k-1}, 1)$, $\sigma(R^-) = (\sigma_1, \dots, \sigma_{k-1}, -1)$, $\sigma(R^0) = (\sigma_1, \dots, \sigma_{k-1}, 0)$, то по лемме 5 классы R^+, R^- смежные по классу R^0 . \square

Лемма 13. Пусть дано разбиение $R(L)$ и его укрупнение $R(L')$. Тогда для любых двух смежных классов $Q'_1, Q'_2 \in R(L')$ выполняется, что $\exists Q_1, Q_2 \in R(L) : Q_1 \subset Q'_1, Q_2 \subset Q'_2, Q_1|Q_2$.

Другими словами, для любых двух смежных классов из укрупнения (двух крупных классов) верно, что найдутся два класса из исходного разбиения (мелкие классы), каждый из которых лежит в своем крупном классе и при этом данные мелкие классы — смежные (см. рис. 3).

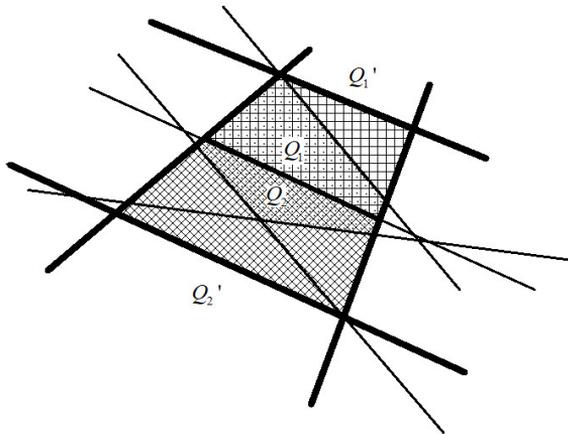


Рис. 3. Иллюстрация к формулировке леммы 13. Жирным выделены линии, оставшиеся после укрупнения, Q'_1, Q'_2 - два ограниченных класса в укрупнении (Q'_1 - класс, отмеченный прямой сеткой, Q'_2 - класс, отмеченный косой сеткой). Классы Q_1, Q_2 содержатся классах Q'_1, Q'_2 и отмечены прямой и косой сетками с точками, соответственно

Доказательство. Рассмотрим следующий пошаговый процесс построения из укрупнения $R(L')$ исходного разбиения $R(L)$:

- 1) Берется набор гиперплоскостей L' и к нему добавляется какая-то одна гиперплоскость из L , которой нет в L' . Получается некоторый набор $L^{(1)}$, которому соответствует некоторое укрупнение $R(L^{(1)})$ разбиения $R(L)$.
- 2) Пусть дан набор $L^{(i)} : L' \subsetneq L^{(i)} \subsetneq L$, полученный из L' , добавлением i штук гиперплоскостей из L , которых нет в L' .

Тогда, добавляя к $L^{(i)}$ еще одну гиперплоскость из L , которой нет в $L^{(i)}$, получим новый набор $L^{(i+1)}$, которому соответствует укрупнение $R(L^{(i+1)})$ разбиения $R(L)$.

3) Если $L^{(i)} = L$, то полученное укрупнение $R(L^{(i)})$ совпадает с исходным разбиением $R(L)$ и построение разбиения заканчивается.

Далее, если показать, что для любых двух смежных классов $Q'_1, Q'_2 \in R(L^{(i)})$, $i = 0, 1, \dots$ (полагаем, что $L^{(0)} = L'$) найдутся два смежных класса $Q''_1, Q''_2 \in R(L^{(i+1)})$: $Q''_1 \subset Q'_1, Q''_2 \subset Q'_2$, то будет выполняться, что и для любых двух смежных классов из $Q'_1, Q'_2 \in R(L')$ найдутся два смежных класса $Q''_1, Q''_2 \in R(L^{(i+1)})$: $Q''_1 \subset Q'_1, Q''_2 \subset Q'_2$.

Действительно, возьмем два смежных класса $Q'_1, Q'_2 \in R(L')$. Тогда по предположению найдутся два смежных класса $Q^{(1)}_1, Q^{(1)}_2 \in R(L^{(1)})$: $Q^{(1)}_1 \subset Q'_1, Q^{(1)}_2 \subset Q'_2$. Но для смежных классов $Q^{(1)}_1, Q^{(1)}_2 \in R(L^{(1)})$, в свою очередь, найдутся два смежных класса $Q^{(2)}_1, Q^{(2)}_2 \in R(L^{(2)})$: $Q^{(2)}_1 \subset Q^{(1)}_1, Q^{(2)}_2 \subset Q^{(1)}_2$ и так далее.

Продолжая аналогично процесс до некоторых смежных классов $Q^{(i+1)}_1, Q^{(i+1)}_2 \in R(L^{(i+1)})$: $Q^{(i+1)}_1 \subset Q^{(i)}_1, Q^{(i+1)}_2 \subset Q^{(i)}_2$, получаем, что нашлись смежные классы $Q''_1 = Q^{(i+1)}_1, Q''_2 = Q^{(i+1)}_2 \in R(L^{(i+1)})$: $Q^{(i+1)}_1 \subset Q^{(i)}_1 \subset \dots \subset Q'_1, Q^{(i+1)}_2 \subset Q^{(i)}_2 \subset \dots \subset Q'_2$. Что и доказывает утверждение.

Продолжая описанный процесс до того момента, когда $L^{(i+1)} = L$, получаем, что найденные $Q''_1, Q''_2 \in R(L^{(i+1)}) = R(L)$ будут обладать свойством смежности и тем свойством, что $Q''_1 \subset Q'_1, Q''_2 \subset Q'_2$. Сказанное доказывает теорему, при условии, что предположение, сделанное в процессе доказательства (о том, что для любых двух смежных классов $Q'_1, Q'_2 \in R(L^{(i)})$ найдутся два смежных класса $Q''_1, Q''_2 \in R(L^{(i+1)})$: $Q''_1 \subset Q'_1, Q''_2 \subset Q'_2$), верное. Покажем, что это так.

Для упрощения доказательства (и уменьшения обозначений) докажем более обобщенное предположение, которое состоит в следующем.

Пусть у нас есть набор гиперплоскостей L' , полученный из набора гиперплоскостей $L'' = \{l_1, \dots, l_k, l_{k+1}\}$ выбрасыванием единственной гиперплоскости (без ограничения общности, считаем, что это гиперплоскость l_{k+1}). Тогда верно, что:

Для любых двух смежных классов $Q'_1, Q'_2 \in R(L')$ выполняется, что существуют смежные классы $Q''_1, Q''_2 \in R(L'')$: $Q''_1 \subset Q'_1, Q''_2 \subset Q'_2$.

Действительно, рассмотрим смежные классы $Q'_1, Q'_2 \in R(L')$. Без ограничения общности, будем считать, что они имеют следующие сигнатуры: $\sigma(Q'_1) = (\sigma_1, \dots, \sigma_{i^*-1}, 1, \sigma_{i^*+1}, \dots, \sigma_k)$, $\sigma(Q'_2) = (\sigma_1, \dots, \sigma_{i^*-1}, -1, \sigma_{i^*+1}, \dots, \sigma_k)$.

Добавим к L' гиперплоскость l_{k+1} и покажем, что в новом разбиении пространства \mathbb{R}^n гиперплоскостями $L'' = L' \cup \{l_{k+1}\}$ найдутся два смежных класса Q''_1, Q''_2 : $Q''_1 \subset Q'_1, Q''_2 \subset Q'_2$.

Для этого рассмотрим три случая:

- Если $Q'_1 \cap l_{k+1} = \emptyset, Q'_2 \cap l_{k+1} = \emptyset$, то по лемме 12, в разбиении $R(L'')$ (после добавления новой гиперплоскости l_{k+1}) классы Q'_1, Q'_2 остались без изменений (как множества точек). Покажем, что тогда Q'_1, Q'_2 – искомые классы.

Действительно, по определению смежности, $Q'_1, Q'_2 \neq \emptyset$. Далее рассмотрим их сигнатуры. Так как $Q'_1|Q'_2$ в исходном разбиении $R(L')$, то $\sigma_i(Q'_1) = \sigma_i(Q'_2), i \in \{1, \dots, k\} \setminus \{i^*\}$ и $\sigma_i(Q'_1) \neq \sigma_i(Q'_2), i = i^*$ для некоторого $i^* \in \{1, \dots, k\}$. При этом $\sigma_i(Q'_1), \sigma_i(Q'_2) \in \{-1, 1\}, i \in \{1, 2, \dots, k\}$.

Далее, мы добавили к L' еще одну гиперплоскость l_{k+1} . Рассмотрим значения $\sigma_{k+1}(Q'_1), \sigma_{k+1}(Q'_2)$ в новом разбиении $R(L'')$. Так как $Q'_1 \cap l_{k+1} = \emptyset, Q'_2 \cap l_{k+1} = \emptyset$, то верно, что $\forall \bar{x} \in Q'_1 \sigma_{k+1}(\bar{x}) \in \{-1, 1\}$ и $\forall \bar{x} \in Q'_2 \sigma_{k+1}(\bar{x}) \in \{-1, 1\}$ (нуля тут быть не может, так как это возможно только для точки из l_{k+1} , но $Q'_1 \cap l_{k+1} = \emptyset, Q'_2 \cap l_{k+1} = \emptyset$, поэтому таких точек у нас нет).

Отсюда сразу же делаем вывод, что классы Q'_1, Q'_2 остаются объемными и в новом разбиении $R(L'')$ (так как в их сигнатурах нет нулей), а учитывая еще, что множества Q'_1, Q'_2 остаются классами эквивалентности в новом разбиении $R(L'')$, получаем, что $\sigma_{k+1}(Q'_1) = \alpha_1 \in \{-1, 1\}$ и $\sigma_{k+1}(Q'_2) = \alpha_2 \in \{-1, 1\}$.

Далее, покажем, что $\sigma_{k+1}(Q'_1) = \sigma_{k+1}(Q'_2)$ (здесь и далее уже рассматриваем исходное разбиение L' , а вместо гиперплоскости l_{k+1} рассматриваем функцию $l_{k+1}(\bar{x})$ и ее поведение относительно разбиения L').

Действительно, пусть, для определенности, $\sigma_{k+1}(Q'_1) = 1$. Последнее означает, что $\forall \bar{x} \in Q'_1 l_{k+1}(\bar{x}) > 0$. Но $l_{k+1}(\bar{x})$ – непрерывная функция, поэтому $\forall \bar{x} \in \overline{Q'_1} l_{k+1}(\bar{x}) \geq 0$.

Так как в исходном разбиении $R(L')$ верно, что $\overline{Q'_1|Q'_2}$, то существует непустой $(n-1)$ -мерный класс R такой, что $R \subset \overline{Q'_1} \cap \overline{Q'_2}$. В частности, $R \subset \overline{Q'_1}$, поэтому $\forall \bar{x} \in R l_{k+1}(\bar{x}) \geq 0$. Далее возможны два случая:

- 1) Если $\forall \bar{x} \in R l_{k+1}(\bar{x}) = 0$. Пусть $l_i \in L' : R \subset l_i$ (так как R – плоский класс в разбиении $R(L')$, то такая гиперплоскость $l_i \in L'$ существует). Тогда по лемме 9 верно, что $\forall \bar{x} \in l_i l_{k+1}(\bar{x}) = 0$. Откуда следует, что $l_{k+1} = l_i$ и это противоречит тому, что l_{k+1} – новая (добавленная) гиперплоскость.
- 2) Если $\exists \bar{x} \in R l_{k+1}(\bar{x}) > 0$. Но тогда, в силу непрерывности функции $l_{k+1}(\bar{x})$, верно выражение (21).

$$\exists O_\varepsilon(\bar{x}) : \forall \bar{y} \in O_\varepsilon(\bar{x}) l_{k+1}(\bar{y}) > 0 \quad (21)$$

Но по определению $R \subset \overline{Q'_2}$, поэтому выполняется выражение (22).

$$\forall \bar{x} \in R \forall O_\varepsilon(\bar{x}) \exists \bar{y} \in Q'_2 \cap O_\varepsilon(\bar{x}) \quad (22)$$

Из (21) и (22) немедленно следует выражение (23).

$$\exists \bar{y} \in Q'_2 : l_{k+1}(\bar{y}) > 0 \quad (23)$$

Теперь, переходя к разбиению $R(L'')$ и учитывая, что Q'_2 является классом эквивалентности в данном разбиении, а также доказанное выражение (23), получаем, что $\sigma_{k+1}(Q'_2) = \sigma_{k+1}(Q'_1) = 1$.

Но тогда имеем, что уже в новом разбиении $R(L'')$ сигнатуры классов Q'_1 и Q'_2 имеют вид $\sigma(Q'_1) = (\sigma_1, \dots, \sigma_{i^*-1}, 1, \sigma_{i^*+1}, \dots, \sigma_k, \sigma_{k+1})$, $\sigma(Q'_2) = (\sigma_1, \dots, \sigma_{i^*-1}, -1, \sigma_{i^*+1}, \dots, \sigma_k, \sigma_{k+1})$. Учитывая из ранее доказанного, что Q'_1, Q'_2 – непустые и объемные, получаем по лемме 8, что $Q'_1|Q'_2$ (эти классы непустые, объемные и их сигнатуры отличаются только в одной компоненте).

• Пусть $Q'_1 \cap l_{k+1} = \emptyset$ и $Q'_2 \cap l_{k+1} \neq \emptyset$ или $Q'_1 \cap l_{k+1} \neq \emptyset$ и $Q'_2 \cap l_{k+1} = \emptyset$. Без ограничения общности, будем считать, что $Q'_1 \cap l_{k+1} = \emptyset$ и $Q'_2 \cap l_{k+1} \neq \emptyset$. Тогда по лемме 12 Q'_2 распадается в новом разбиении $R(L'')$ на три класса $Q_2^{+'}, Q_2^{-'}, Q_2^{0'}$, из которых два класса $Q_2^{+'}, Q_2^{-'} \neq \emptyset$ – смежные и объемные. Покажем, что тогда один из этих объемных классов будет смежен с Q'_1 (который, по лемме 12, остался классом эквивалентности в разбиении $R(L'')$).

Отметим, что $\sigma_{k+1}(Q'_1) = \sigma_{k+1} \in \{-1, 1\}$ (доказательство аналогично предыдущему случаю).

Так как при разбиении $R(L')$ классы Q'_1, Q'_2 имели следующие сигнатуры: $\sigma(Q'_1) = (\sigma_1, \dots, \sigma_{i^*-1}, 1, \sigma_{i^*+1}, \dots, \sigma_k)$, $\sigma(Q'_2) = (\sigma_1, \dots, \sigma_{i^*-1}, -1, \sigma_{i^*+1}, \dots, \sigma_k)$, то при разбиении $R(L'')$ класс Q'_1 останется неизменным (как множество точек), но будет иметь сигнатуру $\sigma(Q'_1) = (\sigma_1, \dots, \sigma_{i^*-1}, 1, \sigma_{i^*+1}, \dots, \sigma_k, \sigma_{k+1})$.

А вместо класса Q'_2 появятся классы $Q_2^{+'}, Q_2^{-'}, Q_2^{0'}$, имеющие сигнатуры $\sigma(Q_2^{+'}) = (\sigma_1, \dots, \sigma_{i^*-1}, -1, \sigma_{i^*+1}, \dots, \sigma_k, 1)$, $\sigma(Q_2^{-'}) = (\sigma_1, \dots, \sigma_{i^*-1}, -1, \sigma_{i^*+1}, \dots, \sigma_k, -1)$ и $\sigma(Q_2^{0'}) = (\sigma_1, \dots, \sigma_{i^*-1}, -1, \sigma_{i^*+1}, \dots, \sigma_k, 0)$, соответственно.

Очевидно, что хотя бы одна из сигнатур $\sigma(Q_2^{+'})$ или $\sigma(Q_2^{-'})$ будет обладать тем свойством, что последняя ее компонента равна $\sigma_{k+1}(Q'_1) = \sigma_{k+1}$ (принцип ящиков Дирихле – ранее мы показали, что $\sigma_{k+1}(Q'_1) = \sigma_{k+1} \in \{-1, 1\}$), а далее мы рассматриваем классы $Q_2^{+'}$ и $Q_2^{-'}$ с сигнатурами, обладающими компонентами $\sigma_{k+1}(Q_2^{+'}) = 1, \sigma_{k+1}(Q_2^{-'}) = -1$; поэтому какой-то из этих компонент $\sigma_{k+1}(Q_2^{+'}), \sigma_{k+1}(Q_2^{-'})$ компонента

$\sigma_{k+1}(Q'_1) = \sigma_{k+1} \in \{-1, 1\}$ окажется равной). Без ограничения общности, пусть это будет класс $Q_2^{+'}$ (то есть $\sigma_{k+1}(Q_2^{+'}) = \sigma_{k+1}(Q'_1) = \sigma_{k+1}$).

Очевидно, что в таком случае сигнатура класса $Q_2^{+'}$ отличается от сигнатуры класса Q'_1 лишь в компоненте i^* . При этом $\sigma_{i^*}(Q'_1) = 1$, а $\sigma_{i^*}(Q_2^{+'}) = -1$.

Тогда, выбирая класс $Q_2^{+'}$ в качестве Q_2'' , а в качестве Q_1'' беря Q'_1 , получаем, что нашлись два непустых класса Q_1'' и Q_2'' такие, что $Q_1'' \subset Q'_1$ (так как по построению $Q'_1 = Q_1''$), $Q_2'' \subset Q'_2$ (доказано в лемме 12) такие, что $Q_1''|Q_2''$ (следует из построения и леммы 8).

• Пусть $Q'_1 \cap l_{k+1} \neq \emptyset$, $Q'_2 \cap l_{k+1} \neq \emptyset$. Но тогда, по лемме 12, $Q'_1 = Q_1^{+'} \cup Q_1^{-'} \cup Q_1^{0'}$, $Q'_2 = Q_2^{+'} \cup Q_2^{-'} \cup Q_2^{0'}$, где $Q_i^{+'}, Q_i^{-'}, Q_i^{0'}$, $i \in \{1, 2\}$ – классы из нового разбиения $R(L'')$ (каждый из классов Q'_1 и Q'_2 распался на три класса $Q_i^{+'}, Q_i^{-'}, Q_i^{0'}$, $i \in \{1, 2\}$). Причем классы $Q_i^{+'}, Q_i^{-'}$, $i \in \{1, 2\}$ непусты, объемны, смежны (при фиксированном i), а также $Q_1^{+'}, Q_1^{-'} \subset Q'_1$, $Q_2^{+'}, Q_2^{-'} \subset Q'_2$.

Но тогда, взяв, например, пару $Q_1^{+'}, Q_2^{+'}$ за классы Q_1'', Q_2'' , соответственно, получаем, что $Q_1^{+'}, Q_2^{+'}$, очевидно, смежны в разбиении $R(L'')$. Откуда и следует доказываемое утверждение. \square

Лемма 14. Пусть дано укрупнение $R(L')$ некоторого разбиения $R(L)$ и взят класс $U \in V(L')$. Тогда верно, что:

- 1) Или U содержит единственный класс эквивалентности $R \in V(L)$.
- 2) Или $\forall R_1, R_2 \in V(L) : R_1, R_2 \subset U$, $R_1 \neq R_2$ выполняется, что $R_1|R_2$ или $\exists R^{(1)}, \dots, R^{(r)} \in V(L) : R^{(1)}, \dots, R^{(r)} \subset U$ и при этом $R_1|R^{(1)}|\dots|R^{(r)}|R_2$ (см. рис. 4).

Доказательство. Будем доказывать по индукции построения укрупнения.

База индукции: Пусть $R(L_1)$ образовано из $R(L)$ вычеркиванием одной гиперплоскости (без ограничения общности будем считать, что это гиперплоскость l_1). Тогда по лемме 12 любой из классов $U \in V(L_1)$ либо совпадает с некоторым классом из $V(L)$, либо образован, как $U = R^+ \cup R^0 \cup R^-$ для некоторых непустых классов R^+, R^0, R^- , из которых R^+, R^- – объемные, а R^0 – $(n-1)$ -мерный. При этом R^+, R^- являются смежными по R^0 .

В первом случае (когда $U \in V(L_1)$ совпадает с некоторым классом из $V(L)$) получаем, что в данном классе $U \in V(L_1)$ содержится всего лишь один класс из $V(L)$ – сам класс $U \in V(L)$ (как подмножество). Отсюда следует, что в данном случае теорема верна.

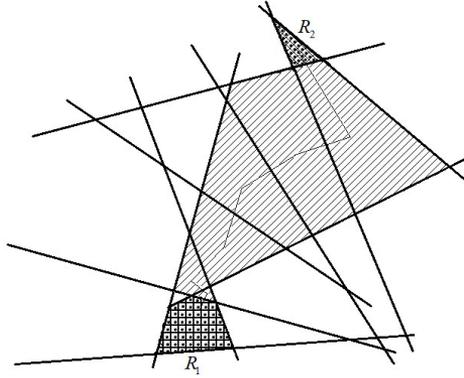


Рис. 4. Иллюстрация утверждения леммы 14 (второй случай) при $U = \mathbb{R}^2$. Классы R_1, R_2 обозначены сеткой; цепь смежных классов $R^{(1)}, \dots, R^{(r)}$ закрашена косыми линиями. Для наглядности путь по смежным классам $R^{(1)}, \dots, R^{(r)}$ через соответствующие смежностям пограничные классы обозначен ломаной линией

Во втором случае теорема также верна, так как для любых $R_1, R_2 \in V(L) : R_1, R_2 \subset U, R_1 \neq R_2$ верно, что $R_1 = R^+, R_2 = R^-$, так как, по построению, из непустых объемных классов в $V(L)$ только R^+ и R^- являются подмножествами U . И данные классы $R_1 = R^+, R_2 = R^-$ по лемме 12 являются смежными в разбиении $R(L)$.

Рассмотрим также несколько экстремальных ситуаций. Так, если в L' нет гиперплоскостей, то по определению $R(L') = V(L') = \{\mathbb{R}^n\}$. Далее возможны два случая:

- Если $L = \{l_1\}$, то, очевидно, что $U = \mathbb{R}^n = l_1^+ \cup l_1 \cup l_1^-$. И поэтому единственные два различных класса из $V(L)$, содержащиеся в U — это $R_1 = l_1^+, R_2 = l_1^-$, которые, очевидно, являются смежными в $R(L)$.

- Если же в L нет гиперплоскостей (то есть $L = \emptyset$), то по определению $V(L') = R(L') = R(L) = V(L) = \{\mathbb{R}^n\}$ и в $V(L')$ содержится единственный класс эквивалентности $R = U = \mathbb{R}^n$ из $V(L)$, поэтому утверждение снова верно.

Шаг индукции: Пусть L_i образовано из L_{i-1} вычеркиванием гиперплоскости l_i (а L_{i-1} образовано из $L = \{l_1, \dots, l_k\}$ вычеркиванием гиперплоскостей l_1, \dots, l_{i-1}). Рассмотрим разбиение $R(L_{i-1})$ и полученное укрупнение $R(L_i)$.

Тогда по лемме 12 каждый $U \in V(L_i)$ либо совпадает с некоторым $R \in V(L_{i-1})$, либо образован, как $U = R^+ \cup R^0 \cup R^-$, где $R^+ | R^-$ и $R^+, R^- \in V(L_{i-1})$.

Если $U \in V(L_i)$ совпадает с некоторым $R \in V(L_{i-1})$, то для него выполняется предположение индукции и все доказано.

Если же $U = R^+ \cup R^0 \cup R^-$, где $R^+ | R^-$ и $R^+, R^- \in V(L_{i-1})$, то для R^+, R^- верно предположение индукции. То есть, либо в R^+ находится единственный класс эквивалентности из $V(L)$, либо в R^+ находится несколько классов эквивалентности из $V(L)$ и тогда $\forall R_1^+, R_2^+ \in V(L) : R_1^+, R_2^+ \subset R^+, R_1^+ \neq R_2^+$ выполняется, что $R_1^+ | R_2^+$ или $\exists R^{(1),+}, \dots, R^{(r_1),+} \in V(L) : R^{(1),+}, \dots, R^{(r_1),+} \subset R^+$ и при этом $R_1^+ | R^{(1),+} | \dots | R^{(r_1),+} | R_2^+$.

И полностью аналогично, либо в R^- находится единственный класс эквивалентности из $V(L)$, либо в R^- находится несколько классов эквивалентности из $V(L)$ и тогда $\forall R_1^-, R_2^- \in V(L) : R_1^-, R_2^- \subset R^-, R_1^- \neq R_2^-$ выполняется, что $R_1^- | R_2^-$ или $\exists R^{(1),-}, \dots, R^{(r_2),-} \in V(L) : R^{(1),-}, \dots, R^{(r_2),-} \subset R^-$ и при этом $R_1^- | R^{(1),-} | \dots | R^{(r_2),-} | R_2^-$.

Отметим, что случай, когда в R^+ или R^- содержится единственный класс из $V(L)$ соответствует (согласно лемме 12) ситуации, когда R^+ или R^- остался классом эквивалентности в $V(L_{i-1})$, поэтому он совпадает, как множество, с классом R^+ или R^- в $V(L)$. В дальнейшем это рассуждение будем опускать и говорить, что это следует из леммы 12.

Также, из леммы 13 известно, что для любых двух смежных классов $Q_1, Q_2 \in R(L_{i-1})$ (из всякого укрупнения разбиения $R(L)$) выполняется, что $\exists Q'_1, Q'_2 \in V(L) : Q'_1 \subset Q_1, Q'_2 \subset Q_2, Q'_1 | Q'_2$.

Но тогда для $R^+, R^- \in R(L_{i-1})$ верно (24).

$$\exists Q'_1, Q'_2 \in V(L) : Q'_1 \subset R^+, Q'_2 \subset R^-, Q'_1 | Q'_2 \quad (24)$$

Далее рассмотрим $\forall R_1, R_2 \in V(L) : R_1, R_2 \subset U$. Согласно предположению индукции, для них возможны следующие случаи:

- Пусть $R_1, R_2 \subset R^+$ или $R_1, R_2 \subset R^-$. В любом случае выполняется предположение индукции для классов R^+ и R^- , откуда следует истинность утверждения.

- Пусть $R_1 \subset R^+, R_2 \subset R^-$ и оба класса R^+, R^- содержат единственный класс эквивалентности из $V(L)$. Тогда из леммы 12 следует, что R^- и R^+ в разбиении $V(L_{i-1})$ совпадают с собой же в разбиении $V(L)$. Тогда существуют единственные отличные друг от друга объемные классы $R_1 = R^+, R_2 = R^-$ из U и они, по построению, смежные.

- Пусть $R_1 \subset R^+, R_2 \subset R^-$ и один из классов $R^+ \in V(L_{i-1}), R^- \in V(L_{i-1})$ содержит единственный класс эквивалентности из $V(L)$. Без ограничения общности, можно считать, что это класс R^+ . Тогда из леммы 12 следует, что R^+ в $V(L_{i-1})$ совпадает с собой же в $V(L)$.

Но тогда отсюда и из (24) получаем, что $R_1 = R^+ = Q'_1$ и $\exists Q'_2 \in V(L) : Q'_2 \subset R^-,$ причем $R_1 | Q'_2$.

В свою очередь, так как $Q'_2 \subset R^-, R_2 \subset R^-$, то по предположению индукции для R^- , будет выполняться либо $Q'_2 = R_2$, либо $Q'_2 | R_2$,

либо $\exists R^{(1),-}, \dots, R^{(r_2),-} \in V(L) : R^{(1),-}, \dots, R^{(r_2),-} \subset R^-$ такие, что $R_2 | R^{(1),-} | \dots | R^{(r_2),-} | Q'_2$.

Тогда, учитывая, что $R_1 | Q'_2$ и симметричность отношения смежности, получаем (на примере случая с самым большим числом промежуточных классов), что $R_1 | Q'_2 | R^{(r_2),-} | \dots | R^{(1),-} | R_2$. Учитывая, что $R^+, R^- \subset U$, то и $Q'_2, R^{(r_2),-}, \dots, R^{(1),-} \subset U$. Откуда и следует доказываемое. Остальные случаи рассматриваются полностью аналогично.

• Пусть R^+ и R^- (каждый) содержат как минимум по два класса из $V(L)$. Выберем $\forall R_1 \in V(L) : R_1 \subset R^+$ и $\forall R_2 \in V(L) : R_2 \subset R^-$. Тогда по предположению индукции $R_1 = Q'_1$, или $R_1 | Q'_1$, или $\exists R^{(1),+}, \dots, R^{(r_1),+} \in V(L) : R^{(1),+}, \dots, R^{(r_1),+} \subset R^+$ и при этом $R_1 | R^{(1),+} | \dots | R^{(r_1),+} | Q'_1$. И, аналогично, $R_2 = Q'_2$ или $R_2 | Q'_2$, или $\exists R^{(1),-}, \dots, R^{(r_2),-} \in V(L) : R^{(1),-}, \dots, R^{(r_2),-} \subset R^-$ и при этом $R_2 | R^{(1),-} | \dots | R^{(r_2),-} | Q'_2$.

Но учитывая, что $Q'_1 | Q'_2$ и симметричность отношения смежности, получаем (снова на примере случая с самым большим числом промежуточных классов), что $R_1 | R^{(1),+} | \dots | R^{(r_1),+} | Q'_1 | Q'_2 | R^{(r_2),-} | \dots | R^{(1),-} | R_2$. Учитывая, что $R^+, R^- \subset U$, то и $Q'_1, Q'_2, R^{(1),+}, \dots, R^{(r_1),+}, R^{(r_2),-}, \dots, R^{(1),-} \subset U$. Откуда и следует доказываемое. Остальные случаи рассматриваются полностью аналогично.

Также отметим, что в случае, если $L_{i-1} = \emptyset$, полагаем, что $R(L_i) = R(L_{i-1}) = V(L_i) = V(L_{i-1}) = \{\mathbb{R}^n\}$. И в данном случае для класса $U = \mathbb{R}^n \in V(L_i)$ выполняется предположение индукции и утверждение можно считать доказанным. \square

Лемма 15. *Все объемные классы произвольного разбиения связаны по смежности друг с другом. Другими словами, для произвольного набора гиперплоскостей $L = \{l_1, \dots, l_k\}$ верно, что $\forall R_1, R_2 \in V(L) : R_1 \neq R_2$ выполняется $R_1 | R_2$ или $\exists R^{(1)}, \dots, R^{(r)} \in V(L) : R_1 | R^{(1)} | \dots | R^{(r)} | R_2$.*

Доказательство. Укрупняя в лемме 14 разбиение $R(L)$ до $R(\emptyset)$, получаем доказываемое утверждение. \square

Лемма 16 (первый критерий стабилизируемости). *Верны следующие утверждения:*

1) *Если цепь $\partial_S^i(R^{(1)}), i \in \mathbb{N}$ стабилизируется при $i = i_{stab}$, то*

$$\forall t \in \mathbb{N} \partial_S^{i_{stab}+t}(R^{(1)}) = \partial_S^{i_{stab}}(R^{(1)}).$$

2) *Стабилизация при некотором $i = i_{stab}$ может произойти в том и только том случае, когда все непустые объемные классы эквивалентности входят во множество $\partial_S^{i_{stab}}(R^{(1)})$.*

Доказательство. **1.** Пусть цепь $\partial_S^i(R^{(1)}), i \in \mathbb{N}$ стабилизировалась при $i = i_{stab}$. Тогда по определению верно, что $\partial_S^{i_{stab}+1}(R^{(1)}) = \partial_S^{i_{stab}}(R^{(1)})$.

Но тогда $\partial_S^{i_{stab}+t}(R^{(1)}) = \partial_S^t(\partial_S^{i_{stab}}(R^{(1)})) = \partial_S^{t-1}(\partial_S(\partial_S^{i_{stab}}(R^{(1)}))) = \partial_S^{t-1}(\partial_S^{i_{stab}+1}(R^{(1)})) = \partial_S^{t-1}(\partial_S^{i_{stab}}(R^{(1)})) = \dots = \partial_S^{i_{stab}}(R^{(1)})$. Откуда и следует доказываемое.

2. Если все непустые объемные классы эквивалентности вошли в $\partial_S^{i_{stab}}(R^{(1)})$, то, очевидно, что $\partial(\partial_S^{i_{stab}}(R^{(1)})) = \partial_S^{i_{stab}}(R^{(1)})$ (так как по определению $\forall i \in \mathbb{N} \partial_S^i(R^{(1)}) \subset V(L)$), откуда следует, что цепь стабилизировалась.

Предположим теперь, что в цепь не вошли все объемные непустые классы эквивалентности. Предположим, что при этом цепь стабилизировалась. Тогда по пункту 1 некоторые объемные непустые классы эквивалентности так и не войдут в цепь $\partial_S^i(R^{(1)}), i \in \mathbb{N}$.

Очевидно, что в цепь входит класс $R^{(1)}$ или такие классы эквивалентности $R' \in V(L)$, что $R'|R^{(1)}$ или $\exists\{R'_1, \dots, R'_r\} \subset V(L) : R'_1|R^{(1)}, \dots, R'_r|R'_r, R'_j|R'_{j-1}, j \in \{2, \dots, r\}$.

Но тогда тот факт, что некоторые непустые объемные классы никогда не войдут в цепь $\partial_S^i(R^{(1)}), i \in \mathbb{N}$ означает, что $\exists R^{fin} \in V(L) : R^{fin} \neq R^{(1)}, R^{fin} \wedge R^{(1)}$ и $\forall r \in \mathbb{N} \nexists\{R'_1, \dots, R'_r\} \subset V(L) : R'_1|R^{(1)}, R'_r|R'_r, R'_j|R'_{j-1}, j \in \{2, \dots, r\}$. Но последнее противоречит лемме 15. Следовательно, наше предположение неверно. Поэтому, цепь не может стабилизироваться, пока в некоторый элемент цепи не вошли все непустые объемные классы эквивалентности. \square

Лемма 17 (второй критерий стабилизируемости). *Цепь $\partial_S^i(R^{(1)}), i \in \mathbb{N}$ стабилизируется (при некотором $i = i_{stab}$) $\iff \partial_{add}^{i_{stab}}(R^{(1)}) = \emptyset$.*

Доказательство. (\Leftarrow) : Пусть существует $i = i_{stab}$, при котором $\partial_{add}^i(R^{(1)}) = \emptyset$. Предположим, что при этом $\partial_S^i(R^{(1)}), i \in \mathbb{N}$ не стабилизировалась на индексе i_{stab} (то есть $\partial_S^{i_{stab}}(R^{(1)}) \neq \partial_S^{i_{stab}+1}(R^{(1)})$). Но тогда $\partial_{add}^{i_{stab}}(R^{(1)}) \stackrel{def}{=} \partial_S^{i_{stab}+1}(R^{(1)}) \setminus \partial_S^{i_{stab}}(R^{(1)}) \neq \emptyset$ – противоречие.

(\Rightarrow) : Пусть цепь стабилизировалась на элементе $\partial_S^{i_{stab}}(R^{(1)})$. Тогда, по определению, $\partial_S^{i_{stab}+1}(R^{(1)}) = \partial_S^{i_{stab}}(R^{(1)})$, откуда следует, что $\partial_{add}^{i_{stab}}(R^{(1)}) \stackrel{def}{=} \partial_S^{i_{stab}+1}(R^{(1)}) \setminus \partial_S^{i_{stab}}(R^{(1)}) = \emptyset$. \square

5. ОСНОВНЫЕ ЛЕММЫ

Лемма 18. Пусть $f : \mathbb{R}^n \rightarrow \mathbb{R}$ и $g : \mathbb{R}^n \rightarrow \mathbb{R}$ – две CPL-функции, заданные над гиперплоскостями $\{l_1, \dots, l_{k_1}\}$ и $\{p_1, \dots, p_{k_2}\}$ и $\alpha \in \mathbb{R}$. Тогда:

- 1) Функция $f + g$ является CPL-функцией, причем ее можно задать над объединением $\{l_1, \dots, l_{k_1}\} \cup \{p_1, \dots, p_{k_2}\}$.

- 2) Функция $\alpha \cdot f$ является CPL-функцией, причем ее можно задать над множеством гиперплоскостей $\{l_1, \dots, l_{k_1}\}$.

Доказательство. **1.** Рассмотрим множество гиперплоскостей $\{l_1, \dots, l_{k_1}\} \cup \{p_1, \dots, p_{k_2}\}$. По лемме 10 можно считать, что $f : \mathbb{R}^n \rightarrow \mathbb{R}$ и $g : \mathbb{R}^n \rightarrow \mathbb{R}$ – непрерывные кусочно-линейные функции, заданные над данным объединением $\{l_1, \dots, l_{k_1}\} \cup \{p_1, \dots, p_{k_2}\}$.

Отметим, что из курса математического анализа, известно, что $f + g$ – также непрерывная функция.

Далее, рассмотрим $\forall \chi \in R(\{l_1, \dots, l_{k_1}\} \cup \{p_1, \dots, p_{k_2}\})$. По определению, $\forall \bar{x} \in \chi$ $f(\bar{x}) = f_\chi(\bar{x})$, $g(\bar{x}) = g_\chi(\bar{x})$, где $f_\chi(\bar{x}), g_\chi(\bar{x})$ – линейные части функций f, g , соответственно, на классе χ .

Но тогда $\forall \bar{x} \in \chi$ $f(\bar{x}) + g(\bar{x}) = f_\chi(\bar{x}) + g_\chi(\bar{x})$. Но $f_\chi(\bar{x}) + g_\chi(\bar{x})$ – это тоже линейная функция. Таким образом, по определению, $f + g$ – кусочно-линейная функция, заданная над гиперплоскостями $\{l_1, \dots, l_{k_1}\} \cup \{p_1, \dots, p_{k_2}\}$.

2. Полностью аналогично, из курса математического анализа известно, что $\alpha \cdot f$ – непрерывная функция. И, кроме того, если f задана над $\{l_1, \dots, l_{k_1}\}$, то $\forall \chi \in R(\{l_1, \dots, l_{k_1}\})$ выполняется, что $\forall \bar{x} \in \chi$ $f(\bar{x}) = f_\chi(\bar{x})$. Но тогда $\forall \bar{x} \in \chi$ $\alpha \cdot f(\bar{x}) = \alpha \cdot f_\chi(\bar{x})$, причем $\alpha \cdot f_\chi(\bar{x})$ – линейная функция. Откуда и следует доказываемое. \square

Лемма 19. Пусть f – некоторая CPL-функция, заданная над разбиением $\{R^1, \dots, R^s\}$, а h – некоторая ее выпуклая склейка на классах $R^+, R^- \in \{R^1, \dots, R^s\}$. Тогда верно, что:

- 1) Функция $f - h$ является CPL-функцией
- 2) Функция $f - h$ задана над теми же классами эквивалентности, что и функция f .
- 3) Число строго выпуклых склеек функции $f - h$ как минимум на одну меньше, чем у функции f .

Доказательство. **1.** Так как h – выпуклая склейка на классах R^+, R^- , то по определению $h(\bar{x}) = \max(f_{R^+}(\bar{x}), f_{R^-}(\bar{x}))$. Поэтому очевидно, что h – выпуклая, непрерывная и кусочно-линейная функция (заданная над единственной гиперплоскостью $l \in \{l_1, \dots, l_k\} : R^0 \subset l$, где R^0 – пограничный класс при смежных классах R^+, R^-).

Но тогда по лемме 18 $f - h$ – CPL-функция.

2. Более того, по той же лемме 18, $f - h$ задается над теми же гиперплоскостями, что и f . Следовательно, $f - h$ можно задать над теми же классами эквивалентности, что и функцию f .

3. Выберем произвольную пару смежных классов R^+, R^- со склейкой φ и обозначим R^0 – пограничный класс для данной пары смежных классов.

Отметим, что, если склейка φ была вогнутая, то функция $f - h$ будет равна на классах R^+, R^-, R^0 функции $\varphi - h$, которая является вогнутой (как сумма двух вогнутых функций). Следовательно, склейка по функции $f - h$ на классах R^+, R^- также будет вогнутой.

Если склейка φ была выпуклой, то мы ничего не можем утверждать про выпуклость или вогнутость функции $\varphi - h$ кроме одного случая. Это случай, когда $\varphi = h$. В этом случае на классах R^+, R^-, R^0 функция $\varphi - h$ будет вести себя, как константа. Поэтому ее можно реализовать как выпуклой, так и вогнутой склейкой. Такие склейки не считаются строго выпуклыми.

Таким образом, функция $f - h$ обладает числом строго выпуклых склеек на единицу меньшим, чем число строго выпуклых склеек у функции f . \square

Лемма 20. *Если функция $f : \mathbb{R}^n \rightarrow \mathbb{R}$ не имеет строго вогнутых склеек, то она выпуклая.*

Доказательство. Пусть f задана над некоторым разбиением $R(L) = \{R^1, \dots, R^s\}$, порожденным гиперплоскостями $L = \{l_1, \dots, l_k\}$. Без ограничения общности положим, что $V(L) = \{R^1, \dots, R^{s'}\}$, где $\{1, \dots, s'\} \subset \{1, \dots, s\}$. Отметим, что отсутствие строго вогнутых склеек у f означает, что все ее склейки являются выпуклыми (и какие-то из них, быть может, одновременно являются вогнутыми).

По определению, это означает, что для любых двух смежных классов $R^i, R^j \in V(L)$ верно, что $\forall \bar{x} \in R^i \ f_{R^i}(\bar{x}) \geq f_{R^j}(\bar{x})$. Покажем, что $\forall R^i, R^j \in V(L)$ (не обязательно смежных) выполняется, что $\forall \bar{x} \in R^i \ f_{R^i}(\bar{x}) \geq f_{R^j}(\bar{x})$.

Сначала выберем (зафиксируем) $\forall R^{(1)} \in V(L)$ и покажем, что $\forall R^j \in V(L) \ \forall \bar{x} \in R^{(1)} \ f_{R^{(1)}}(\bar{x}) \geq f_{R^j}(\bar{x})$. Для этого рассмотрим цепочку расширений $\partial_S^i(R^{(1)}) = \underbrace{\partial_S(\dots \partial_S(R^{(1)}))}_{i \text{ раз}}, \ i \in \mathbb{N}$.

По лемме 16 данная цепочка стабилизируется лишь при достижении всего множества $V(L)$. Обозначим момент $i \in \mathbb{N}$ стабилизации цепочки $\partial_S^i(R^{(1)})$, $i \in \mathbb{N}$ через i_{stab} .

Покажем теперь по индукции, что $\forall i \in \{1, \dots, i_{stab}\}$ и $\forall R^{(i+1)} \in \partial_S^i(R^{(1)})$ выполняется, что $\forall \bar{x} \in R^{(1)} \ f_{R^{(1)}}(\bar{x}) \geq f_{R^{(i+1)}}(\bar{x})$.

База индукции: Пусть $i = 1$. Тогда $\partial_S^1(R^{(1)}) = \partial_S(R^{(1)})$. И по построению $\forall R^{(2)} \in \partial_S(R^{(1)})$ либо совпадает с $R^{(1)}$, либо является смежным к $R^{(1)}$ и по условию леммы $\forall \bar{x} \in R^{(1)} \ f_{R^{(1)}}(\bar{x}) \geq f_{R^{(2)}}(\bar{x})$.

Шаг индукции: Пусть утверждение верно до $i - 1$ включительно. Покажем, что утверждение верно для i . Действительно, если $i - 1 \geq i_{stab}$, то при переходе от $i - 1$ к i новых классов не добавляется (так как цепь стабилизируется на множестве всех непустых объемных классов эквивалентности) и утверждение доказано.

Если же $i - 1 < i_{stab}$, то по лемме 16 цепь $\partial_S^i(R^{(1)})$, $i \in \mathbb{N}$ еще не стабилизировалась, поэтому по лемме 17 $\partial_{add}^{i-1}(R^{(1)}) = \partial_S^i(R^{(1)}) \setminus \partial_S^{i-1}(R^{(1)}) \neq \emptyset$. Тогда $\partial_S^i(R^{(1)}) = \partial_{add}^{i-1}(R^{(1)}) \cup \partial_S^{i-1}(R^{(1)})$. Причем для $\partial_S^{i-1}(R^{(1)})$ по предположению индукции утверждение верно (то есть $\forall R^{(i+1)} = R^{(i)} \in \partial_S^{i-1}(R^{(1)}) \forall \bar{x} \in R^{(1)} f_{R^{(1)}}(\bar{x}) \geq f_{R^{(i)}}(\bar{x})$). Следовательно, остается доказать утверждение только для $\partial_{add}^{i-1}(R^{(1)})$.

Возьмем $\forall R^{(i+1)} \in \partial_{add}^{i-1}(R^{(1)})$ и покажем, что $\forall \bar{x} \in R^{(1)} f_{R^{(1)}}(\bar{x}) \geq f_{R^{(i+1)}}(\bar{x})$. Так как в $\partial_{add}^{i-1}(R^{(1)})$ по построению содержатся только новые классы, смежные с классами из $\partial_S^{i-1}(R^{(1)})$, то для $R^{(i+1)}$ найдется класс $R^{(i)} \in \partial_S^{i-1}(R^{(1)})$, смежный с классом $R^{(i+1)}$. По индукции, $\forall \bar{x} \in R^{(1)} f_{R^{(1)}}(\bar{x}) \geq f_{R^{(i)}}(\bar{x})$.

Пусть также сигнатуры классов $R^{(i)}$ и $R^{(i+1)}$ отличаются в компоненте $j_{i,i+1} \in \{1, \dots, k\}$.

Далее, так как $R^{(i)}$ и $R^{(i+1)}$ – смежные классы и все склейки у функции f – выпуклы, то $\forall \bar{x} \in R^{(i)} f_{R^{(i)}}(\bar{x}) \geq f_{R^{(i+1)}}(\bar{x})$.

Далее возможны два случая:

- Пусть $\sigma_{j_{i,i+1}}(R^{(1)}) = \sigma_{j_{i,i+1}}(R^{(i)})$. Это означает, что классы $R^{(1)}$, $R^{(i)}$ лежат по одну сторону от гиперплоскости l , разделяющей классы $R^{(i)}$, $R^{(i+1)}$ (на которой всегда достигается равенство $f_{R^{(i)}}, f_{R^{(i+1)}}$). Без ограничения общности, можно считать, что $R^{(1)}, R^{(i)} \in l^+$. Тогда по пунктам 2 и 4 леммы 9 и из выражения $\forall \bar{x} \in R^{(i)} f_{R^{(i)}}(\bar{x}) \geq f_{R^{(i+1)}}(\bar{x})$ получаем, что $\forall \bar{x} \in l^+ f_{R^{(i)}}(\bar{x}) \geq f_{R^{(i+1)}}(\bar{x})$. Откуда следует, что $\forall \bar{x} \in R^{(1)} f_{R^{(i)}}(\bar{x}) \geq f_{R^{(i+1)}}(\bar{x})$.

Учитывая, что $\forall \bar{x} \in R^{(1)} f_{R^{(1)}}(\bar{x}) \geq f_{R^{(i)}}(\bar{x})$, получаем, что в данном случае $\forall \bar{x} \in R^{(1)} f_{R^{(1)}}(\bar{x}) \geq f_{R^{(i+1)}}(\bar{x})$ и утверждение для этого случая доказано.

- Пусть $\sigma_{j_{i,i+1}}(R^{(1)}) \neq \sigma_{j_{i,i+1}}(R^{(i)})$. Это означает, что классы $R^{(1)}$, $R^{(i)}$ лежат по разные стороны от гиперплоскости l , разделяющей классы $R^{(i)}$, $R^{(i+1)}$. Но тогда $\sigma_{j_{i,i+1}}(R^{(1)}) = \sigma_{j_{i,i+1}}(R^{(i+1)})$ (так как именно в этой компоненте с номером $j_{i,i+1}$ и отличаются классы $R^{(i)}$, $R^{(i+1)}$) и получается, что классы $R^{(1)}$, $R^{(i+1)}$ находятся по одну сторону от гиперплоскости l .

Обозначим $N = |\{j | \sigma_j(R^{(1)}) \neq \sigma_j(R^{(i)})\}|$. Но тогда выполняется $|\{j | \sigma_j(R^{(1)}) \neq \sigma_j(R^{(i+1)})\}| = N - 1$, что противоречит построению $\partial_{add}^{i-1}(R^{(1)})$.

Действительно, по построению и лемме 8 во множестве $\partial_S^i(R^{(1)})$ содержатся классы, сигнатуры которых отличаются от сигнатуры $\sigma(R^{(1)})$

не более, чем в i компонентах. Причем, по построению ($\partial_S^i(R^{(1)}) = \partial_{add}^{i-1}(R^{(1)}) \cup \partial_S^{i-1}(R^{(1)})$), во множестве $\partial_{add}^{i-1}(R^{(1)})$ содержатся только те классы, сигнатуры которых отличаются от сигнатуры $\sigma(R^{(1)})$ ровно в i компонентах. Таким образом, на i -ом шаге в $\partial_{add}^{i-1}(R^{(1)})$ не могут попасть классы с $i - 1$ инверсией, так как они уже есть в $\partial_S^{i-1}(R^{(1)})$. Получили противоречие, поэтому данный случай невозможен.

Таким образом, показано, что $\forall R^j \in V(L) \forall \bar{x} \in R^{(1)} f_{R^{(1)}} \geq f_{R^j}(\bar{x})$. А в силу того, что $R^{(1)}$ – это произвольный непустой объемный класс эквивалентности, то отсюда и получаем доказываемое (что $\forall R^i, R^j \in V(L) \forall \bar{x} \in R^i f_{R^i}(\bar{x}) \geq f_{R^j}(\bar{x})$).

Но тогда для $f(\bar{x})$ верен тот же вывод, что и для любой выпуклой CPL-функции (см. лемму 4). Отсюда и из основной теоремы в [11] получаем, что функция $f(\bar{x})$ представима в виде $\max_{i \in \{1, \dots, s'\}} (f_{R^i}(\bar{x}))$. А так как последняя функция выпукла, то и $f(\bar{x})$ – тоже выпукла. \square

Лемма 21. *Если функция $f : \mathbb{R}^n \rightarrow \mathbb{R}$ не имеет строго выпуклых склеек, то она вогнутая.*

Доказательство. Отметим, что $-f$ не имеет строго вогнутых склеек. Но тогда данная функция является выпуклой по лемме 20. А тогда f – вогнутая. \square

6. Основные результаты

Теорема 1. *Любую CPL-функцию $f : \mathbb{R}^n \rightarrow \mathbb{R}$, заданную над разбиением $R(L) = \{R^1, \dots, R^s\}$, порожденным гиперплоскостями $L = \{l_1, \dots, l_k\}$, можно восстановить нейронной схемой над базисом B_1 нелинейной глубины 1 и нелинейной сложности, не превосходящей $k \cdot \lceil s'/2 \rceil + 1$, где $s' = |V(L)|$.*

Доказательство. Рассмотрим множество строго выпуклых склеек функции f . Пусть это множество $S^{(0)}$. Выберем произвольную строго выпуклую склейку $h_1 \in S^{(0)}$ и рассмотрим функцию $g_1 = f - h_1$. По лемме 19 функция g_1 также является CPL-функцией, заданной над теми же гиперплоскостями $\{l_1, \dots, l_k\}$, но при этом множество строго выпуклых склеек $S^{(1)}$ для функции g_1 обладает тем свойством, что $|S^{(1)}| \leq |S^{(0)}| - 1$.

Продолжая процесс до некоторого N , при котором $S^{(N)} = \emptyset$, получаем функцию $g_N = f - h_1 - h_2 - \dots - h_N$. Таким образом, функция g_N обладает пустым множеством строго выпуклых склеек. Но тогда по лемме 21 функция g_N – вогнутая.

Вогнутую функцию можно представить нейронной схемой над базисом B_1 [11], поэтому g_N выразима нейронной схемой над B_1 . Но тогда

$f = h_1 + \dots + h_N + g_N$, где h_1, \dots, h_N, g_N – функции, выразимые нейронными схемами. Следовательно, f также выразима нейронной схемой.

Отметим, что так как h_1, \dots, h_N, g_N можно выразить в виде нейронной схемы нелинейной глубины 1 [11], то f тоже является нейронной схемой нелинейной глубины 1 над базисом B_1 .

Оценим нелинейную сложность такой нейронной схемы. Так как функции h_1, \dots, h_N, g_N выразимы над базисом B_1 нейронными схемами нелинейной сложности 1, то достаточно оценить число N . Самая простая оценка сверху – это число выпуклых склеек функции f . Но тогда $|\{h_1, \dots, h_N, g_N\}| = N + 1 \leq |S^{(0)}| + 1$. Оценим теперь число выпуклых склеек.

Для этого возьмем произвольную гиперплоскость l . Так как в каждой склейке участвует два непустых объемных класса, то данная гиперплоскость может дать нам максимум $\lceil s'/2 \rceil$ склеек, где s' – число непустых объемных классов. Так как гиперплоскостей k штук, то получаем оценку сверху $|S^{(0)}| \leq k \cdot \lceil s'/2 \rceil$.

Но тогда получается, что $|\{h_1, \dots, h_N, g_N\}| \leq k \cdot \lceil s'/2 \rceil + 1$. Таким образом, нелинейную сложность полученной нейронной схемы можно оценить сверху числом $k \cdot \lceil s'/2 \rceil + 1$. \square

Любую CPL-функцию $f : \mathbb{R}^n \rightarrow \mathbb{R}$, заданную над разбиением $R(L) = \{R^1, \dots, R^s\}$, порожденным гиперплоскостями $L = \{l_1, \dots, l_k\}$, можно восстановить нейронной схемой над базисом B_2 нелинейной глубины $\lceil \log_2 s' \rceil$ и нелинейной сложности, не превосходящей $s' \cdot (k \cdot \lceil s'/2 \rceil + 1)$, где $s' = |V(L)|$.

Доказательство. По теореме 1 данную функцию f можно представить в виде суммы $f = h_1 + \dots + h_N + g_N$, где h_1, \dots, h_N, g_N – выпуклые или вогнутые функции, а $|\{h_1, \dots, h_N, g_N\}| = N + 1 \leq k \cdot \lceil s'/2 \rceil + 1$.

Но по следствию к теореме 1 в работе [11] каждую функцию $\varphi \in \{h_1, \dots, h_N, g_N\}$ можно представить нейронной схемой нелинейной глубины $\lceil \log_2 s' \rceil$ и нелинейной сложности s' в базисе B_2 .

Тогда из выражения $h_1 + \dots + h_N + g_N$ следует, что функцию f можно реализовать нейронной схемой нелинейной сложности $s' \cdot (N + 1) \leq s' \cdot (k \cdot \lceil s'/2 \rceil + 1)$. Причем, так как нелинейная глубина функции $h_1 + \dots + h_N + g_N$ равна максимальной нелинейной глубине ее аргументов, а все ее аргументы обладают нелинейной глубиной $\lceil \log_2 s' \rceil$, то получаем, что нелинейная глубина f равна $\lceil \log_2 s' \rceil$ в базисе B_2 . \square

Теорема 2. $[B_1] = CPL$, $[B_2] = CPL$

Доказательство. Докажем, что $[B_1] = CPL$, равенство $[B_2] = CPL$ доказывается аналогично. Доказывать будем методом двойного включения:

- $([B_1] \subset CPL)$: Так как в базисе B_1 содержатся только кусочно-линейные непрерывные функции, то при суперпозициях также будут получаться кусочно-линейные непрерывные функции [6].
- $(CPL \subset [B_1])$: Пусть есть произвольная CPL-функция f . Тогда по теореме 1 данную функцию можно представить в виде нейронной схемы над базисом B_1 . Следовательно, $f \in [B_1]$. \square

Автор выражает благодарность научному руководителю, к.ф.-м.н., научному сотруднику В.С. Половникову за постановку задачи и научное руководство, а также д.ф.-м.н., доценту А.А. Часовских за помощь в проверке полученных результатов.

Список литературы

- [1] Половников В.С., *Об оптимизации структурной реализации нейронных сетей*, Диссертация на соискание степени кандидата наук, Москва, 2007.
- [2] Яблонский С.В., *Введение в дискретную математику*, Наука. Гл. ред. физ.-мат. лит., Москва, 1986.
- [3] Simon Haykin, *Neural Networks. A Comprehensive Foundation*, Prentice Hall International, Inc., Canada, 2006.
- [4] Шишляков В.Г., “О построении явной архитектуры нейронной сети, приближающей кусочно-линейные функции”, *Интеллектуальные системы. Теория и приложения*, **26**:2 (2022), 42–60.
- [5] McCulloch W.S., Pitts W., “A logical calculus of the ideas immanent nervous activity”, *Bull. Of math. Biophysics*, **5** (1943), 115–133.
- [6] Кан А.Н., “Вопросы выразимости в классе нейронных функций”, *Интеллектуальные системы. Теория и приложения*, **19**:1 (2015), 35–38.
- [7] Кан А.Н., “Вопросы полноты в классе кусочно-линейных непрерывных функций”, *Интеллектуальные системы. Теория и приложения*, **21**:2 (2017), 46–56.
- [8] Кан А.Н., “Вопросы выразимости в классе согласованных функций”, *Интеллектуальные системы. Теория и приложения*, **23**:2 (2019), 125–133.

- [9] Кан А.Н., “Решетка 1-следов замкнутых классов кусочно-линейных функций”, *Интеллектуальные системы. Теория и приложения*, **24**:3 (2020), 121–142.
- [10] Самсонова Н.А., *Класс кусочно-линейных непрерывных функций*, Бакалаврская работа, Якутск, 2015.
- [11] Шишляков В.Г., “Восстановление выпуклых функций класса CPL нейронными сетями над RELU-базисами”, *Интеллектуальные системы. Теория и приложения*, **26**:4 (2022), 174–197.
- [12] Мищенко А.С., Фоменко А.Т., *Курс дифференциальной геометрии и топологии*, Факториал Пресс, Москва, 2000.
- [13] Виро О.Я., Иванов О.А., Нецветаев Н.Ю., Харламов В.М., *Задачи по топологии*, СПбГУ, Санкт-Петербург, 2000.

CPL-functions expressibility by neural circuits on ReLU bases Shishlyakov V.G.

The paper considers the question of the expressibility of any continuous piecewise-linear function of several real variables in the form of a neural circuit over a basis with nonlinearities of the max type. Then the result is transferred to neural circuits built over a basis with a single non-linear RELU function.

Before proving the result, several auxiliary, technical lemmas are formulated and proved, expanding the existing knowledge about the properties of piecewise-linear functions and equivalence classes generated by a certain set of hyperplanes.

The paper also gives estimates of nonlinear complexity and depth for the constructed neural circuits in two given bases.

Finally, the paper proves the equality of the class of continuous piecewise-linear functions, the class of functions representable by neural circuits over a basis of the first type, and the class of functions representable by neural circuits over a basis of the second type.

Keywords: Neural networks, architecture, functions recovery, functions expressibility, convex functions, continuous piecewise-linear functions, ReLU function, maximum function.

References

- [1] Polovnikov V.S., *On optimization of the structural implementation of neural networks*, Ph.D. Thesis ... physical and mathematical sciences, MSU, Moscow, 2007 (In Russian).

- [2] YAblonskij S.V., *Introduction to discrete mathematics*, eds. fiz.-mat.lit., «Science», Moscow, 1986 (In Russian).
- [3] Simon Haykin, *Neural Networks. A Comprehensive Foundation*, Prentice Hall International, Inc., Canada, 2006.
- [4] Shishlyakov V.G., “On the construction of an explicit neural network architecture that approximates particle-linear functions”, *Intelligent systems. Theory and applications.*, **26**:2 (2022), 42–60 (In Russian).
- [5] McCulloch W.S., Pitts W., “A logical calculus of the ideas immanent nervous activity”, *Bull. Of math. Biophysics*, **5** (1943), 115–133.
- [6] Kan A.N., “Issues of expressibility in the class of neural functions”, *Intelligent systems. Theory and applications.*, **19**:1 (2015), 35–38 (In Russian).
- [7] Kan A.N., “Questions of completeness in the class of continuous particle-linear functions”, *Intelligent systems. Theory and applications.*, **21**:2 (2017), 46–56 (In Russian).
- [8] Kan A.N., “Issues of expressibility in the class of consistent functions”, *Intelligent systems. Theory and applications.*, **23**:2 (2019), 125–133 (In Russian).
- [9] Kan A.N., “Lattice of 1-traces of closed classes of particle-linear functions”, *Intelligent systems. Theory and applications.*, **24**:3 (2020), 121–142 (In Russian).
- [10] Samsonova N.A., *Class of continuous particle-linear functions*, Graduate work, Yakutsk, 2015 (In Russian).
- [11] Shishlyakov V.G., “Convex CPL-functions recovering by neural networks on RELU-bases”, *Intelligent systems. Theory and applications.*, **26**:3 (2022), 174–197 (In Russian).
- [12] Mishchenko A.S., Fomenko A.T., *Course in Differential Geometry and Topology*, Factorial Press, Moscow, 2000 (In Russian).
- [13] Viro O.Ya., Ivanov O.A., Netsvetaev N.Yu., Kharlamov V.M., *Topology tasks*, St. Petersburg State University, St. Petersburg, 2000 (In Russian).

Часть 3.
Математические модели

Вычислительная сложность определения локальности кода

Д. Ю. Валинуров¹

Локально восстанавливаемые коды (LRC коды) это линейные коды с представляющим большой интерес для приложений свойством, что каждый символ кодового слова можно восстановить по небольшому множеству других символов. В статье рассматривается сведение известных NP-полных задач теории кодирования к задаче проверки свойства локальности кода, и доказывается NP-полнота данной задачи для кода над произвольным фиксированным конечным полем.

Ключевые слова: коды исправляющие ошибки, локально восстанавливаемые коды, NP-полнота.

1. Введение

Обозначим через \mathbb{F}_q конечное поле из q элементов. Назовём (n, k) кодом над алфавитом A подмножество $C \subseteq A^n$ мощности $|C| = |A|^k$. Далее будем рассматривать *линейные* $[n, k]$ коды² над конечным полем \mathbb{F}_q , то есть k -мерные линейные подпространства \mathbb{F}_q^n , где $k = \dim C$ называется *размерностью* кода C .

Порождающей матрицей линейного $[n, k]$ кода является такая матрица G размера $k \times n$, что слово $c \in C$ получается как $c = vG$, где v — некоторое слово из \mathbb{F}_q^k . *Проверочной матрицей* кода называется такая матрица H размера $(n - k) \times n$, что $cH^T = 0$ для любого $c \in C$.

Определение 1. Минимальным расстоянием кода C называется величина $d = \min_{x, y \in C, x \neq y} h(x, y)$, где h — расстояние Хэмминга, то есть количество компонент, в которых векторы не равны. Нетрудно показать, что для линейных кодов $d = \min_{x \in C, x \neq 0} w(x)$, где $w(x)$ — вес слова x , то есть количество ненулевых компонент.

Обозначим через $[n]$ множество $\{1, 2, \dots, n\}$. Для произвольного множества $A \subseteq [n]$ ограничением $H|_A$ матрицы H на A будем обозначать

¹Валинуров Денис Юрьевич — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: denis.valinurov@yandex.ru.

Valinurov Denis Yurevich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

²В дальнейшем, когда речь будет идти о линейных кодах, мы обычно будем использовать квадратные скобки вместо круглых.

подматрицу, полученную удалением из H столбцов не из A , ограничением $C|_A$ кода C на A будем обозначать код, получаемый удалением из кодовых слов всех символов с индексами не из A .

Определение 2. *Говорим, что (n, k) код обладает свойством r -локальности, если выполняется следующее: для любого $i \in [n]$ существует подмножество $R_i \subseteq [n] \setminus i, |R_i| \leq r$ такое, что ограничения множества $C(i, a) = \{x \in C : x_i = a\}$ на R_i имеют пустое пересечение для $a \neq a'$, то есть $C|_{R_i}(i, a) \cap C|_{R_i}(i, a') = \emptyset$.*

Линейный код с таким свойством называется LRC $[n, k, r]$ кодом (locally recoverable code). Множества R_i будем называть *локальностями*. Из определения видно, что i -ый символ не может принимать разные значения при одинаковых значениях символов из R_i . Поэтому можно говорить, что символ c_i кодового слова $c \in C$ однозначно восстанавливается по множеству R_i и является функцией компонент $c_j, j \in R_i$.

Далее также будут упомянуты линейные коды над \mathbb{F}_q , элементы которых являются векторами над $A = \mathbb{F}_q^w$. Каждый символ такого кода будем интерпретировать как *сервер*, хранящий вектор из w значений из \mathbb{F}_q . В литературе параметр w называется субпакетизацией. Обозначим общую длину такого кода как $N = nw$, размерность³ как $K = kw$. Если на множестве серверов такого кода задана локальность, то соответствующий r -локальный код будем называть $[n, k, r, w]$ кодом.

Определение 3. *Кодом, двойственным к линейному коду $C \subseteq \mathbb{F}_q^n$ называется код $C^\perp = \{b \in \mathbb{F}_q^n : b \cdot c = 0, \forall c \in C\}$, где $b \cdot c = \sum_{i \in [n]} b_i c_i$ это стандартное скалярное произведение векторов $b, c \in \mathbb{F}_q^n$.*

Заметим следующую связь параметра локальности r с минимальным расстоянием d двойственного кода. Если в двойственном коде имеется кодовое слово веса d , то значит в исходном коде имеется проверочное соотношение, в котором d ненулевых коэффициентов. Поэтому видна связь задачи определения локальности с задачей определения минимального расстояния.

Определение 4. *Автоморфизм кода C — перестановка π на множестве индексов $[n]$ такая, что для любого кодового слова $c \in C$ выполнено $\pi(c) \in C$. Легко заметить, что автоморфизмы кода замкнуты относительно композиции и образуют группу, называемую группой автоморфизмов кода.*

³Для простоты мы считаем, что размерность всегда делится на w .

Определение 5. Код называется транзитивным, если для любых $i, j \in [n]$ в группе автоморфизмов найдётся такой автоморфизм π , что для него выполнено $\pi(i) = j$.

Для транзитивных кодов можно отметить следующее утверждение. Пусть d — минимальное расстояние двойственного кода, тогда из сказанного выше имеется проверочное соотношение, в котором d ненулевых коэффициентов. Вследствие транзитивности для каждого индекса i имеется проверочное соотношение с d ненулевыми коэффициентами, в которое входит индекс i , то есть локальность кода равна $d - 1$. Таким образом, для транзитивных кодов задача поиска параметра локальности равносильна задаче поиска минимального расстояния.

В статье [6] была доказана NP-полнота следующей задачи, имеющей отношение к декодированию по максимальному правдоподобию:

Задача 1. *Coset Weights.*

Дано: Двоичная матрица H размера $m \times n$, вектор $s \in \mathbb{F}_2^m$, целое число $w > 0$.

Вопрос: Существует ли вектор $x \in \mathbb{F}_2^n$ веса не более w такой, что $Hx^\top = s^\top$?

В статье [7] показано, что доказательство обобщается и на случай произвольного алфавита. В статье [4] была доказана NP-полнота задачи поиска минимального расстояния сведением задачи Coset Weights. В качестве вспомогательной задачи использовалась модификация известной NP-полной задачи Subset Sum для конечного поля. Эта вспомогательная задача также будет использована далее.

Далее будет показано, что задача проверки свойства r -локальности кода в общем случае для линейного кода тоже является NP-полной. Также в статье приведён переборный алгоритм проверки свойства r -локальности.

2. Алгоритм проверки r -локальности

Рассмотрим алгоритм определения является ли код заданный проверочной матрицей H кодом с параметрами $[n, k, r, w]$. Простейший алгоритм заключается в полном переборе всех возможных локальностей для каждого i -ого сервера и проверки, что сервер i может быть однозначно восстановлен по подбираемой локальности из r серверов. Приведём ниже описание алгоритма.

Положим для начала $w = 1$. Нам потребуется вспомогательная функция `CheckNodeLocality`, которая по заданным матрице H , столбцу i и

подмножеству столбцов $R_i \subseteq [n] \setminus i$ будет определять, является ли R_i локальностью столбца i . Обозначим через $e_i \in \mathbb{F}_q^n$ вектор с единицей в позиции i и нулями во всех остальных. Тогда псевдокод функции будет выглядеть следующим образом:

```

function CHECKNODELOCALITY( $H, i, R_i$ )
   $n \leftarrow$  число столбцов  $H$ 
   $H' \leftarrow \begin{pmatrix} H \\ e_i \end{pmatrix}$ 
   $cols \leftarrow [n] \setminus R_i$ 
  return  $(H'|_{cols}) = (H|_{cols})$ 
end function

```

В случае $w > 1$ вектор e_i в функции CheckNodeLocality необходимо заменить матрицей размера $w \times n$, в которой все элементы нулевые кроме единичной подматрицы $w \times w$ на месте i -ого сервера. Далее опишем основную функцию CheckFullLocality, осуществляющую перебор всех локальностей для каждого столбца:

```

function CHECKFULLLOCALITY( $H, r$ )
  for  $i \in [n]$  do
    checked = false
    for  $R_i \in \{A : A \subseteq [n] \setminus i, |A| = r\}$  do
      if CheckNodeLocality( $H, i, R_i$ ) then
        checked = true
        break
      end if
    end for
    if not checked then
      return false
    end if
  end for
  return true
end function

```

Правильность работы функции CheckNodeLocality основана на том, что R_i тогда и только тогда является локальностью i -ого символа, когда при занулении всех символов из R_i символ i также становится тождественно равным нулю. Это следует из того, что зависимость символа от своей локальности в случае линейного кода должна выражаться линейной комбинацией, что можно будет нетрудно видеть далее.

В CheckNodeLocality можно воспользоваться модификацией метода Гаусса, поэтому скорость работы CheckNodeLocality можно оценить свер-

ху как $\mathcal{O}(n^3)$. Тогда CheckFullLocality содержит полный перебор и оценивается экспоненциальным временем $\mathcal{O}(n^4 \binom{n-1}{r})$.

3. Доказательство NP-полноты проверки свойства r -локальности

Покажем NP-полноту проверки свойства r -локальности для линейного кода, заданного порождающей матрицей.

Задача 2. *Локальность кода C .*

Дано: Порождающая матрица G линейного $[n, k]$ кода C над полем \mathbb{F}_q . Целое положительное число $r < n$.

Вопрос: Является ли C LRC кодом с параметрами $[n, k, r]$?

Далее будут описаны несколько вспомогательных лемм и задач.

Лемма 1. *Дан линейный $[n, k]$ код C . Для $i \in [n]$ существует локальность R_i тогда и только тогда, когда существует линейная комбинация, выражающая зависимость i -ого символа от символов из R_i .*

Доказательство. Пусть G - порождающая матрица кода C . Рассмотрим ограничение G на $R_i \cup \{i\}$. Обозначим $A = G|_{R_i}$, $y = G|_{\{i\}}$. Система $Ax = y$ совместна тогда и только тогда, когда $\text{rank}(A|y) = \text{rank}(A)$. Последнее равенство означает, что y однозначно определяется столбцами A , то есть символами из R_i , что является определением локальности. Если $Ax = y$ совместна, то её решение x является коэффициентами искомой линейной комбинации. \square

Задача 3. *Локальность для одного символа кода C .*

Дано: Порождающая матрица G линейного $[n, k]$ кода C над полем \mathbb{F}_q . Целое положительное число $r < n$. Целое число $i \in [n]$.

Вопрос: Существует ли локальность $R_i \subseteq [n] \setminus \{i\}, |R_i| \leq r$ для индекса $i \in [n]$?

Лемма 2. *Задача 3 полиномиально сводится к задаче 2.*

Доказательство. Без ограничения общности будем проверять r -локальность последнего символа. Из входной матрицы G получим матрицу G' дублированием в G всех столбцов кроме последнего. Очевидно, что теперь у всех символов кроме последнего имеется локальность размера один — его копия. Локальность последнего символа при этом не изменилась, поэтому применяя задачу определения r -локальности для кода заданного порождающей матрицей G' получим ответ существует ли локальность для последнего символа. \square

Нетрудно заметить, что задачи определения локальности 2 и 3 лежат в классе NP. Оракулу достаточно указать индексы входящие в локальность R_i для всех или для одного $i \in [n]$ соответственно, тогда модифицированным методом Гаусса можно будет проверить наличие линейной зависимости за полиномиальное время. Таким образом, если задача 3 является NP-полной, то и задача 2 является NP-полной.

Как было упомянуто, в задаче Coset Weights можно \mathbb{F}_2 поменять на произвольный фиксированный алфавит и требовать, чтобы s был ненулевым вектором. В качестве доказательства NP-полноты такой задачи можно без изменений использовать доказательство для задачи 1 из статьи [6]. Приведём его для полноты:

Задача 4. *Coset Weights над произвольным фиксированным конечным полем.*

Дано: Матрица H размера $m \times n$, вектор s , $s \neq \mathbf{0}$, целое число $w > 0$.

Вопрос: Существует ли вектор x веса не более w такой, что $Hx^\top = s$?

Утверждение 1. ([6]) *Задача 4 для произвольного фиксированного конечного поля является NP-полной.*

Доказательство. Задача лежит в классе NP, так как при заданном x проверка свойства происходит за полиномиальное время прямым подсчётом. Будем доказывать NP-полноту сведением следующей известной задачи из статьи [3]:

Задача 5. *Трёхмерное сочетание.*

Дано: $U \subseteq T \times T \times T$, где T - конечное множество.

Вопрос: Существует ли подмножество $W \subseteq U$, $|W| = |T|$ такое, что никакие два элемента W не совпадают ни в какой координате?

Построим матрицу инцидентности H размера $3|T| \times |U|$. Каждый столбец в этой матрице содержит в точности $3T - 3$ нулей и три единицы и соответствует элементу $(i, j, k) \in U$ так, что единицы в этом столбце стоят в строках с номерами i , $T + j$, $2T + k$.

Подадим задаче 4 на вход матрицу H , вектор $s = (1, 1, \dots, 1)$ размера $3|T|$, $w = T$. Нетрудно видеть, что вывод для такого входа совпадает с ответом на задачу Three-dimensional matching. Действительно, если существует подмножество W и x -ого характеристический вектор, то $Hx^\top = s$. Обратно, если $Hx^\top = s$ для некоторого x , $|x| \leq T$, то $|x| = T$ и в сумме $\sum_{\substack{1 \leq j \leq |U| \\ x_j = 1}} H_{ij} = s_i = 1$ ровно один ненулевой элемент, то есть x задаёт трёхмерное сочетание W .

□

Теорема 1. *Задача 3 для произвольного фиксированного конечного поля является NP-полной.*

Доказательство. Будем сводить задачу 4 к задаче 3. На вход задачи 4 имеем набор H, s, w . В качестве порождающей матрицы G возьмём матрицу $(H|s^T)$, без ограничения общности можно убрать из этой матрицы строки, линейно зависмые от других строк. Тогда по лемме 1 наличие локальности размера w у последнего символа эквивалентно существованию такого $x, |x| \leq w$, что $Hx^T = s$. \square

4. Другое сведение к задаче проверки свойства r -локальности

На практике используются поля характеристики два, и часто матрицы в построениях используют в качестве подматрицы матрицы Вандермонда. Далее опишем другое доказательство NP-полноты задачи 3 для полей характеристики два путём сведения непосредственно задачи Coset Weights или же декодирования по максимум правдоподобия над полем \mathbb{F}_2 . Также для задачи 3 входная матрица будет определённого вида, содержащая подматрицу Вандермонда, что можно использовать как уточнение задачи определения локальности.

В задаче Coset Weights можно рассмотреть столбцы двоичной матрицы H как вектора над \mathbb{F}_2^m и представить их элементами \mathbb{F}_{2^m} , аналогично представляется и синдром $s \in \mathbb{F}_2^m$. Без ограничения общности можно положить, что матрица H полного ранга. Также если два столбца матрицы H , совпадают, то один из них можно убрать, при этом результат задачи не изменится. В случае нулевого вектора s решение x будет тривиальным решением, поэтому $s = 0$ можно также убрать из рассмотрения. В статье [4] похожим образом был осуществлён переход к следующей эквивалентной задаче:

Задача 6. *Finite-Field Subset Sum.*

Дано: Целое $m \geq 2$, множество из $n \leq 2^m$ различных элементов $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_{2^m}$, ненулевой элемент $\beta \in \mathbb{F}_{2^m}$ и целое положительное $r \leq m - 1$.

Вопрос: Существует ли подмножество $\{\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_\delta}\}$ множества $\alpha_1, \alpha_2, \dots, \alpha_n$ такое, что $\alpha_{i_1} + \alpha_{i_2} + \dots + \alpha_{i_\delta} = \beta$ и $\delta \leq r$?

Лемма 3. ([4]) Пусть $\alpha_1, \alpha_2, \dots, \alpha_\delta, \beta$ - различные элементы некоторого поля \mathbb{F}_q . Квадратная матрица M имеет следующий вид:

$$M = \begin{pmatrix} 1 & 1 & \dots & 1 & 0 \\ \alpha_1 & \alpha_2 & \dots & \alpha_\delta & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{\delta-2} & \alpha_2^{\delta-2} & \dots & \alpha_\delta^{\delta-2} & 0 \\ \alpha_1^{\delta-1} & \alpha_2^{\delta-1} & \dots & \alpha_\delta^{\delta-1} & 1 \\ \alpha_1^\delta & \alpha_2^\delta & \dots & \alpha_\delta^\delta & \beta \end{pmatrix}$$

Тогда $\det M = -(\alpha_1 + \alpha_2 + \dots + \alpha_\delta - \beta) \prod_{1 \leq i < j \leq \delta} (\alpha_j - \alpha_i)$

Доказательство. Разложим определитель M по последнему столбцу:

$$\det M = \beta \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_\delta \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{\delta-2} & \alpha_2^{\delta-2} & \dots & \alpha_\delta^{\delta-2} \\ \alpha_1^{\delta-1} & \alpha_2^{\delta-1} & \dots & \alpha_\delta^{\delta-1} \end{vmatrix} - \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_\delta \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{\delta-2} & \alpha_2^{\delta-2} & \dots & \alpha_\delta^{\delta-2} \\ \alpha_1^\delta & \alpha_2^\delta & \dots & \alpha_\delta^\delta \end{vmatrix}$$

В уменьшаемом содержится определитель матрицы Вандермонда. В вычитаемом содержится выражение для альтернанта [5], для которого имеем следующее:

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_\delta \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{j-1} & \alpha_2^{j-1} & \dots & \alpha_\delta^{j-1} \\ \alpha_1^{j+1} & \alpha_2^{j+1} & \dots & \alpha_\delta^{j+1} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^\delta & \alpha_2^\delta & \dots & \alpha_\delta^\delta \end{vmatrix} = S_{\delta-j}(\alpha_1, \dots, \alpha_\delta) \prod_{1 \leq i < j \leq \delta} (\alpha_j - \alpha_i),$$

где S_r — элементарная симметрическая функция порядка r . В частности, $S_1 = \sum_{1 \leq i \leq \delta} \alpha_i$, откуда получаем:

$$\begin{aligned} \det M &= \beta \prod_{1 \leq i < j \leq \delta} (\alpha_j - \alpha_i) - S_1 \prod_{1 \leq i < j \leq \delta} (\alpha_j - \alpha_i) = \\ &= -(\alpha_1 + \alpha_2 + \dots + \alpha_\delta - \beta) \prod_{1 \leq i < j \leq \delta} (\alpha_j - \alpha_i) \end{aligned}$$

□

Утверждение 2. *Задача 6 сводится к задаче 3 над полем \mathbb{F}_{2^m} .*

Доказательство. Положим

$$M_\delta = \begin{pmatrix} 1 & 1 & \dots & 1 & 0 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{\delta-2} & \alpha_2^{\delta-2} & \dots & \alpha_n^{\delta-2} & 0 \\ \alpha_1^{\delta-1} & \alpha_2^{\delta-1} & \dots & \alpha_n^{\delta-1} & 1 \\ \alpha_1^\delta & \alpha_2^\delta & \dots & \alpha_n^\delta & \beta \end{pmatrix}$$

Через M'_δ обозначим матрицу M_δ без последнего столбца, последний столбец обозначим m_δ .

В M'_δ выберем столбцы с некоторыми произвольными индексами $i_1, i_2, \dots, i_\delta$. Составим подматрицу \mathfrak{M} размера $(\delta + 1) \times (\delta + 1)$ из выбранных столбцов и столбца m_δ . По лемме 1 символы с индексами $i_1, i_2, \dots, i_\delta$ образуют δ -локальность для последнего символа ($R_\delta = \{i_1, i_2, \dots, i_\delta\}$) в коде с порождающей матрицей M_δ тогда и только тогда, когда система $\mathfrak{M}x = 0$ имеет ненулевое решение $(x_1, x_2, \dots, x_{i+1})$ с $x_{i+1} \neq 0$. Если $x_{i+1} = 0$, то и все решение x нулевое. Поэтому δ -локальность последнего символа имеет место тогда и только тогда, когда $\det(\mathfrak{M}) = 0$. По лемме 3 для различных элементов $\alpha_1, \dots, \alpha_n$ условие $\det(\mathfrak{M}) = 0$ равносильно $\beta = \alpha_{i_1} + \alpha_{i_2} + \dots + \alpha_{i_\delta}$, то есть δ -локальность последнего символа эквивалентна существованию $\alpha_{i_1}, \dots, \alpha_{i_\delta}$ таких, что $\beta = \alpha_{i_1} + \alpha_{i_2} + \dots + \alpha_{i_\delta}$. Заметим, что $|R_\delta| \geq \delta$, так как если матрицу \mathfrak{M} составить из меньшего количества столбцов из M'_δ , то система $\mathfrak{M}x = 0$ будет иметь только нулевое решение, а максимально возможная локальность будет $\delta + 1$, когда последний столбец просто выражается через базис из $\delta + 1$ столбцов матрицы Вандермонда M'_δ .

Для искомого сведения можно было бы рассмотреть все матрицы M_δ для $\delta = 1, \dots, r$. Тогда существование подмножества $\{\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_\delta}\}$, $\delta \leq r$ из задачи 6 равносильно тому, что хотя бы для одной матрицы M_δ получили положительный ответ на вопрос δ -локальности для последнего столбца. Но это являлось бы сводимостью по Тьюрингу, которое не обязательно означает сводимость по Карпу. Вместо этого объединим все матрицы M_δ в одну матрицу и будем получать один ответ. Сделаем это следующим образом:

$$M = \begin{pmatrix} M'_1 & 0 & \dots & 0 & m_1 \\ 0 & M'_2 & \dots & 0 & m_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & M'_r & m_r \end{pmatrix}$$

Локальность последнего символа кода с порождающей матрицей M равняется сумме локальностей последних символов в кодах с соответствующими порождающими матрицами M_i . Как было замечено, если для $\delta \in \{1, \dots, r\}$ существует множество $\{\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_\delta}\} : \beta = \alpha_{i_1} + \alpha_{i_2} + \dots + \alpha_{i_\delta}$, то последний символ кода с порождающей матрицей M_δ является δ -локальным, иначе он является $\delta + 1$ -локальным. Значит, если локальность r' последнего символа кода с порождающей матрицей M равна $\sum_{i \in [r]} (i+1) = (r+3)r/2$, то подмножества из задачи б не существует, иначе такое подмножество существует.

□

5. Заключение

В разделе 2 был приведён переборный алгоритм определения локальности кода. В разделе 3 было показано, что полиномиальный алгоритм определения локальности существует только в случае если $P=NP$. В разделе 4 было приведено сведение оригинальной задачи Coset Weights с бинарной матрицей и задачи Finite-Field Subset Sum к задаче определения локальности.

Список литературы

- [1] Ф.Дж.Мак-Вильямс, Н.Дж.А.Слоэн, *Теория кодов исправляющих ошибки*, «Связь», Москва, 1979, 744 с.
- [2] I. Tamo, A. Barg, “A family of optimal locally recoverable codes”, *IEEE Transactions on Information Theory*, **80**:8 (2014), 4661–4676.
- [3] Michael R. Garey, David S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman, New York, 1979, 340 pp.
- [4] A. Vardy, “Algorithmic Complexity in Coding Theory and the Minimum distance Problem”, *The Twenty-Ninth annual ACM symposium*, 1997, 92–109.
- [5] Thomas Muir, *A Treatise On The Theory Of Determinants*, Nabu Press, 2011, 296 pp.
- [6] E. Berlekamp, R. McEliece, H. van Tilborg, “On the inherent intractability of certain coding problems”, *IEEE Transactions on Information Theory*, **24**:3 (1978), 384–386.

- [7] С. Барг, “Некоторые новые NP-полные задачи кодирования”, *Пробл. передачи информ.*, **30:3** (1994), 23–28.

Computational complexity of finding code locality Valinurov D.Y.

The locally recoverable codes (LRC codes) are linear codes with an important for applications property that every symbol of a codeword can be recovered from a small set of other symbols. The paper provides reductions from known decision problems of coding theory to the problem of checking such property and a proof for the NP-completeness of this problem for an arbitrary fixed finite field.

Keywords: erasure coding, locally recoverable codes, NP-complete.

References

- [1] F.J. MacWilliams , N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Svyaz, Moscow, 1979, 744 pp.
- [2] I. Tamo, A. Barg, “A family of optimal locally recoverable codes”, *IEEE Transactions on Information Theory*, **80:8** (2014), 4661–4676
- [3] Michael R. Garey, David S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman, New York, 1979, 340 pp.
- [4] A. Vardy, “Algorithmic Complexity in Coding Theory and the Minimum distance Problem”, *The Twenty-Ninth annual ACM symposium*, 1997, 92–109
- [5] Thomas Muir, *A Treatise On The Theory Of Determinants*, Nabu Press, 2011, 296 pp.
- [6] E. Berlekamp, R. McEliece, H. van Tilborg, “On the inherent intractability of certain coding problems”, *IEEE Transactions on Information Theory*, **24:3** (1978), 384–386
- [7] S. Barg, “Some new NP-complete coding problems”, *Probl. Pered. Inform.*, **30:3** (1994), 23–28

Нижняя оценка энергопотребления для класса объёмных схем.

А. А. Ефимов¹

В данной работе рассматриваются объёмные схемы, являющиеся укладкой схем функциональных элементов в пространстве. Для объёмных схем получена нижняя оценка потенциала — меры мощности, равной количеству элементов схемы, выдающих единицу на данном входном наборе. Показано, что для почти всех частичных операторов с n входами и m выходами сложность реализующей их объёмной схемы по порядку не меньше, чем $\frac{m \sqrt[3]{d}}{\min^{2/3}(m, \log_2 d)}$, где d — размер области определения.

Ключевые слова: схемы из функциональных элементов, объёмные схемы, сложность схем, мощность схемы, потенциал.

1. Введение

Интенсивное развитие науки и вычислительной техники в XX веке породило одну из интереснейших проблем — задачу синтеза схем, вычисляющих булевы функции и операторы. Одной из основных моделей схем является схема из функциональных элементов (СФЭ). В качестве характеристики оптимальности СФЭ можно рассматривать сложность — количество функциональных элементов, содержащихся в схеме. Таким образом, под сложностью булевой функции или оператора будем понимать минимальную сложность схемы, реализующую данную функцию или оператор. В 1956 году Д. Маллер [1] посчитал сложность любой булевой функции, а в 1965 году О.Б. Лупанов [3] вычислил сложность почти всех булевых функций в стандартном базисе.

Отметим, что в 1961 году М.Н. Вайнцвайг [2] определил другую меру сложности СФЭ — мощность. Мощность или активность СФЭ — это максимальное количество элементов схемы, выдающих на выходе единицу, где максимум берётся по всем входным наборам. О.М. Касим-Заде [6] исследовал мощность в различных базисах и установил порядок функции Шеннона для произвольного конечного базиса.

¹Ефимов Алексей Андреевич — м.н.с каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: efimovqwerty@yandex.ru.

Efimov Alexey Andreevich — junior researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

Существенным недостатком модели СФЭ является то, что в ней не учитываются вполне естественные ограничения на размещение элементов схемы в плоскости или пространстве, способы их соединения, разводка проводов и т.п. В 1967 году С.С. Кравцов [4] впервые рассмотрел модель плоских прямоугольных схем, учитывающую данные ограничения. Им было показано, что порядок функции Шеннона площади плоских схем, реализующих функции от n переменных, равен 2^n . Одновременно с ним А.Д. Коршунов [5] начал рассматривать два класса схем: схемы из объёмных функциональных элементов и объёмные схемы из функциональных элементов. Для обоих классов порядок функции Шеннона также равен 2^n .

Интересное обобщение модели клеточных схем — многослойные d -мерные схемы были рассмотрены Т.Р. Сытдыковым [23, 24]. Если k — число слоев в d -мерной схеме, то были получены верхняя и нижняя оценки функции Шеннона сложности прямоугольных многомерных схем равны $\Theta\left(\frac{2^n}{\min(n, d \log k)}\right)$.

Н.А. Шкаликова в работе [7] одной из первых исследовала связь между площадью плоских схем и объёмом трёхмерных схем, реализующих булевы операторы. О.В. Черемисин [9] показал, что в классе прямоугольных схем невозможна одновременная минимизация площади и мощности плоских схем, реализующих систему всех конъюнкций.

Также интересные результаты были получены С.А. Ложкиным и другими авторами в работе [8]. Ими была получена нижняя оценка сложности одной специальной булевой функции, причём как для плоской, так и для объёмной реализации.

Особый интерес представляют работы Г.В. Калачёва [13]–[20], посвящённые плоским схемам. Автор также, как и Г.В. Калачёв, использует такую меру сложности схемы как потенциал. Он равен среднему значению количества единиц на всех внутренних узлах схемы. Неформально говоря, потенциал играет роль средней «энергии» схемы, необходимой для её функционирования. Кроме того, рассматривается и другая мера мощности — переключательная мощность — максимальное количество внутренних узлов схемы, изменяющих своё значение при изменении входных наборов схемы.

В статье [13] исследованы функции Шеннона потенциала и переключательной мощности плоских схем, реализующих булевы функции. В частности, было показано, что для рассматриваемых мер мощности получен одинаковый порядок функции Шеннона, равный $\Theta(2^{n/2})$.

В работе [14] для почти всех частичных булевых операторов с областью определения D и m выходами получена нижняя оценка

$\frac{m\sqrt{|D|}}{\sqrt{\min(m, \log_2 |D|)}}$ средней мощности. Отметим, что был применён метод расчленения, непрерывный аналог которого используется в данной статье.

Позднее в статье [15] было показано, что при незначительных ограничениях на область определения оператора существует схема, имеющая оптимальный порядок мощности, площади и глубины. В частности, для всюду определённых операторов с n входами и m выходами мощность равна $\Theta\left(\frac{m\sqrt{2^n}}{\min(n, \log_2 m)}\right)$, а глубина равна $\Theta(\max(n, \log_2 m))$.

Для класса монотонных функций также был получен порядок функции Шеннона для среднего и максимального потенциала. В частности, в работе [16], функция Шеннона для максимального потенциала равна $\Theta\left(\frac{2^{n/2}}{n^{1/4}}\right)$, а для среднего потенциала равна $\Theta\left(\frac{2^{n/2}}{n^{3/4}}\right)$.

В статье [17] исследована функция Шеннона максимального потенциала плоских схем, реализующих функции от n переменных с ограниченным числом единиц. В частности, было показано, что если количество единиц функции ограничено числом N , при условии $\log_2 N \asymp n$, то порядок функции Шеннона равен $\Theta(N(n - \log_2 N))$.

Также Г.В. Калачёвым в работе [16] были доказаны универсальные нижние оценки функции Шеннона мощности плоских схем. Кроме того, найден порядок роста функции Шеннона мощности схем, реализующих монотонные функции.

Позднее в статье [19] был исследован порядок функции Шеннона потенциала плоских схем, реализующих частичные булевы операторы при наличии ограничений на количество различных значений, принимаемых оператором. Было показано, что в классе частичных операторов с m выходами, областью определения мощности d и областью значения мощности не более r как средний, так и максимальный потенциал по порядку равны $\Theta\left(\left(\sqrt{d} + \frac{m\sqrt{r}}{\log_2 r}\right)\sqrt{\log_2 r}\right)$.

Очень интересный результат получен в работе [20]. Исследуется связь между площадью и максимальным потенциалом плоских схем, реализующих булевы операторы. Показано, что для произвольного булева оператора потенциал не меньше, чем $\sqrt{S}/4\sqrt{2}$, где S — площадь минимальной схемы, реализующей данный оператор.

Плоские автоматные схемы были недавно рассмотрены А.С. Воронниковым [25]. В качестве клеточного элемента здесь рассматривается автомат с не более чем двумя состояниями. А.С. Воронников получил верхнюю оценку переключательной мощности реализации периодической последовательности автоматной схемой. В работе приводится схема, реализующая произвольную последовательность длины 2^n с переключательной мощностью не более $\frac{2^{n/2}}{n}$.

В качестве альтернативной модели СФЭ рассматриваются контактные схемы (КС). Сложностью КС считается количество её контактов. Ю.С. Шуткин [11] ввёл понятие временной сложности КС, являющиеся некоторым аналогом мощности СФЭ. Им было установлено, что функция Шеннона сложности моделирования КС для функций от n переменных равна $2n - 1$.

Данная работа посвящена объёмным схемам [21, 22, 26], которые определяются аналогично плоским схемам, но в трёхмерном пространстве. Под объёмной схемой будем понимать укладку схемы из функциональных элементов в пространстве. Объёмная схема состоит из кубических элементов. Каждый кубический элемент реализует булев оператор, у которого в сумме не более 6 входов и выходов.

В данной работе впервые была получена нижняя оценка потенциала для частичных булевых операторов. А именно показано, что для почти всех булевых операторов $f : D \rightarrow \{0, 1\}^m$ порядок потенциала реализующих их объёмных схем не меньше $\frac{m \sqrt[3]{d}}{\min^{2/3}(m, \log_2 d)}$, где $d = |D|$. Отметим, что для всюду определенных операторов нижняя оценка совпадает с верхней оценкой, доказанной в работе [22].

Автор выражает особую признательность научному руководителю д.ф.-м.н. профессору Э.Э. Гасанову за постановку задачи и научное руководство. Также автор благодарит Г.В. Калачёва за помощь и внимание к работе.

2. Основные понятия и формулировка результатов

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

Метки будем называть сторонами элемента:

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

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

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

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

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

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

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

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

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

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

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

Объёмной схемой или схемой из кубических элементов на множестве $M \subseteq \mathbb{Z}^3$ будем называть корректную сеть из кубических элементов, в графе которой нет ориентированных циклов. Множество M будем называть носителем схемы K .

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

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

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

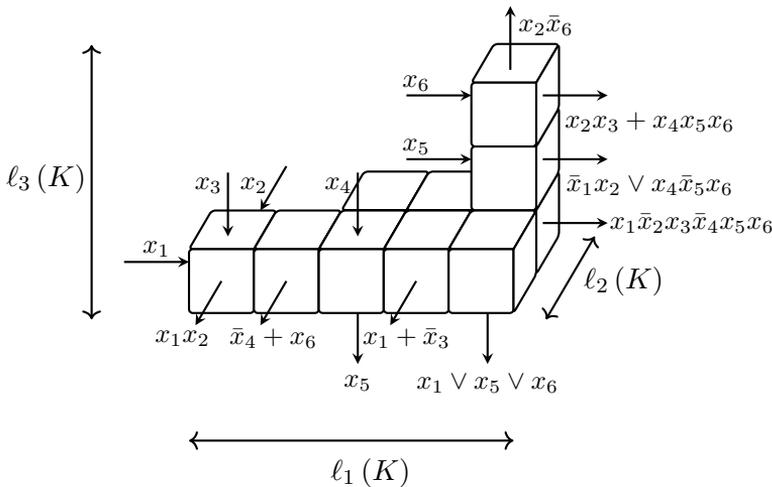


Рис. 1. Изображение объёмной схемы K .

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

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

Узлами схемы K будем называть вершины графа G_K .

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

Каждой объёмной схеме K можно сопоставить схему их функциональных элементов (K) следующим образом:

- 1) каждой функции $f_{s,i}$, которую реализует i -й выход элемента s объёмной схемы, сопоставим функциональный элемент $e_{s,i}$, реализующий $f_{s,i}$; если на i -м и j -м выходе реализуется одна и та же функция, то им будет соответствовать один и тот же функциональный элемент;
- 2) если i -й выход элемента s_1 подключен к j -му входу элемента s_2 , то соединим выход элемента $e_{s_1,i}$ с j -ми входами элементов $e_{s_2,k}$ для всех k , для которых $f_{s_2,k}$ существенно зависит от j -го аргумента.

Будем говорить, что схема K реализует булев оператор F , если схема из функциональных элементов (K) реализует F . Через (F) обозначим множество всех объёмных схем, реализующих оператор F .

Через $V(F)$ обозначим объём схемы, реализующей оператор F , и обладающей минимальным объёмом среди всех объёмных схем, реализующих F .

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

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

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

Также далее будем считать, что схема K имеет n входов, m выходов и l узлов. Состоянием схемы K на входном наборе x назовём вектор

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

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

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

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

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

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

Пусть $f \in P_2(D, m)$. Тогда

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

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

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

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

Пусть $f \in P_2(D, m)$. Тогда

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

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

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

Введём функцию Шеннона для среднего и максимального потенциала:

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

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

Теорема 1. Если $D \subseteq \{0, 1\}^n$, то для некоторой константы $C > 0$ верно

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

для почти всех операторов $f \in P_2(D, m)$ при $n \log_2 n = o(|D|)$, $\log_2 m = o(2^n)$, $|D| \rightarrow \infty$.

С учётом верхней оценки, доказанной в работе [22], получаем следующие следствия.

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

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

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

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

3. Доказательство основной теоремы

3.1. Метод расслоения

Для доказательства основной теоремы воспользуемся некоторыми определениями, введёнными ранее в работах Г.В. Калачёва [13], [14].

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

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

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

Через (MK) обозначим множество выходов M , которые являются выходами K , то есть

$$(MK) = (M) \cap (K).$$

Идея метода расслоения состоит в том, чтобы считать потенциал схемы по слоям. В работах [13], [14] выделяется множество подсхем такое, чтобы их контакты, не являющиеся контактами всей схемы, не пересекались, а оценивается снизу сумма потенциалов на контактах каждой подсхемы. В доказательстве нижней оценки для частичных операторов такой подход приводит к существенным техническим трудностям, связанным с тем, что при построении расслоения характеристики подсхем изменяются дискретно, что сильно осложняет точные оценки и ведёт к необходимости некоторых огрублений. В частности, в работе [13] из-за этого возникает дополнительный случай $\log t \succeq \sqrt{|D|}$, рассмотрение которого занимает несколько страниц.

В данной работе предлагается модифицированный подход, позволяющий строить «непрерывное» расслоение. Он основан на геометрическом представлении схемы в пространстве таким образом, что элементы расположены в узлах целочисленной решётки, а провода — отрезки, соединяющие соседние вершины. При этом если провод активен, то энергия выделяется равномерно по всей его длине. Вместо того чтобы рассматривать расслоение, в котором границей является множество проводов (контактов подсхемы), мы будем рассматривать пересечение бесконечного семейства слоёв с проводами схемы. Вместо суммирования мы будем интегрировать по элементам расслоения таким образом, чтобы потенциал каждого провода получался как интеграл по множеству слоёв, пересекающих этот провод.

Такой подход требует некоторого количества дополнительных подготовительных определений, но зато доказательство основного результата

будет более прозрачным и не потребует рассмотрения дополнительных случаев ограничений на параметры m , n и $|D|$. Итак, перейдём к формальным определениям.

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

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

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

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

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

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

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

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

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

Лемма 1. *Рассмотрим на множестве слоёв Ω такую σ -алгебру \mathcal{A} , что функции $I_w(R)$ измеримы для каждого w . Пусть на измеримом пространстве (Ω, \mathcal{A}) введена такая мера μ , что для любого ребра w целочисленной решётки \mathbb{Z}^3 верно условие:*

$$\int_{\Omega} I_w(R) d\mu(R) \leq C, \quad (2)$$

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

$$U_D(K) \geq \frac{1}{C} \int_{\Omega} U_D(K(R)|K) d\mu(R). \quad (3)$$

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

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

Интегрируя по множеству слоёв и используя (2), получим

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

□

3.2. Идея и схема доказательства

Нижнюю оценку будем доказывать следующим образом. Пусть есть класс B операторов, причём для каждого оператора $f \in B$ и любой схемы K , реализующей оператор f есть нижние оценки для потенциала на границе любой подсхемы, удовлетворяющей определённым ограничениям. Тогда будем строить непрерывное расслоение $\mathfrak{R} = \mathfrak{R}(K)$ такое, что для всех $R \in \mathfrak{R}$ подсхемы $K(R)$ удовлетворяют этим ограничениям, и затем интегрировать оценку потенциала на границе $(K(R)|K)$ по слоям, чтобы получить оценку для всей схемы K по формуле (3).

На рис. 2 изображена схема доказательства. Леммы 1–2 посвящены методу расслоения. В лемме 1 получено общее неравенство на потенциал с использованием расслоения, удовлетворяющего некоторым условиям. В лемме 2 получено свойство конкретного расслоения \mathfrak{R} , а в лемме 3 проверено, что расслоение \mathfrak{R} удовлетворяет условию леммы 1.

Геометрическим оценкам посвящены леммы 4–12. Вводим вспомогательную величину $u_I(t)$, через которую будем оценивать снизу потенциал схемы K . Для этого нам потребуется оценка из леммы 10: $u_I(t) \geq \frac{1}{32} \frac{s_I^2(t)}{v_I(t)}$. Но напрямую получить искомую оценку не получается, поэтому вводим величину $G_I(t)$, зависящую от длины остовного дерева некоторого взвешенного графа. Оценив $G_I(t)$ в леммах 5 и 9, получаем результат леммы 10.

Основное доказательство состоит из лемм 13–18, леммы 19 и теоремы 1. В леммах 13–18 рассматриваются классы операторов $L_0(D, m)$ и $L_1(D, m)$, такие, что для любого оператора B из $L_0(D, m)$ или $L_1(D, m)$ существует реализующая их объёмная схема K и её подсхема K_0 , что на границе подсхемы K_0 имеются ограничения на потенциал. Показывается, что $|L_0(D, m)| = o(2^{md})$ и $|L_1(D, m)| = o(2^{md})$. Таким образом,

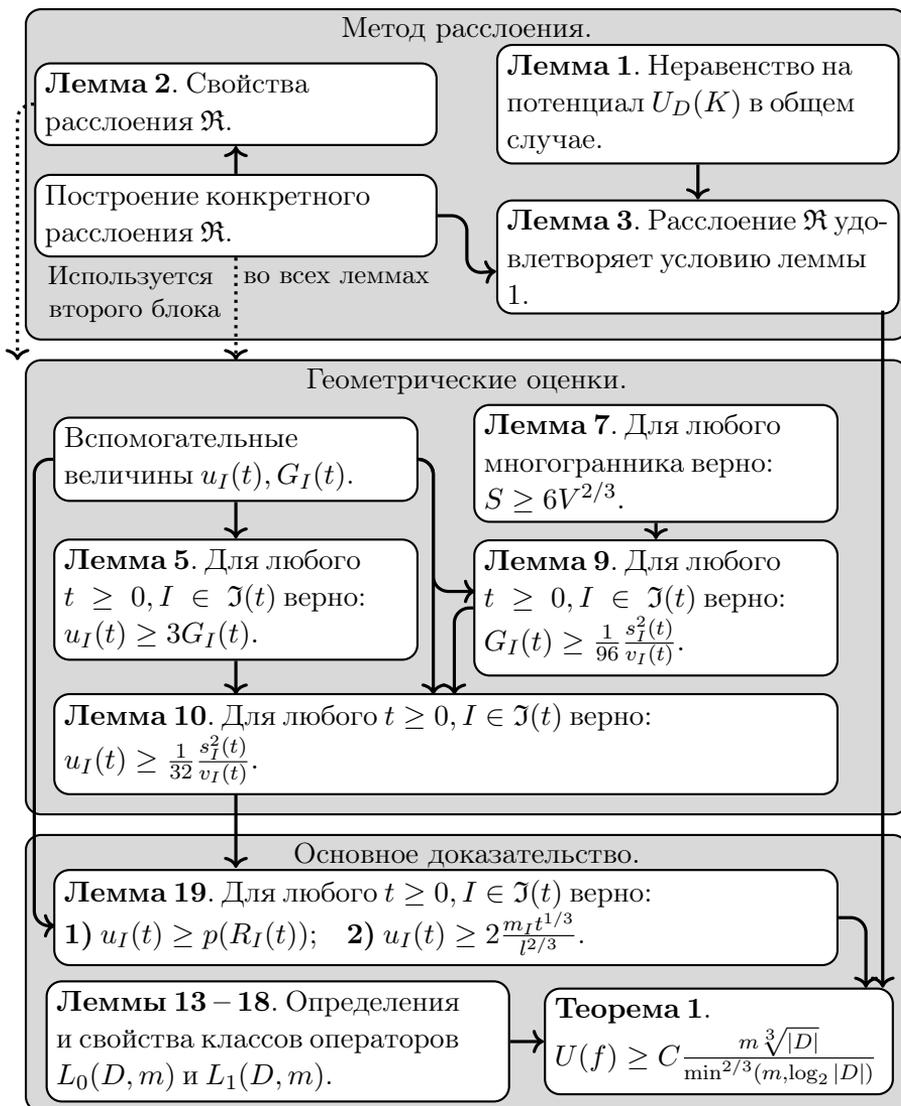


Рис. 2. Схема доказательства нижней оценки.

для почти всех операторов на любом разрезе имеются нижние оценки на потенциал, которые определенным образом суммируются (интегрируются). В лемме 19 и теореме 1 собираются все предыдущие оценки и получается итоговый результат.

3.3. Построение непрерывного расслоения \mathfrak{K}

Рассмотрим произвольную объёмную схему K , имеющую n входов и m выходов. Далее в разделах 3.3 и 3.4 будем считать схему K фиксированной. Пусть в схеме имеется s элементов, к которым подключены выходы схемы, занумеруем их от 1 до s . Центры этих элементов обозначим через c_1, \dots, c_s . Для удобства для любого $q \in \mathbb{N}$ положим $[q] = \{1, 2, \dots, q\}$. Через m_i обозначим число выходов элемента с центром c_i , $i = 1, \dots, s$. Для произвольного $I \subseteq 2^{[s]}$ положим $m_I = \sum_{i \in I} m_i$.

Формальное построение расслоения немного громоздкое, но оно имеет достаточно естественную физическую интерпретацию. Опишем неформально эту интерпретацию. Допустим, что точка c_i является источником жидкости с интенсивностью m_i . В момент $t = 0$ в пространстве нет жидкости. Начиная с момента $t = 0$ в каждую точку c_i , $i = 1, \dots, s$, начинает подаваться жидкость со скоростью m_i , при этом каждая точка изначально окружена абсолютно эластичной плёнкой, ограничивающей жидкость. При подаче жидкости плёнка расширяется равномерно по всей поверхности, то есть скорость её расширения перпендикулярно поверхности одинаковая во всех точках поверхности. В момент, когда две плёнки касаются друг друга, они сливаются и начинают образовывать одну единую компоненту связности, которая дальше расширяется равномерно по всей поверхности объединения. Важным свойством этого процесса является то, что по построению в момент времени t объём компоненты связности $R_I(t)$, содержащей внутри источники c_i , $i \in I$, равен в точности $m_I \cdot t$. Это свойство является ключевым для доказательства основной теоремы.

Поскольку компоненты, расширяясь, иногда объединяются, в конечном итоге они сливаются в одну компоненту, поэтому множество элементов расслоения можно представлять в виде дерева, изображённого ниже на рисунке 3. С целью выполнить условие (2) леммы 1, меру на расслоении вводим таким образом, чтобы её плотность в каждой точке была пропорциональна скорости расширения компоненты связности расслоения, соответствующей этой точке, перпендикулярно поверхности.

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

Для множеств $A_1, A_2 \subseteq \mathbb{R}^3$ определим оператор сложения множеств $A_1 + A_2 = \{x + y \mid x \in A_1, y \in A_2\}$. Введём $A + r := A + B(\mathbf{0}, r)$, $A \in \mathbb{R}^3, r \in \mathbb{R}^+$.

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

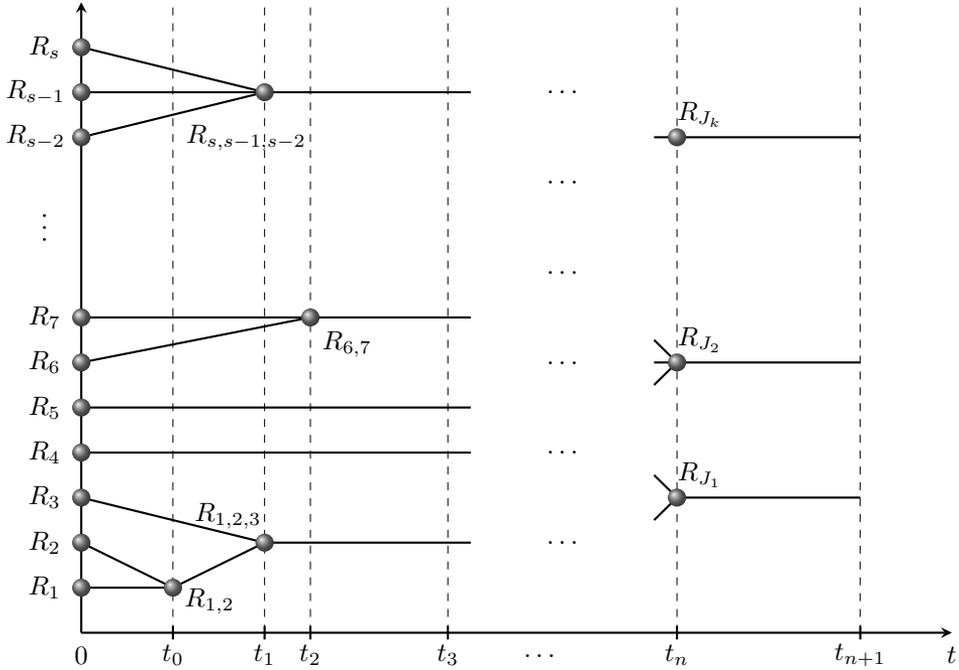


Рис. 3. Построение множеств $R_I(t)$.

База индукции. Положим

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

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

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

- Рассмотрим $I \in \mathfrak{I}(t_i)$. Если $i > 0$ и $I \in \mathfrak{I}(t_{i-1})$, то $R_I(t)$ при $t \geq t_i > t_{i-1}$ определено по предположению индукции. Иначе $R_I(t_i)$

было получено операцией объединения в момент t_i , либо $t_i = 0$. Поскольку для любого $I \in \mathfrak{I}(t_i)$ выполнено $V(R_I(t_i)) = m_i t_i$, и функция $V(R_I(t_i) + r)$ строго возрастает по r , то для $t \geq t_i$, существует единственное r такое, что $V(R_I(t_i) + r) = m_i t$; обозначим его через $r_I(t)$. Определим $R_I(t) = R_I(t_i) + r_I(t)$ при $t \geq t_i$. Отметим, что $V(R_I(t)) = m_i t$ выполнено по определению $r_I(t)$.

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

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

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

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

Заметим, что существуют такие $q \geq 1$ групп индексов $I_1^j, I_2^j, \dots, I_{k_j}^j \in \mathfrak{I}(t_i)$, $j \in [q]$, что множества $R_{I_1^j}(t), R_{I_2^j}(t), \dots, R_{I_{k_j}^j}(t)$ попарно не имеют общих точек при $t < t_{i+1}$, а при $t = t_{i+1}$ образуют одну компоненту связности. Положим

$$J^j = I_1^j \cup I_2^j \cup \dots \cup I_{k_j}^j, \quad R_{J^j}(t) = R_{I_1^j}(t) \cup \dots \cup R_{I_{k_j}^j}(t), \quad j \in [q]$$

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

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

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

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

Обозначим $\mathfrak{I} = \bigcup_{t \geq 0} \mathfrak{I}(t)$. Для фиксированного $I \in \mathfrak{I}$ введём числа

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

(если $I = \{1, \dots, s\}$, то $b_I = \infty$, иначе b_I конечно). Заметим, что $I \in \mathfrak{I}(t)$ тогда и только тогда, когда $t \in [a_I, b_I)$.

Нам также понадобится объединение множеств $R(t) = \bigcup_{I \in \mathfrak{I}(t)} R_I(t)$.

Введём подсхемы $M_I(t) = K(R_I(t))$, и $M(t) = K(R(t))$.

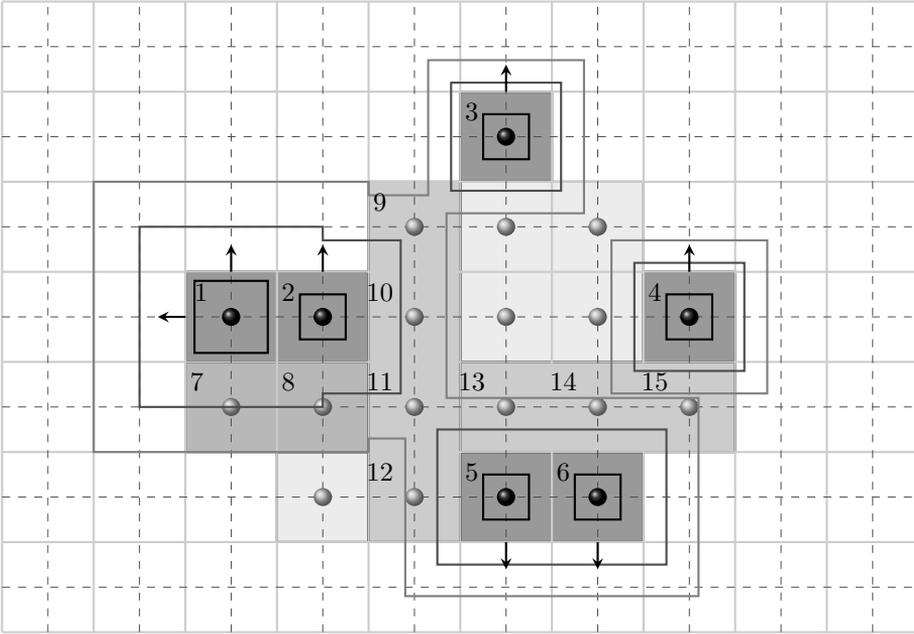


Рис. 4. Построение $M(t)$.

Опишем процесс построения подсхемы $M(t)$ на примере плоской схемы (на рис. 4 центры обозначены точками, выходы — стрелками). Сплошные серые линии — это границы элементов, пересечения пунктирных линий — это центры элементов. Отрезки пунктирных линий, соединяющие центры соседних элементов, — это провода схемы. Сплошными линиями обозначены границы некоторых множеств 1–6 из $R(t_0)$ при некотором $t_0 > 0$; элементы 1–6 принадлежат подсхеме $M(t_0)$. Более светлыми сплошными линиями обозначены границы некоторых множеств 7–8 из $R(t_1)$ при некотором $t_1 > t_0$; элементы 7–8 принадлежат подсхеме $M(t_1)$, но не входят в подсхему $M(t_0)$, то есть те элементы, которые добавляются в $M(t)$ при $t = t_1$ по сравнению с $t = t_0$. Аналогично, самыми светлыми сплошными линиями обозначены границы некоторых множеств 9–15 из $R(t_2)$ при некотором $t_2 > t_1$; элементы 9–15 принадлежат подсхеме $M(t_2)$, но не входят в подсхему $M(t_1)$.

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

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

Построим меру ρ для расслоения \mathfrak{R} , которое можно представить в виде дерева (см. рис. 3). Рёбра дерева индексируются элементами множества \mathfrak{I} . Положим $\mathfrak{R}_I = \{R_I(t) \mid t \in [a_I, b_I]\}$, это множество соответствует ребру в дереве \mathfrak{R} с индексом I . Легко видеть, что $\mathfrak{R} = \bigsqcup_{I \in \mathfrak{I}} \mathfrak{R}_I$. Поскольку множество \mathfrak{R}_I является образом промежутка $[a_I, b_I]$, на нём определена мера Лебега-Стилтьеса ρ_I с функцией распределения $p_I(t) = p(R_I(t))$, $t \in [a_I, b_I]$. В частности,

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

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

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

Сформулируем в виде леммы некоторые дополнительные свойства построенного расслоения \mathfrak{R} . Пусть $B(x, r)$ — шар с центром $x \in \mathbb{R}^3$ и радиусом $r \geq 0$, то есть $B(x, r) = \{y \in \mathbb{R}^3 \mid \|x - y\|_\infty \leq r\}$.

Лемма 2. *Для любого $t > 0$ выполнено:*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Учитывая определение J^j , получаем

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

Покажем, что $\forall A, B \in \mathfrak{I}(t_i)$ верно $A \cap B = \emptyset$. Если $A \neq J^j, B \neq J^j$, то $A, B \in \mathfrak{I}(t_{i-1})$, значит по предположению индукции верно $A \cap B = \emptyset$.

Пусть без ограничения общности $B = J^j$. Тогда по предположению индукции $A \cap I_z^j = \emptyset$, $z \in [k_j]$, а значит $A \cap J^j = \emptyset$.

- 2) Для всех $j \in [q]$ верно

$$R_{J^j}(t_i) = \bigcup_{z=1}^{k_j} R_{I_z^j}(t_i) = \bigcup_{z=1}^{k_j} \bigcup_{q \in I_z^j} B(c_q, r_q(t_i)) = \bigcup_{z \in J^j} B(c_z, r_z(t_i)).$$

При $t \in (t_i, t_{i+1})$ получаем

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

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

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

3) Если $i \in I, j \in J, I \neq J$, то шары $B(c_i, r_i(t))$ и $B(c_j, r_j(t))$ не пересекаются, а значит и не вложены друг в друга.

Рассмотрим случай $i, j \in I$. Так как $R_I(t) = \bigcup_{q \in I} B(c_q, r_q(a_I) + r_I(t))$

при $t \in [a_I, b_I]$, то

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

Так как по предположению индукции верно

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

То имеем при $t \in [a_I, b_I]$

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

Докажем последний пункт леммы 2. По определению R_I и r_i выполнено

$$\begin{aligned} R_I(x) &= R_I(a_I) + r_I(x), & R_I(y) &= R_I(a_I) + r_I(y), \\ r_i(x) &= r_i(a_I) + r_I(x), & r_i(y) &= r_i(a_I) + r_I(y). \end{aligned}$$

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

$$\ell_q(A + r) = \ell_q(A) + 2r, \quad q = 1, 2, 3.$$

Таким образом, имеем

$$\begin{aligned} p(R_I(y)) - p(R_I(x)) &= \sum_{q=1}^3 (\ell_q(R_I(a_I) + r_I(y)) - \ell_q(R_I(a_I) + r_I(x))) = \\ &= 6(r_I(y) - r_I(x)) = 6(r_i(y) - r_i(x)). \end{aligned}$$

□

С учётом последнего пункта леммы 2, для $x, y \in [a_I, b_I]$ можно определить величину $\Delta r_I(x, y)$ такую, что

$$r_i(y) - r_i(x) = \Delta r_I(x, y) \text{ для всех } i \in I. \quad (4)$$

Покажем, что мера ρ удовлетворяет неравенству (2), а именно верно следующее утверждение:

Лемма 3. Пусть \mathfrak{R} — расслоение на множестве \mathbb{R}^3 . Тогда для любого ребра w в целочисленной решетке \mathbb{Z}^3 верно неравенство:

$$\int_{\mathfrak{R}} I_w(R) d\rho(R) \leq 6. \quad (5)$$

Доказательство. Зафиксируем ребро w . Пусть $A \in \mathbb{R}^3$. Обозначим $\lambda(A)$ длину $w \cap A$. Тогда на множестве \mathfrak{R}_I можно определить меру λ_I с функцией распределения $\lambda(R_I(t))$.

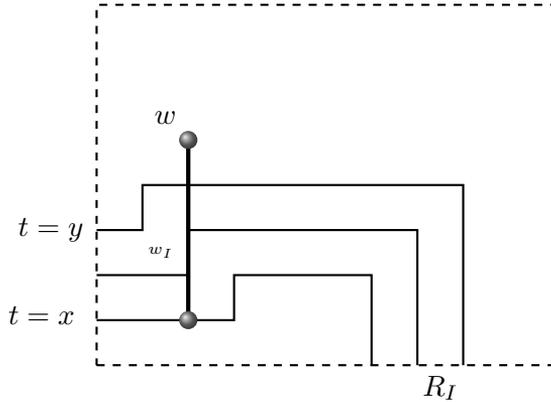


Рис. 5. Свойство расслоения \mathfrak{R} .

Докажем, что если $a_I \leq x < y < b_I$, $I_w(R_I(x)) = I_w(R_I(y)) = 1$ (см. рис. 5), то верно

$$p(R_I(y)) - p(R_I(x)) \leq 6(\lambda(R_I(y)) - \lambda(R_I(x))). \quad (6)$$

Заметим, что

$$\begin{aligned} p(R_I(y)) - p(R_I(x)) &= \sum_{i=1}^3 (\ell_i(R_I(y)) - \ell_i(R_I(x))) = 6(r_I(y) - r_I(x)) \leq \\ &\leq 6(\lambda(R_I(y)) - \lambda(R_I(x))). \end{aligned}$$

Обозначим w_I ту часть отрезка w , что пересекается со слоем $\partial R_I(t)$, $t \in [a_I, b_I]$. Отметим, что при $I \neq J \in \mathfrak{J}$, верно $w_I \cap w_J = \emptyset$, так как слои в расслоении \mathfrak{R} не пересекаются. В таком случае, в силу неравенства (6) имеем

$$\begin{aligned} \int_{\mathfrak{R}_I} I_w(R) d\rho(R) &= \int_{a_I}^{b_I} I_w(R_I(t)) dp(R_I(t)) \leq \\ &\leq 6 \int_{a_I}^{b_I} I_w(R_I(t)) d\lambda(R_I(t)) = 6|w_I|. \end{aligned}$$

Таким образом, имеем

$$\int_{\mathfrak{R}} I_w(R) d\rho(R) = \sum_{I \in \mathfrak{J}} \int_{R_I} I_w(R) d\rho(R) \leq \sum_{I \in \mathfrak{J}} 6|w_I| \leq 6|w| = 6.$$

□

Таким образом, по лемме 1 для данной меры p и данного расслоения \mathfrak{R} имеет место неравенство, полученное из неравенства (3):

$$U_D(K) \geq \frac{1}{6} \int_{\mathfrak{R}} U_D(M|K) d\rho(R). \quad (7)$$

3.4. Геометрические оценки

Для множества $I \subseteq \{1, \dots, s\}$ рассмотрим полный взвешенный граф с вершинами в точках c_i , $i \in I$, где вес ребра $\{c_i, c_j\}$ равен $w(\{c_i, c_j\}) = \|c_i - c_j\|_\infty$, то есть расстоянию между точками c_i и c_j (напомним, что c_i — центр i -го выходного элемента схемы). Пусть T — некоторое остовное дерево этого графа с множеством рёбер $E(T)$. Через $w(T)$ обозначим сумму весов его рёбер. Введём также величину $G_I^T(t)$:

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

где $\deg_T(c)$ — степень вершины c в дереве T . В основном нас будет интересовать величина $G_I(t) = \min_T G_I^T(t)$, где минимум берётся по всем остовным деревьям T . Из (4) для всех $I \in \mathfrak{J}(t)$ следует, что

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

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

$$G_I(t) = G_I(a_I) + 2\Delta r_I(a_I, t) \quad \text{при } t \in [a_I, b_I]. \quad (8)$$

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

$$u_I(t) = \sum_{J \in \mathfrak{I}: J \subseteq I} \int_{a_J}^{\min(b_J, t)} \max\left(\frac{m_J}{l}, 1\right) d(p(R_J(t))). \quad (9)$$

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

Лемма 4. *Для любого $t \geq 0$ и $I \in \mathfrak{I}(t)$ верно:*

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

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

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

$$1) \quad u_I(0) = \sum_{J \in \mathfrak{I}: J \subseteq I} \int_0^{\min(b_J, 0)} \alpha_J dp_J(t) = 0.$$

2) Так как $I = J_1 \cup J_2 \cup \dots \cup J_k$, то при $t = a_I$

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

3) Пусть $t \in [a_I, b_I]$. По пункту 1 леммы 2 элементы $\mathfrak{J}(t')$ не пересекаются при $t' \geq 0$, значит $b_J \leq a_I \leq t$ для всех $J \subsetneq I$, поэтому

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

□

Заметим, что поскольку интегрируется константа, то

$$u_I(t) = u_I(a_I) + \max\left(\frac{m_I}{l}, 1\right) (p(R_I(t)) - p(R_I(a_I))). \quad (10)$$

С учётом леммы 2, для всех $i \in I$ выполнено

$$u_I(t) = u_I(a_I) + 6 \max\left(\frac{m_I}{l}, 1\right) (r_i(t) - r_i(a_I)). \quad (11)$$

Используя (4), это можно переписать также в виде

$$u_I(t) = u_I(a_I) + 6 \max\left(\frac{m_I}{l}, 1\right) \Delta r_I(a_I, t). \quad (12)$$

Лемма 5. Для любого $t \geq 0$ и $I \in \mathfrak{J}(t)$ верна оценка:

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

Доказательство. Будем строить рассуждения индукцией по мощности множества I .

База индукции: $|I| = 1$ (множество $R_I(t)$ состоит из одного шара). Тогда $I = \{i\}$ для некоторого $i \in [s]$ и $I \in \mathfrak{J}(0)$, значит $a_I = 0$. Тогда из (11) получим:

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

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

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

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

Сначала покажем, что $u_I(a) \geq G_I(a)$. Поскольку $|I| > 1$, то $I \notin \mathfrak{J}(0)$, значит $a = a_I > 0$, то есть a — момент объединения. Без ограничения общности считаем, что $R_I(a) = R_{I_1}(a) \cup R_{I_2}(a)$ (см. рис. 6), иначе проделаем операцию несколько раз, последовательно добавляя элементы.

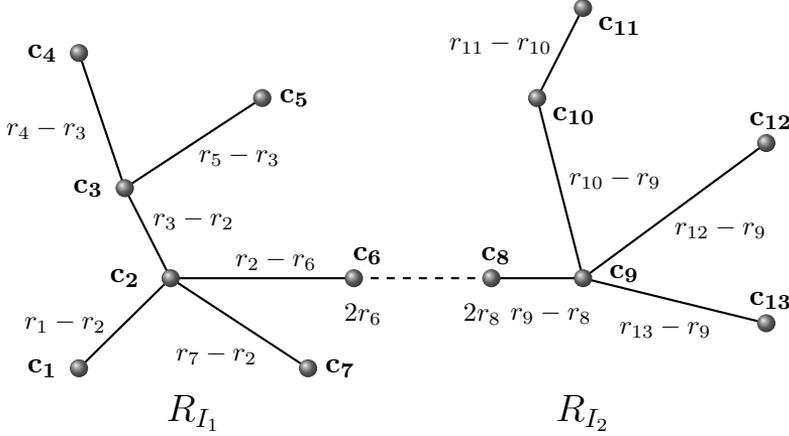


Рис. 6. Операция объединения.

По лемме 2 множества $R_{I_1}(a)$, $R_{I_2}(a)$ представляются в виде объединения шаров:

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

Отметим, что если множества $R_{I_1}(a)$ и $R_{I_2}(a)$ коснулись в точке, которая принадлежит шарам $B(c_{j_1}, r_{j_1}(a))$ и $B(c_{j_2}, r_{j_2}(a))$, то $w(\{c_{j_1}, c_{j_2}\}) = \|c_{j_1} - c_{j_2}\|_\infty = r_{j_1}(a) + r_{j_2}(a)$. Рассмотрим дерево T , полученное соединением деревьев T_{I_1} и T_{I_2} ребром $\{c_{j_1}, c_{j_2}\}$. Формально, дерево T является графом с множеством вершин $\{c_i \mid i \in I\}$ и множеством рёбер $E(T) = E(T_{I_1}) \cup E(T_{I_2}) \cup \{\{c_{j_1}, c_{j_2}\}\}$.

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

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

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

$$u_{I_1}(a) \geq 3G_{I_1}(a), \quad u_{I_2}(a) \geq 3G_{I_2}(a).$$

Таким образом, получаем оценку:

$$u_I(a) = u_{I_1}(a) + u_{I_2}(a) \geq 3G_{I_1}(a) + 3G_{I_2}(a) = 3G_I^T(a) \geq 3G_I(a). \quad (13)$$

Пусть $t \in [a_I, b_I]$, тогда, применяя (12), затем (13) и (8), получим:

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

что и требовалось. \square

Лемма 6. *Для любого измеримого ограниченного множества A выполнено*

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

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

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

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

Лемма 7 (Изопериметрическое неравенство). *Для любого многогранника $A \subseteq \mathbb{R}^3$ с гранями, параллельными координатным плоскостям, верна следующая оценка:*

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

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

Доказательство.

Искомую оценку получим, используя аналогичный результат в плоскости и интегрируя его по слоям (см. рис. 7). Обозначим $w(x)$, $x \in [0; h]$ длину границы слоя (x — параметр, указывающий высоту слоя), $s(x)$ — площадь слоя. Также обозначим $s_{\max} = \max_{x \in [0; h]} s(x)$. Тогда площадь горизонтальных граней множества A не меньше $2s_{\max}$. Выражая площадь вертикальных граней и объём множества A через интеграл, получим:

$$S \geq \int_0^h w(x) dx + 2s_{\max}, \quad V = \int_0^h s(x) dx.$$

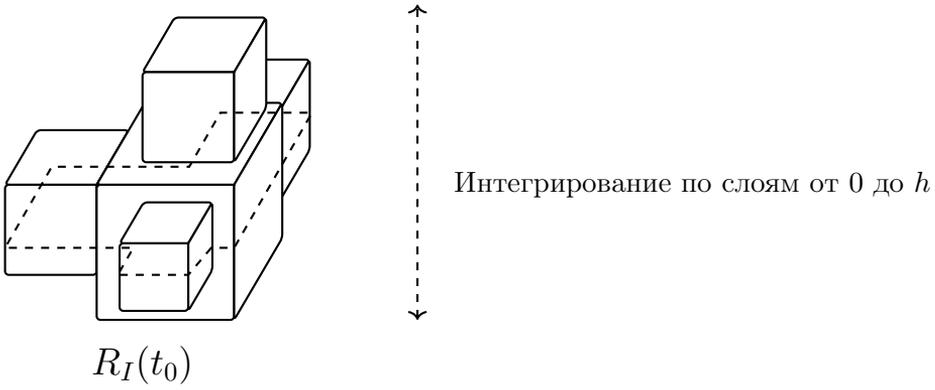


Рис. 7. Оценка площади боковой поверхности через объём.

Существует аналог искомого утверждения для плоского случая, который был показан в работе [14, стр.20, лемма 11]:

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

Используя данное неравенство и неравенство средних, получаем:

$$\begin{aligned} S &\geq \int_0^h w(x)dx + 2s_{max} \geq \int_0^h 4\sqrt{s(x)}dx + 2s_{max} = \\ &= 2 \left(\int_0^h \sqrt{s(x)}dx + \int_0^h \sqrt{s(x)}dx + s_{max} \right) \geq \\ &\geq 6 \sqrt[3]{\left(\int_0^h \sqrt{s(x)}dx \right)^2 \cdot s_{max}} = 6 \sqrt[3]{\left(\int_0^h \sqrt{s(x) \cdot s_{max}}dx \right)^2} \geq \\ &\geq 6 \sqrt[3]{\left(\int_0^h s(x)dx \right)^2} = 6V^{2/3}. \end{aligned}$$

□

По лемме 2 множество $R_I(t)$ является объединением шаров в метрике l_∞ . Шар в метрике l_∞ является кубом с гранями, параллельными координатным плоскостям, а значит $R_I(t)$ является многогранником с гранями, параллельными координатным плоскостям. Таким образом, по лемме 7 имеем

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

Нам понадобится следующая простая лемма

Лемма 8. Для любых $a, b \in \mathbb{R}$ выполнено неравенство:

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

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

$$\begin{aligned} 4(a - b)(a^3 - b^3) - 3(a^2 - b^2)^2 &= \\ &= 4(a - b)^2(a^2 + ab + b^2) - 3(a - b)^2(a + b)^2 = \\ &= (a - b)^2(4a^2 + 4ab + 4b^2 - 3(a + b)^2) = \\ &= (a - b)^4 \geq 0. \end{aligned}$$

□

Лемма 9. Для любого $t \geq 0$ и $I \in \mathfrak{J}(t)$ верна следующая оценка:

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

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

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

По лемме 2 множество R_I является объединением шаров $R_I(t) = \bigcup_{i \in I} B(c_i, r_i)$.

Для доказательства нам понадобится по индукции собирать множество $R_I(t)$ из шаров, поэтому введём вспомогательные множества $J_1 \subseteq J_2 \subseteq \dots \subseteq J_{|I|} = I$, а также для $k = 1, \dots, |I|$ определим множество

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

и граф T_k — подграф T_I с множеством вершин $\{c_i \mid i \in J_k\}$. Множества J_k построим так, чтобы T_k было деревом с k вершинами, причём $T_{|I|} = T_I$ и T_{k-1} получалось из T_k удалением одного листа для $k = 2, \dots, |I|$.

По индукции покажем, что

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

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

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

Подставим в правую часть:

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

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

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

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

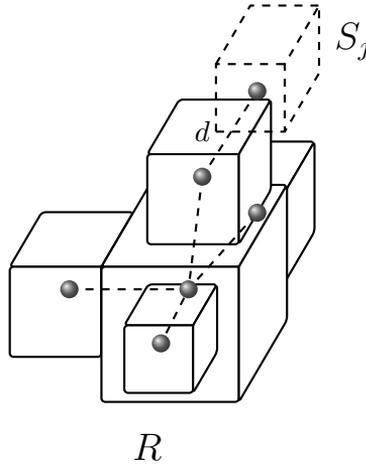


Рис. 8. Переход индукции.

По предположению индукции имеем:

$$G \geq \frac{1}{96} \cdot \frac{S^2}{V}. \quad (14)$$

Докажем, что:

$$G' \geq \frac{1}{96} \cdot \frac{S'^2}{V'}. \quad (15)$$

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

$$\Delta G = d + r_j - r_i, \quad \Delta S = 24r_j^2 - s, \quad \Delta V = 8r_j^3 - v, \quad (16)$$

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

Заметим, что неравенство (15) равносильно:

$$(G + \Delta G)(V + \Delta V) \geq \frac{1}{96} \cdot (S + \Delta S)^2. \quad (17)$$

Докажем вспомогательное неравенство:

$$\Delta G \cdot \Delta V \geq \frac{1}{96}(\Delta S)^2. \quad (18)$$

Сначала оценим ΔG снизу, а именно, покажем, что

$$\Delta G \geq r_j - \frac{1}{2}v^{1/3}, \quad (19)$$

- 1) Если $r_i \leq d$, то $\Delta G = d - r_i + r_j \geq r_j$, и (19) выполнено.
- 2) Рассмотрим случай $r_i > d$. По лемме 2 шар $B(c_j, r_j)$ не вложен в шар $B(c_i, r_i)$. Тогда заметим, что множество $A_k \cap B(c_j, r_j)$ содержит пересечение $B(c_i, r_i) \cap B(c_j, r_j)$, внутри которого помещается шар радиуса $r_i - d$ (см. рис. 9).

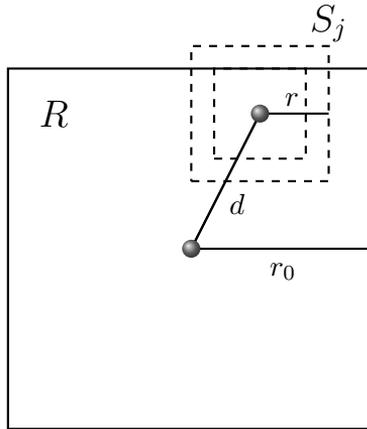


Рис. 9. Переход индукции при $d \leq r_i$.

Таким образом, имеет место неравенство $v \geq (2(r_i - d))^3$, а значит $r_i - d \leq \frac{1}{2}v^{1/3}$, значит (19) выполнено.

Используя (19), (16), затем лемму 8 при $a = 2r_j$, $b = v^{1/3}$, получим

$$\Delta G \cdot \Delta V \geq \left(r_j - \frac{1}{2}v^{1/3}\right) (8r_j^3 - v) \geq \frac{3}{8}(4r_j^2 - v^{2/3})^2. \quad (20)$$

Применяя лемму 7 для множества $A_k \cap B(c_j, r_j)$, имеем $s \geq 6v^{2/3}$, значит с учётом (20) получим

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

Таким образом, вспомогательное неравенство (18) доказано. Используя его, докажем основное неравенство (17):

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

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

По неравенству (14) имеем:

$$G \cdot V \geq \frac{1}{96} S^2. \quad (21)$$

Далее по неравенству средних и из неравенств (21), (18) следует:

$$\Delta G \cdot V + \Delta V \cdot G \geq 2\sqrt{G \cdot V \cdot \Delta V \cdot \Delta G} \geq \frac{1}{96} (2S \cdot \Delta S). \quad (22)$$

Таким образом, сложив неравенства (21), (18) и (22), получим требуемое неравенство (17). \square

В качестве прямого следствия из лемм 5 и 9 получаем утверждение:

Лемма 10. Для любого $t \geq 0$, $I \in \mathfrak{I}(t)$ верна следующая оценка:

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

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

Также имеет место следующее соотношение:

Лемма 11. Для любого множества $I \in \mathfrak{I}$, $t \in (a_I, b_I)$ верно равенство:

$$v'_I(t) = \frac{1}{6} s_I(t) p'_I(t),$$

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

Доказательство. По определению производной с учётом леммы 2 имеем:

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

\square

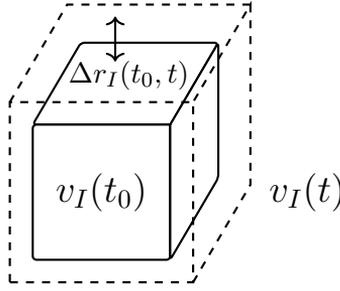


Рис. 10. Расширение множества $R_I(t)$.

Лемма 12. Для любого $t \geq 0$, $I \in \mathfrak{I}(t)$ верно следующее утверждение:

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

Доказательство. Заметим, что множество $M_I(t)$ состоит из $|I|$ кубических элементов, в которых находятся выходы схемы K (на рис. 11 центры этих элементов обозначены черными точками) и оставшихся элементов (их центры обозначены серыми точками). Объем кубических элементов с выходами схемы K равен $|I| \leq m_I$. Объем оставшихся элементов не больше $8V(R_I(t))$, так как если кубический элемент $s \in M_I(t)$, то центр s находится в $R_I(t)$, а значит пересечение с множеством $R_I(t)$ занимает не менее $1/8$ части s . Таким образом, получаем требуемую оценку. \square

3.5. Вспомогательные утверждения

В данном параграфе обобщим некоторые результаты для плоских схем, полученные в работе [14], на объёмные схемы, и также воспользуемся результатами работы [26]. Доказательство всех лемм аналогично и отличается лишь заменой некоторых констант, которые будут явно указаны ниже и никак не влияют на идею рассуждений.

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

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

Лемма 13. (Калачёв Г.В., [14, лемма 1]) Если $u \leq h$, то

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

Лемма 14. (Ефимов А.А., [26, лемма 7]) Количество объёмных схем объёмом v не больше, чем $2^{C_2 v}$, где C_2 — некоторая константа.

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

$$V(K_0) \leq \frac{1}{C_0} |(K_0K)|d, \quad U_D((K_0|K)) \leq \frac{|(K_0K)|}{5 \log_2 d}, \quad (23)$$

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

Лемма 16. (Калачёв Г.В., [13, лемма 10]) Для любой плоской схемы K и любого подмножества её выходов U существует схема K_U , носитель которой лежит в носителе схемы K , множество её выходов совпадает с U и на каждом из этих выходов K_U реализует ту же функцию, что и схема K .

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

Лемма 17. (Ефимов А.А., [26, лемма 10]) Пусть $\log_2 m \leq \frac{\varepsilon_1}{6}d$, где значение ε_1 взято из условия леммы 15. Тогда $|L_0(D, m)| = o(2^{md})$ при $d \rightarrow \infty$, $n \log_2 n = o(d)$.

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

Определение: Рассмотрим множество $L_1(D, m)$ операторов $f : D \rightarrow \{0, 1\}^m$, реализуемых некоторой схемой K так, что существует подсхема K_0 такая, что все входы $(K_0|K)$ лежат на последнем слое схемы K_0 относительно выходов (K_0K) и

$$V(K_0) \leq \frac{1}{C_4} |(K_0K)|d, \quad U_D(K_0|K) \leq \frac{1}{9}, \quad (24)$$

где $C_4 = \frac{32}{15}C_2$.

Лемма 18. (Аналог [14, лемма 10] для объёмных схем). Пусть $m, n \in \mathbb{N}$, $D \subseteq \{0, 1\}^n$, $d = |D|$. Тогда

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

Доказательство. Отметим, что подобный выбор константы C_4 в определении класса L_1 позволил оставить все технические выкладки в неизменном виде. Единственный геометрический факт, который следует учесть: имеется не более $2^{C_2 \frac{1}{C_4} m_0 d} = 2^{\frac{15}{32} m_0 d}$ схем объёма не более $\frac{1}{C_4} m_0 d$ (лемма 14). \square

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

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

3.6. Основное доказательство

Лемма 19. *Для любого $t \geq 0$ и множества $I \in \mathfrak{I}(t)$ верны следующие оценки:*

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

Доказательство. Проведём доказательство индукцией по мощности множества I .

База индукции: $|I| = 0$. Поскольку $\emptyset \notin \mathfrak{I}$, то здесь доказывать нечего.

Шаг индукции: $|I| \geq 1$.

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

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

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

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

- 1) $u_I = \sum_{j=1}^k u_{I_j}$ по определению. Верна оценка

$$\ell_q(R_I) = \ell_q \left(\bigcup_{j=1}^k R_{I_j} \right) \leq \sum_{j=1}^k \ell_q(R_{I_j}), \quad q = 1, 2, 3.$$

Складывая неравенства, получаем

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

Поскольку $|I_j| \leq |I|$, $j = 1, \dots, k$, то по предположению индукции верно

$$u_{I_j} \geq p(R_{I_j}), \quad j = 1, \dots, k.$$

Отсюда получаем оценку

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

- 2) По определению и свойствам u_I , верно $u_I = \sum_{j=1}^k u_{I_j}$, $m_I = \sum_{j=1}^k m_{I_j}$.

По предположению индукции имеем:

$$u_J \geq 2 \frac{m_J t^{1/3}}{l^{2/3}}, \quad J = I_1, \dots, I_k.$$

Складывая неравенства, получаем требуемую оценку:

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

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

- 1) Покажем, что

$$u_I(t) \geq p(R_I(t)) \quad \text{при} \quad t \in [a_I, b_I]. \quad (25)$$

Случай $t = a_I$ рассмотрен в пункте I. Из (10) имеем:

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

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

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

Преобразуем:

$$u_I^{3/2}(t) \geq 2^{3/2} \cdot \frac{m_I}{l} v_I^{1/2}(t). \quad (26)$$

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

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

Преобразуем неравенство:

$$\frac{3}{2}(u_I(t))^{1/2} u_I'(t) \geq \sqrt{2} \cdot \frac{m_I}{l} \frac{v_I'(t)}{(v_I(t))^{1/2}}. \quad (27)$$

По определению $u_I(t)$ имеем неравенство:

$$u_I'(t) \geq \frac{m_I}{l} p_I'(t). \quad (28)$$

Также из лемм 10 и 11 имеем:

$$(u_I(t))^{1/2} \geq \sqrt{\frac{1}{32} \frac{s_I(t)}{(v_I(t))^{1/2}}} = \frac{3}{\sqrt{8}} \frac{v_I'(t)}{(v_I(t))^{1/2} \cdot p_I'(t)}. \quad (29)$$

Перемножив неравенства (28) и (29) и огрубив константу, получим неравенство (27).

Таким образом, основная лемма доказана. \square

Теорема 1. Если $D \subseteq \{0, 1\}^n$, то для некоторой константы $C > 0$ верно

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

для почти всех операторов $f \in P_2(D, m)$ при $n \log_2 n = o(|D|)$, $\log_2 m = o(2^n)$, $|D| \rightarrow \infty$.

Доказательство. Обозначим $d := |D|$, $l := \log_2 d$. Можно считать, что d достаточно велико, и $d \geq \frac{1}{8\alpha}$. Зафиксируем произвольный оператор $f \in P_2(D, m) \setminus L_0(D, m) \setminus L_1(D, m)$ и оценим его средний потенциал. Заметим, что по леммам 17 и 18 верно $|L_0(D, m) \cup L_1(D, m)| = o(2^{md})$. Таким образом, полученная далее оценка верна для почти всех операторов из $P_2(D, m)$ при $n \log_2 n = o(d)$, $\log_2 m = o(2^n)$, $d \rightarrow \infty$. Зафиксируем схему K , реализующую f с минимальным потенциалом (то есть, такую, что $U_D(K) = U(f)$), и построим для неё расслоение \mathfrak{R} .

Обозначим $t_0 = \alpha d$. По лемме 12 и определению α для $t \in [0, t_0]$ имеем:

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

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

$$U_D(M_I(t)|K) \geq \max\left(\frac{1}{9}, \frac{(M_I(t)K)}{5l}\right) \geq \frac{1}{9} \max\left(1, \frac{m_I}{l}\right). \quad (30)$$

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

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

Из неравенств (7), (30) и определения $u_I(t)$ получаем:

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

Из леммы 6 и пункта 1) леммы 19 следует:

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

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

$$U_D(K) \geq \frac{1}{54} \sum_{I \in \mathfrak{I}(t_0)} u_I(t_0) \geq \frac{1}{18} \sum_{I \in \mathfrak{I}(t_0)} v_I(t_0)^{1/3} = \frac{t_0^{1/3}}{18} \sum_{I \in \mathfrak{I}(t_0)} m_I^{1/3}. \quad (31)$$

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

$$\begin{aligned} (x_1^3)^{1/3} + (x_2^3)^{1/3} + \dots + (x_s^3)^{1/3} &\geq (x_1^3 + x_2^3 + \dots + x_s^3)^{1/3}, \\ x_1 + x_2 + \dots + x_s &\geq (x_1^3 + x_2^3 + \dots + x_s^3)^{1/3}. \end{aligned}$$

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

$$m_1^{1/3} + m_2^{1/3} + \dots + m_s^{1/3} \geq (m_1 + m_2 + \dots + m_s)^{1/3}.$$

Воспользуемся полученным результатом и продолжим неравенство (31):

$$U_D(K) \geq \frac{1}{18} \left(\sum_{I \in \mathcal{J}(t_0)} m_I^{1/3} \right) \cdot t_0^{1/3} \geq \frac{1}{18} m^{1/3} \cdot t_0^{1/3} = \frac{\alpha^{1/3}}{18} \sqrt[3]{m \cdot d}. \quad (32)$$

При $m > l$ по пункту 2) леммы 12 получаем:

$$\begin{aligned} U_D(K) &\geq \frac{1}{54} \sum_{I \in \mathcal{J}(t_0)} u_I(t_0) \geq \\ &\geq \frac{1}{27} \sum_{I \in \mathcal{J}(t_0)} \frac{m_I \cdot t_0^{1/3}}{l^{2/3}} = \frac{1}{27} \frac{m \cdot t_0^{1/3}}{l^{2/3}} = \frac{\alpha^{1/3}}{27} \frac{m \sqrt[3]{d}}{l^{2/3}}. \end{aligned} \quad (33)$$

Соединив результаты неравенств (32) и (33) и приняв $C = \alpha^{1/3}/27$, получаем требуемое условие теоремы. \square

Список литературы

- [1] Muller D.E., "Complexity in Electronics Switching Circuits", *IRE Transactions on Electronic Computers*, **EC-5**, no. 1 (1956), 15–19.
- [2] Вайнцвайг М.Н., "О мощности схем из функциональных элементов", *Докл. АН СССР*, **Т. 139**, № 2 (1961), 320–323.
- [3] Лупанов О.Б., "Об одном подходе к синтезу управляющих систем – принципе локального кодирования", *Проблемы кибернетики*, **14** (1965), 31–110.
- [4] Кравцов С.С., "О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов", *Проблемы кибернетики*, **19** (1967), 285–293.
- [5] Коршунов А.Д., "Об оценках сложности из объемных функциональных элементов и объемных схем из функциональных элементов", *Проблемы кибернетики*, **19** (1967), 275–283.
- [6] Касим-Заде О.М., "Об одной мере сложности схем из функциональных элементов", *Проблемы кибернетики*, **38** (1981), 117–179.

- [7] Шкаликowa Н.А., “О реализации булевых функций схемами из клеточных элементов”, *Математические вопросы кибернетики*, **2** (1989), 177–197.
- [8] Ложкин С.А., Рыбко А.И., Сапоженко А.А., Хромкович Ю., Шкаликowa Н.А., “Об одном подходе к оценке пространственной сложности схем из функциональных элементов”, *Mathematical Problems in Computation Theory. Banach Center Publications*, 1987, 501–510.
- [9] Черемисин О.В., “Об активности схем из клеточных элементов, реализующих систему всех конъюнкций”, *Дискретная математика*, **15:2** (2003), 113–122.
- [10] Ronnie Barequet, Gill Barequet, Gunter Rote, “Formulae and Growth Rates of High-Dimensional Polycubes”, *Electronic Notes in Discrete Mathematics*, **34** (2009), 459–463..
- [11] Шуткин Ю.С., “Об одновременной минимизации объёмной и временной сложности контактных и вентильных схем”, *Интеллектуальные системы. Теория и приложения*, **14**, № 1-4 (2010), 595–615.
- [12] Чашкин А.В., “Дискретная математика”, *Академия Москва*, 2012, 352.
- [13] Калачёв Г.В., “Порядок мощности плоских схем, реализующих булевы функции”, *Дискретная математика*, **26:1** (2014), 49–74.
- [14] Калачёв Г.В., “Нижние оценки мощности плоских схем, реализующих частичные булевы операторы”, *Интеллектуальные системы. Теория и приложения*, **18:2** (2014), 279–322.
- [15] Калачёв Г.В., “Об одновременной минимизации площади, мощности и глубины плоских схем, реализующих частичные булевы операторы”, *Интеллектуальные системы. Теория и приложения*, **20:2** (2016), 203–266.
- [16] Калачёв Г.В., “Об оценках мощности плоских схем для замкнутых классов булевых функций”, *Интеллектуальные системы. Теория и приложения*, **20:3** (2016), 52–57.
- [17] Калачёв Г.В., “Оценки мощности плоских схем, реализующих функции с ограниченным числом единиц”, *Интеллектуальные системы. Теория и приложения*, **21:1** (2017).
- [18] Калачёв Г.В., “Оценки мощности плоских схем, реализующих монотонные функции”, *Интеллектуальные системы. Теория и приложения*, **21:2** (2017).

- [19] Калачёв Г.В., “Обобщение оценок мощности плоских схем, реализующих частичные булевы операторы”, *Вестник Московского университета. Серия 1: Математика. Механика*, **73**:3 (2018), 60–64.
- [20] Калачёв Г.В., “О нижней оценке максимального потенциала плоских схем с несколькими выходами через площадь”, *Интеллектуальные системы. Теория и приложения*, **22**:1 (2018), 111–117.
- [21] Ефимов А.А., “Верхняя оценка энергопотребления в классе объемных схем”, *Интеллектуальные системы. Теория и приложения*, **23**:1 (2019), 117–132.
- [22] Ефимов А.А., “Верхняя оценка энергопотребления объемных схем, реализующих булевы операторы”, *Интеллектуальные системы. Теория и приложения*, **23**:2 (2019), 105–124.
- [23] Сытдыков Т.Р., “Сложность синтеза многомерных прямоугольных схем”, *Интеллектуальные системы. Теория и приложения*, **23**:3 (2019), 61–80.
- [24] Сытдыков Т.Р., Калачёв Г.В., “Сложность многослойных d-мерных схем”, *Интеллектуальные системы. Теория и приложения*, **25**:2 (2021), 131–154.
- [25] Воротников А.С., “Верхние оценки переключательной мощности плоских схем, реализующих автономные автоматные функции”, *Интеллектуальные системы. Теория и приложения*, **25**:4 (2021), 96–99.
- [26] Ефимов А.А., “Оценки энергопотребления для класса объёмных схем с близкими выходами”, *Интеллектуальные системы. Теория и приложения*, **27**:3 (2022), 109–150.

Lower estimate of potential for a class of volume circuits.

Efimov A.A.

In this paper, volume circuits are considered, which are the embeddings of Boolean circuits in space. For volume circuits, the lower bound on the potential is obtained. Potential is a measure of circuit activity equal to the number of gates that produce one on a given input. It is shown that for almost all partial operators with n inputs and m outputs, the potential of the volume circuit that implements them is not less than $\frac{m \sqrt[3]{d}}{\min^{2/3}(m, \log_2 d)}$, where d is the size of the domain.

Keywords: Boolean circuits, volume circuits, circuit complexity, circuit activity, potential.

References

- [1] Muller D.E., “Complexity in Electronics Switching Circuits”, *IRE Transactions on Electronic Computers*, **EC-5**, no. 1 (1956), 15–19.
- [2] Weinzweig M.N., “On the power of circuits from functional elements”, *Report of the Academy of Sciences of the USSR*, **T. 139**, № 2 (1961), 320–323.
- [3] Lupanov O.B., “On one approach to the synthesis of control systems - the principle of local coding”, *Problems of cybernetics*, **14** (1965), 31–110.
- [4] Kravtsov S.S., “On the implementation of logic algebra functions in one class of circuits from functional and switching elements”, *Problems of cybernetics*, **19** (1967), 285–293.
- [5] Korshunov A.D., “On complexity estimates from three-dimensional functional elements and three-dimensional circuits from functional elements”, *Problems of cybernetics*, **19** (1967), 275–283.
- [6] Qasim-Zade O.M., “On one measure of complexity of circuits from functional elements”, *Problems of cybernetics*, **38** (1981), 117–179.
- [7] Shkalikova N.A., “On the implementation of Boolean functions by circuits of cellular elements”, *Mathematical problems of cybernetics*, **2** (1989), 177–197.
- [8] Lozhkin S.A., Rybko A.I., Sapozhenko A.A., Khromkovich Yu., Shkalikova N.A., “On one approach to estimating the spatial complexity of circuits from functional elements”, *Mathematical Problems in Computation Theory. Banach Center Publications*, 1987, 501–510.
- [9] Cheremisin O.V., “On the activity of schemes of cellular elements that implement the system of all conjunctions”, *Discrete Math*, **15:2** (2003), 113–122.
- [10] Ronnie Barequet, Gill Barequet, Gunter Rote, “Formulae and Growth Rates of High-Dimensional Polycubes”, *Electronic Notes in Discrete Mathematics*, **34** (2009), 459–463..
- [11] Shutkin Yu.S., “On the Simultaneous Minimization of the Volumetric and Time Complexity of Contact and Gate Circuits”, *Intelligent systems*, **14**, № 1-4 (2010), 595–615.
- [12] Chashkin A.V., “Discrete Math”, *Academy Moscow*, 2012, 352.

- [13] Kalachev G.V., “Power order of flat circuits that implement Boolean functions”, *Discrete Math*, **26**:1 (2014), 49–74.
- [14] Kalachev G.V., “Lower Bounds for the Cardinality of Planar Circuits Implementing Partial Boolean Operators”, *Intelligent systems*, **18**:2 (2014), 279–322.
- [15] Kalachev G.V., “On the Simultaneous Minimization of Area, Power, and Depth of Flat Circuits Realizing Partial Boolean Operators”, *Intelligent systems*, **20**:2 (2016), 203–266.
- [16] Kalachev G.V., “On Estimates for the Cardinality of Flat Circuits for Closed Classes of Boolean Functions”, *Intelligent systems*, **20**:3 (2016), 52–57.
- [17] Kalachev G.V., “Estimates for the Power of Flat Circuits Implementing Functions with a Limited Number of Ones”, *Intelligent systems*, **21**:1 (2017).
- [18] Kalachev G.V., “Estimates for the Power of Flat Circuits Implementing Monotone Functions”, *Intelligent systems*, **21**:2 (2017).
- [19] Kalachev G.V., “Generalization of Cardinality Estimates for Planar Circuits Implementing Partial Boolean Operators”, *Bulletin of Moscow University. Series 1: Mathematics. Mechanics*, **73**:3 (2018), 60–64.
- [20] Kalachev G.V., “On a lower bound for the maximum potential of planar circuits with several outputs through an area”, *Intelligent systems*, **22**:1 (2018), 111–117.
- [21] Efimov A.A., “Upper estimate of power consumption in the class of volumetric circuits”, *Intelligent systems*, **23**:1 (2019), 117–132.
- [22] Efimov A.A., “Upper Bound for Energy Consumption of Volumetric Circuits Implementing Boolean Operators”, *Intelligent systems*, **23**:2 (2019), 105–124.
- [23] Sytdykov T.R., “Complexity of synthesis of multidimensional rectangular schemes”, *Intelligent systems*, **23**:3 (2019), 61–80.
- [24] Sytdykov T.R., Kalachev G.V., “Complexity of multilayer d-dimensional circuits”, *Intelligent systems*, **25**:2 (2021), 131–154.
- [25] Vorotnikov A.S., “Upper Bounds for the Switching Power of Flat Circuits Realizing Autonomous Automaton Functions”, *Intelligent systems*, **25**:4 (2021), 96–99.

- [26] Efimov A.A., “Energy consumption estimates for a class of volumetric circuits with similar outputs”, *Intelligent systems*, **27**:3 (2022), 109–150.

О числе p -сократимых индуцированных вероятностных функций

Е. Е. Трифонова¹

Статья посвящена изучению доли булевых функций, индуцирующих p -сократимые функции разного типа, среди всех булевых функций.

Ключевые слова: бернуллиевская случайная величина, конечная порожденность, преобразование случайных величин.

1. Введение

Преобразования бернуллиевских случайных величин с рациональными вероятностями посредством булевых функций рассматривались в работах Р. Л. Схиртладзе, Ф. И. Салимова и Р. М. Колпакова (см. [1, 2, 3], а также обзор в [4]). Р. Л. Схиртладзе [1] показал, что преобразования с помощью конъюнкций и дизъюнкций ($\&$ и \vee) позволяют породить все множества двоично-рациональных и троично-рациональных распределений, используя конечное множество распределений. Ф. И. Салимов в [2] показал, что множества p -ично-рациональных распределений конечно порождены при преобразованиях операциями системы $\{x_1x_2 \vee \bar{x}_1x_3, 0, 1\}$. В работах Р. М. Колпакова [3] установлена конечная порожденность относительно преобразований системой $\{\&, \vee\}$ множеств рациональных бернуллиевских распределений, у которых в разложении знаменателя на простые множители могут встречаться простые числа из заданного конечного множества мощности не менее 2.

Ранее автором было получено, что преобразования случайных величин с распределениями из конечного множества с помощью функции голосования не позволяют выразить все вероятности, записываемые пятнадцатеричными дробями [5]. Этот результат можно также распространить на все p -ичные дроби для произвольного простого p , $p \geq 5$. Кроме того, в статье [6] сформулированы некоторые свойства, которыми должны обладать функции из конечно порождающего множества при условии, что функции индуцируют p -несократимые вероятностные функции. Под p -несократимыми функциями понимаются такие функции, которые при подстановке в качестве значений переменных несократимых правильных дробей, на выходе дают также несократимые дроби со знамена-

¹Трифопова Екатерина Евгеньевна — инженер-исследователь, ИПМ им. М.В.Келдыша РАН, e-mail: etrifonova@keldysh.ru.

Trifonova Ekaterina Evgen'evna — research engineer, Keldysh Institute of Applied Mathematics (Russian Academy of Sciences)

телем, степень которого есть сумма степеней знаменателей подставляемых дробей. Если называть вероятностные функции, не обладающие подобным свойством, p -сократимыми, то возникает вопрос, какова доля p -сократимых вероятностных функций среди всех вероятностных функций, индуцированных булевыми функциями без фиктивных переменных. Решению именно этой задачи посвящена данная работа. Особенно важной эта задача представляется в связи с тем, что универсальная функция, входящая в состав конечно порождающей системы, описанной Ф.И.Салимовым, индуцирует p -сократимую функцию.

2. Основные понятия

Пусть x — случайная величина, принимающая значение 1 и 0 с вероятностью \hat{x} и $1 - \hat{x}$ соответственно. Тогда распределение этой случайной величины однозначно определяется значением \hat{x} . Будем считать, что каждой случайной величине x , принимающей значения 0 и 1, сопоставлено число $\hat{x} \in [0; 1]$.

Будем рассматривать преобразования, осуществляемые в результате подстановки независимых в совокупности случайных величин со значениями 0 и 1 вместо переменных булевых функций. При этом в качестве преобразователей будем брать только булевы функции без фиктивных переменных.

Пусть задана булева функция $f(x_1, \dots, x_n): \{0, 1\}^n \rightarrow \{0, 1\}$, тогда вероятностная функция $f(\hat{x}_1, \dots, \hat{x}_n): [0; 1]^n \rightarrow [0; 1]$, индуцированная булевой функцией $f(x_1, \dots, x_n)$, определяется соотношением:

$$\hat{f}(\hat{x}_1, \dots, \hat{x}_n) = \sum_{\substack{(x_1, \dots, x_n): \\ f(x_1, \dots, x_n)=1}} \prod_{i=1}^n (x_i \hat{x}_i + (1 - x_i)(1 - \hat{x}_i)).$$

Будем обозначать как $H(p^k)$ всевозможные правильные несократимые дроби со знаменателем p^k .

Пусть $f(x_1, \dots, x_n) \in P_2$, $\hat{f}(\hat{x}_1, \dots, \hat{x}_n)$ — индуцированная f вероятностная функция, p — простое, $p \geq 5$. Тогда если $\hat{x}_i \in H(p^{k_i})$ для $i \in \{1, \dots, n\}$, то значение индуцированной функции \hat{f} можно представить как $\hat{f}(\hat{x}_1, \dots, \hat{x}_n) = \frac{D}{p^m}$, $D \bmod p \neq 0$. При этом если $m = k_1 + \dots + k_n$ для заданного p , любых $\hat{x}_i \in H(p^{k_i})$, а также любых $k_i \in \mathbb{N}$, $i \in \{1, \dots, n\}$, то \hat{f} будем называть p -несократимой функцией.

Будем называть индуцированные функции, которые не обладают такими свойствами, p -сократимыми функциями. При этом заметим, что для каждой p -сократимой функции найдется хотя бы один такой набор значений переменных $\hat{x}_i \in H(p^{k_i})$, что $m < k_1 + \dots + k_n$, а равенство

$m = k_1 + \dots + k_n$ может как выполняться, так и не выполняться при других значения переменных $\widehat{x}_i \in H(p^{k_i})$.

Между булевой функцией и индуцированной ей функцией существует взаимнооднозначное соответствие. Говоря о числе p -сократимых функций, мы одновременно говорим и о числе булевых функций, индуцирующих p -сократимые функции.

Вероятностную функцию, индуцированную булевой функцией, можно записать в виде

$$\widehat{f}(\widehat{x}_1, \dots, \widehat{x}_n) = \sum_{\kappa_1, \dots, \kappa_n \in \{0;1\}} \alpha_{\kappa_1 \dots \kappa_n} \widehat{x}_1^{\kappa_1} \dots \widehat{x}_n^{\kappa_n},$$

где $\widehat{x}_i^0 = 1$, $\widehat{x}_i^1 = \widehat{x}_i$. Тогда будет ли являться функция p -сократимой или p -несократимой, определяется величиной коэффициента $\alpha_{1\dots 1}$ при $\widehat{x}_1 \dots \widehat{x}_n$. Очевидно, что \widehat{f} будет p -сократимой в двух случаях:

- 1) $\alpha_{1\dots 1} = 0$, в этом случае функцию \widehat{f} будем называть p -сократимой первого типа;
- 2) $\alpha_{1\dots 1} = p^t A$, где $t \geq 1$, $A \in \mathbb{Z}$, $A \bmod p \neq 0$, в этом случае функцию \widehat{f} будем называть p -сократимой второго типа.

Заметим, что p -сократимые функции первого типа будут p -сократимыми для любого простого $p \geq 5$, а p -сократимые функции второго типа будут являться таковыми для одних p и не будут для других.

Напомним, что для булевой функции $f(x_1, \dots, x_n)$ единичными наборами называются совокупности значений переменных x_1, \dots, x_n , на которых функция f принимает единичное значение.

Обозначим число нулей в наборе (x_1, \dots, x_n) как

$$\theta(x_1, \dots, x_n) = \sum_{i=1}^n (1 - x_i).$$

Число наборов с нечетным числом нулей среди единичных наборов булевой функции $f(x_1, \dots, x_n)$ запишем как

$$\eta_o(f) = \sum_{\substack{(x_1, \dots, x_n): \\ f(x_1, \dots, x_n)=1}} \theta(x_1, \dots, x_n) \bmod 2.$$

Выразим число наборов с четным числом нулей среди единичных наборов булевой функции $f(x_1, \dots, x_n)$ следующим образом:

$$\eta_e(f) = \sum_{\substack{(x_1, \dots, x_n): \\ f(x_1, \dots, x_n)=1}} (1 - \theta(x_1, \dots, x_n) \bmod 2).$$

Лемма 1. Для булевой функции $f(x_1, \dots, x_n)$, не содержащей фиктивных переменных, и индуцированной ей функции $\widehat{f}(\widehat{x}_1, \dots, \widehat{x}_n)$ выполняется $\alpha_{1\dots 1} = \eta_e(f) - \eta_o(f)$

Доказательство. Из определения вероятностной функции $\widehat{f}(\widehat{x}_1, \dots, \widehat{x}_n)$, индуцированной булевой функцией $f(x_1, \dots, x_n)$, следует, что функцию $\widehat{f}(\widehat{x}_1, \dots, \widehat{x}_n)$ можно записать в виде:

$$\widehat{f}(\widehat{x}_1, \dots, \widehat{x}_n) = \sum_{j=1}^{\omega_1(f)} \delta_{1j} \dots \delta_{nj},$$

где $\delta_{1j} \dots \delta_{nj}$ соответствует единичному набору функции f следующим образом: $\delta_{ij} = \widehat{x}_i$, если $x_i = 1$, $\delta_{ij} = 1 - \widehat{x}_i$, если $x_i = 0$, $\omega_1(f)$ — число единичных наборов функции f .

Очевидно, что после раскрытия всех скобок у выражения $\delta_{1j} \dots \delta_{nj}$, коэффициент перед слагаемым $\widehat{x}_1 \dots \widehat{x}_n$ будет равен либо 1, либо -1 . Коэффициент будет равен 1 в том случае, если число скобок вида $1 - \widehat{x}_i$ будет четно, и будет равен -1 , если нечетно. Соответственно, для всех единичных наборов получим, что суммарный коэффициент (обозначаемый как $\alpha_{1\dots 1}$) перед $\widehat{x}_1 \dots \widehat{x}_n$ будет равен $\eta_e(f) - \eta_o(f)$. Таким образом, $\alpha_{1\dots 1} = \eta_e(f) - \eta_o(f)$. □

Лемма 2. Если f индуцирует p -сократимую функцию первого типа \widehat{f} , то $\eta_e(f) = \eta_o(f)$.

Доказательство. По определению p -сократимой функции первого типа $\alpha_{1\dots 1} = 0$. Из леммы 1 получаем, что $\alpha_{1\dots 1} = \eta_e(f) - \eta_o(f) = 0$. Следовательно, $\eta_e(f) = \eta_o(f)$. □

Лемма 3. Если $f(x_1, \dots, x_n)$ содержит фиктивные переменные, то $\eta_e(f) = \eta_o(f)$.

Доказательство. Без ограничения общности будем считать, что x_1 — фиктивная переменная. Тогда для любого набора (x_2, \dots, x_n) будет выполнено $f(0, x_2, \dots, x_n) = f(1, x_2, \dots, x_n)$. Отсюда очевидно следует, что $\eta_e(f) = \eta_o(f)$. □

Лемма 4. Для булевой функции f $\eta_e(f) = \eta_o(f)$ тогда и только тогда, когда либо f содержит не менее одной фиктивной переменной, либо когда f индуцирует p -сократимую функция первого типа.

Доказательство. Докажем необходимость. Пусть для булевой функции f $\eta_e(f) = \eta_o(f)$, а наше предположение неверно. Т.е. f не будет содержать фиктивных переменных и индуцированная функция \widehat{f} не будет являться p -сократимой первого типа, то есть $\alpha_{1\dots 1} \neq 0$. По лемме 1 имеем

$\alpha_{1\dots 1} = \eta_e(f) - \eta_o(f)$, т. е. $\alpha_{1\dots 1} = 0$. Получили противоречие, необходимость доказана.

Достаточность доказана в леммах 2 и 3. □

Лемма 5. *Если булева функция f индуцирует p -сократимую функцию второго типа \hat{f} , то $\eta_e(f) - \eta_o(f)$ будет кратна p .*

Доказательство. Следует из леммы 1 и определения p -сократимых функций второго типа. □

3. Оценка числа p -сократимых функций первого типа

Число булевых функций f таких, что $\eta_e(f) = \eta_o(f)$, мы можем посчитать как

$$\sum_{k=0}^{2^n-1} C_{2^n-1}^k C_{2^n-1}^k.$$

При этом согласно лемме 4 это число будет включать в себя все функции, которые индуцируют p -сократимые первого типа, и также и все функции, которые содержат фиктивные переменные.

Число функций от n , содержащих фиктивные переменные, может быть вычислено как:

$$2^{2^n} - \sum_{k=0}^n (-1)^k C_n^k 2^{2^{n-k}} = - \sum_{k=1}^n (-1)^k C_n^k 2^{2^{n-k}}.$$

Тогда число p -сократимых функций первого типа, будет равно разности двух выражений, приведенных выше:

$$\sum_{k=0}^{2^n-1} C_{2^n-1}^k C_{2^n-1}^k + \sum_{k=1}^n (-1)^k C_n^k 2^{2^{n-k}}.$$

Используя свертку Вандермонда [7], преобразуем первое слагаемое следующим образом:

$$\sum_{k=0}^{2^n-1} C_{2^n-1}^k C_{2^n-1}^k = \sum_{k=0}^{2^n-1} C_{2^n-1}^k C_{2^n-1}^{2^n-1-k} = C_{2^n-1+2^n-1}^{2^n-1} = C_{2^n}^{2^n-1} = C_{2^n}^{2^n/2}.$$

Теперь оценим величину второго слагаемого.

$$\sum_{k=1}^n (-1)^k C_n^k 2^{2^{n-k}} = -n2^{2^{n-1}} + \dots$$

Известно, что его асимптотика равна $-n2^{2^n-1}$.

Для оценки значения выражения вида C_{2l}^l при $n \rightarrow \infty$ будем использовать формулу Стирлинга в виде $l! \sim \sqrt{2\pi l} \left(\frac{l}{e}\right)^l$. Тогда $C_{2l}^l \sim \frac{2^{2l}}{\sqrt{\pi l}}$.

Подставим 2^n вместо $2l$, а 2^{n-1} вместо l . Получаем, что $C_{2^n}^{2^{n-1}} \sim \frac{2^{2^n}}{\sqrt{\pi 2^{n-1}}} =$

$$\frac{2^{2^n}}{\sqrt{\frac{\pi}{2}}(\sqrt{2^n})} = \sqrt{\frac{2}{\pi}} \frac{2^{2^n}}{2^{n/2}}.$$

Оценим асимптотику разности выражений $C_{2^n}^{2^n/2} - n2^{2^n-1}$. Для этого представим $n2^{2^n-1}$ как $n\sqrt{2^{2^n}}$.

$$\text{Тогда } C_{2^n}^{2^n/2} - n2^{2^n-1} \sim \sqrt{2^{2^n}} \left(\sqrt{\frac{2}{\pi}} \frac{\sqrt{2^{2^n}}}{2^{n/2}} - n \right) \sim \sqrt{\frac{2}{\pi}} \frac{2^{2^n}}{2^{n/2}}.$$

Заметим, что число всех булевых функций асимптотически равно числу всех булевых функций без фиктивных переменных.

Поскольку число всех булевых функций от n переменных равно 2^{2^n} , то получаем, что доля сократимых функций первого типа при $n \rightarrow \infty$ асимптотически убывает как $\sqrt{\frac{2}{\pi}} \frac{1}{2^{n/2}}$.

4. Оценка числа p -сократимых функций второго типа

Для p -сократимых функций второго типа по определению $\alpha_{1\dots 1} = p^t A$, где $t \geq 1$, $A \in \mathbb{Z}$, $A \bmod p \neq 0$. По лемме 1 имеем, что $\eta_e(f) - \eta_o(f) = \alpha_{1\dots 1} = p^t A$. Тогда можем записать, что $|\eta_e(f) - \eta_o(f)| = sp$, где $s \in \mathbb{N}$, т. е. либо $\eta_e(f) = \eta_o(f) + ps$, если $\eta_e(f) > \eta_o(f)$, либо $\eta_o(f) = \eta_e(f) + ps$, если $\eta_o(f) > \eta_e(f)$. Для фиксированного s число таких функций равно

$$2 \sum_{i=0}^{2^{n-1}-sp} C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^i,$$

для всех допустимых s получаем, что общее число таких функций равно

$$\sum_{s=1}^{\lfloor \frac{2^n-1}{p} \rfloor} 2 \sum_{i=0}^{2^{n-1}-sp} C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^i.$$

Таким образом, число p -сократимых функций второго типа можно записать как

$$2 \sum_{s=1}^{\lfloor \frac{2^n-1}{p} \rfloor} \sum_{i=0}^{2^{n-1}-sp} C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^i.$$

Преобразуем выражение $C_{2^{n-1}}^i$ следующим образом

$$C_{2^{n-1}}^i = C_{2^{n-1}}^{2^{n-1}-i} = C_{2^{n-1}}^{2^{n-1}-i+sp-sp} = C_{2^{n-1}}^{2^{n-1}+sp-(sp+i)}.$$

Запишем число p -сократимых функций второго типа в виде

$$2 \sum_{s=1}^{\lfloor \frac{2^n-1}{p} \rfloor} \sum_i C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^{2^{n-1}+sp-(sp+i)}.$$

Рассмотрим сумму $\sum_i C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^{2^{n-1}+sp-(sp+i)}$. Положим $j = sp + i$. Применяя свертку Вандермонда [7], получаем следующую оценку сверху:

$$\sum_i C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^{2^{n-1}+sp-(sp+i)} \leq \sum_{j=0}^{2^{n-1}+sp} C_{2^{n-1}}^j C_{2^{n-1}}^{2^{n-1}+sp-j} = C_{2^n}^{2^{n-1}+sp}.$$

Оценим значение

$$2 \sum_{s=1}^{\lfloor \frac{2^n-1}{p} \rfloor} C_{2^n}^{2^{n-1}+sp}.$$

Используя метод мультисекции рядов (см., например, [7]), и применяя его к формуле бинома Ньютона, получим $p \sum_{s=0}^{\lfloor \frac{n-m}{p} \rfloor} C_n^{m+sp} \sim 2^n$ при $m < p$. Следовательно, с учетом симметрии биномиальных коэффициентов можем получить, что

$$2 \sum_{s=1}^{\lfloor \frac{2^n-1}{p} \rfloor} C_{2^n}^{2^{n-1}+sp} \sim 2 \frac{1}{2p} 2^{2^n} = \frac{1}{p} 2^{2^n}.$$

Соответственно, доля сократимых функций второго типа при $n \rightarrow \infty$ асимптотически не превышает $\frac{1}{p}$.

5. Заключение

Получено, что при $n \rightarrow \infty$ доля p -сократимых функций первого типа асимптотически равна $\sqrt{\frac{2}{\pi}} \frac{1}{2^{n/2}}$, а доля p -сократимых функций второго типа асимптотически не превышает $\frac{1}{p}$.

Следовательно, p -несократимые функции составляют асимптотически при $p \geq 5$ «большую часть» всех индуцированных вероятностных функций, однако если с ростом n доля p -сократимых функций первого типа уменьшается, то верхняя оценка доли p -сократимых функций второго типа асимптотически постоянна и зависит только от величины p .

Список литературы

- [1] Схиртладзе Р. Л., “О синтезе p -схемы из контактов со случайными дискретными состояниями”, *Сообщ. АН ГрузССР*, **26**:2 (1961), 181–186.
- [2] Салимов Ф. И., “Об одном семействе алгебр распределений”, *Изв. вузов. Математика*, 1988, № 7, 64–72.
- [3] Колпаков Р. М., “Об оценках сложности порождения рациональных чисел вероятностными контактными π -сетями”, *Вестн. Моск. ун-та. Математика. Механика*, 1992, № 6, 62–65.
- [4] Яшунский А. Д., “Алгебры вероятностных распределений на конечных множествах”, *Тр. МИАН*, **301** (2018), 320–335.
- [5] Трифонова Е. Е., “О бесконечной порожденности пятеричных дробей в одном классе преобразователей вероятностей”, *Изв. высш. учебн. завед. Поволжский регион. Физ.-мат. науки*, 2021, № 1, 39–48.
- [6] Трифонова Е. Е., “О некоторых свойствах конечно порождающих систем преобразователей p -ичных дробей”, *Дискретный анализ и исследование операций*, 2022, в печати.
- [7] Риордан Дж., *Комбинаторные тождества*, Наука, Москва, 1982, 255 pp.

On the number of p -reducible induced probability functions

Trifonova E.E.

We study the proportion of Boolean functions inducing p -reducible functions of various types among all Boolean functions.

Keywords: Bernoulli random variable, finite generation, random variable transformation.

References

- [1] Skhirtladze R. L., “On synthesis of p -schemes using switches with random discrete states”, *Soobshch. Akad. Nauk Gruz. SSR*, **26**:2 (1961), 181–186 (In Russian)
- [2] Salimov F. I., “A family of distribution algebras”, *Izv. vuzov. Matematika*, 1988, № 7, 64–72 (In Russian)

- [3] Kolpakov R. M., “On the bounds for the complexity of generation of rational numbers by stochastic contact π -networks”, *Vestn. Moskov. Univ. Ser. 1. Mat. Mekh.*, 1992, № 6, 62–65 (In Russian)
- [4] Yashunsky A. D., “Algebras of Probability Distributions on Finite Sets”, *Tr. MIAN*, **301** (2018), 320–335 (In Russian)
- [5] Trifonova E. E., “On infinite generativeness of quinary fractions in a class of probability transformers”, *Izv. vyssh. uchebn. zaved. Povolzhskiy region. Fiz.-mat. nauki*, 2021, № 1, 39–48 (In Russian)
- [6] Trifonova E. E., “On some properties of finitely generating transformer sets for p -ary fractions”, *Discrete Analysis and Operations Research*, 2022, in print (In Russian)
- [7] Riordan J., *Combinatorial identities*, Wiley, New York, 1968, 244 pp.

Часть 4.
Семинары кафедры MaTIC

Доклады семинара «Теория автоматов»

В 2022 году на научном семинаре «Теория автоматов» под руководством профессора Эльяра Эльдаровича Гасанова состоялось 14 докладов.

2 марта 2022 года

Асимптотически хорошие семейства классических и квантовых LDPC кодов

н.с. Пантелеев П. А., м.н.с. Калачев Г. В.

Классические LDPC коды являются важными компонентами современных систем хранения и передачи данных. Их квантовые аналоги (qLDPC коды) обещают значительную экономию ресурсов в протоколах для отказоустойчивых квантовых вычислений. Начиная с основополагающей работы Роберта Галлагера в начале 1960-х годов было известно, что существуют асимптотически хорошие семейства классических LDPC кодов, т.е. семейства, где размерность и минимальное расстояние растут линейно с ростом длины кода. Более того, 35 лет спустя Сипсер и Спилмен нашли эффективный способ построения таких кодов на основе графов расширителей (экспандерные коды). В то же время, вопрос о существовании асимптотически хороших квантовых LDPC кодов (qLDPC гипотеза) оставался открытым уже более двух десятилетий.

В докладе будет рассказано об аналоге экспандерных кодов Сипсера и Спилмена, позволяющем строить асимптотически хорошие семейства квантовых LDPC кодов на основе первых групп гомологий некоторого двумерного цепного комплекса, что доказывает qLDPC гипотезу. Более того, будет продемонстрировано как рассматривая вторые группы гомологий полученных цепных комплексов можно доказать существование классических локально тестируемых кодов с оптимальными асимптотическими параметрами, что в свою очередь решает другую важную открытую проблему, называемую s^3 -гипотезой, ответ на которую также недавно независимо был получен в работе arXiv: 2111.04808.

В выступлении предполагается дать обзор конструкции и показать некоторые основные идеи, используемые в доказательстве, такие как понятие локальной минимальности, заимствованное из теории многомерных расширителей. Доклад основан на работе arXiv: 2111.03654.

9 марта 2022 года

Предикаты k -значной логики и задача удовлетворения ограничениям

с.н.с. Жук Д. Н.

В 1969 году была открыта удивительная связь между функциями и предикатами, а именно, было построено взаимно-однозначное соответствие между замкнутыми классами функций и замкнутыми классами предикатов. Несмотря на этот результат, многие годы именно функции были главным объектом исследований, а предикаты (отношения) оставались вспомогательным инструментом для описания предполных и замкнутых классов.

В докладе будет представлен обзор результатов, полученных с помощью подхода, в котором основным объектом являются предикаты, а функции играют лишь вспомогательную роль.

23 марта 2022 года

Оценки энергопотребления объёмных схем

м.н.с. Ефимов А. А.

Ещё в середине XX века в связи с интенсивным развитием вычислительной техники возникла задача синтеза схем, вычисляющих булевы функции и операторы. Одной из основных и наиболее подробно исследованных моделей схем является схема из функциональных элементов (СФЭ). В качестве характеристики оптимальности СФЭ можно рассматривать сложность — количество функциональных элементов, содержащихся в схеме. Таким образом, под сложностью булевой функции или оператора будем понимать минимальную сложность схемы, реализующую данную функцию или оператор.

Отметим, что в модели СФЭ не учитываются вполне естественные ограничения на размещение элементов схемы в плоскости или пространстве, способы их соединения, разводка проводов и т.п. В действительности, любая схема состоит из отдельных элементарных частей (функциональных элементов), которые имеют определенную длину, ширину и соединяются проводниками, размеры которых следует учитывать при оценке сложности реальных устройств.

В докладе рассматриваются объёмные схемы, являющиеся укладкой схем функциональных элементов в пространстве. Был рассмотрен класс объёмных схем, реализующих булевы операторы. Для этого класса получены верхняя и нижняя оценка потенциала — меры мощности, равной

количеству элементов схемы, выдающих единицу на данном входном наборе. Получен порядок функции Шеннона потенциала для класса всюду определенных операторов для объёмных схем без ограничений и схем с близкими выходами, а также нижняя оценка для частичных операторов.

30 марта 2022 года

Алгоритм, практически максимизирующий точность k -классификации на множестве представителей k классов эквивалентности

доц. Бернадотт А. К.

Идея данной работы родилась при решении задачи выбора словаря для разработки неинвазивного интерфейса мозг-компьютер с манипулятором для людей с ограниченными возможностями. При разработке устройства возникла необходимость подобрать словарь из слов-синонимов, объединенных в k классов эквивалентности по семантической близости. Задача состояла в том, чтобы найти такое множество представителей k классов эквивалентности, на котором k -точность классификации классификатором K удовлетворяет определенным критериям: (1) максимальная точность классификации, (2) максимальная точность — точность классификации каждой пары распределений слов не ниже определенного значения. Идея заключалась в том, чтобы представить слова (множества), сгруппированные в k классов эквивалентности, в виде k -дольного взвешенного графа G и найти k -дольную клику, удовлетворяющую определенным критериям. Предложенный Алгоритм 1 позволял получить k -дольные клики с максимальной точностью классификации наихудшего случая; Алгоритм 2 обеспечивал k -дольные клики с максимальным суммарным весом. Задача поиска максимальной клики относится к классу NP-трудных. Однако представленные алгоритмы позволяют выбрать набор представителей оптимально с точки зрения практической максимизации точности классификации и времени выполнения. Алгоритмы увеличивают скорость подбора представителей на 5 порядков по сравнению с алгоритмом полного перебора с небольшой потерей точности.

13 апреля 2022 года

Вопросы выразимости в классах кусочно-линейных функций

инженер Кан А. Н.

Кусочно-линейные функции используются при проектировании искусственных нейронных сетей, к ним относятся суперпозиции из линейных функций и ReLU. Работа продолжает исследования В. С. Половникова по выразимости через суперпозиции в классах кусочно-линейных функций, содержащих линейные функции. При этом ограничении для класса кусочно-линейных функций найдены предполные классы. Одним из них является класс согласованных функций, который содержит единственный предполный подкласс, включающий линейные функции. Показано, что любая кусочно-линейная непрерывная функция двух переменных выражается через линейные функции и ReLU. Построена решетка одноместных следов замкнутых классов кусочно-линейных функций с рассматриваемым ограничением.

18 мая 2022 года

Асимптотика числа пороговых функций и асимптотика числа вырожденных ± 1 -матриц

доц. Ирматов А. А.

В докладе будет рассказано о решении двух, ставших уже классическими, проблем дискретной математики, математической кибернетики и комбинаторики. Одной из этих проблем является нахождение асимптотики числа пороговых функций, которая в статье А.Д.Коршунова (см. А.Д.Коршунов, УМН, 2009, Т.64, В.5(389)) включена в список важных нерешенных проблем дискретной математики и математической кибернетики. В 19 веке L. Schläfli в эквивалентных терминах получил (около 1850 г.) верхнюю оценку для числа пороговых функций $P(2, n)$:

$$P(2, n) \leq 2 \sum_{i=0}^n \binom{2^n - 1}{i}.$$

С конца 50-х годов прошлого века вопрос о нахождении числа пороговых функций стал одним из центральных вопросов пороговой логики. В ряде статей были получены нижние оценки для $P(2, n)$, близкие по порядку логарифма к верхней оценке L. Schläfli. Наилучшая нижняя оценка в этой серии работ была получена автором в 1993 году:

$$P(2, n) \geq 2^{n^2(1-\frac{7}{\ln n})} \cdot P\left(2, \left\lceil \frac{7(n-1)}{\log_2(n-1)} \right\rceil\right).$$

Проблема о распределении значений детерминанта ± 1 -матрицы интенсивно изучается с 30-х годов 20-го века (см. А.М. Odlyzko, Journal of Comb.Theory, Ser.A 47, 124-133 (1988)). В 1963 году Komlós J. (опубликовано в 1967 году) доказал, что вероятность вырожденности случайной Бернуллиевой 0,1-матрицы M_n с ростом размерности стремится к нулю, что верно и для ± 1 -матриц:

$$\mathbb{P}_n \stackrel{def}{=} \Pr(\det M_n = 0) = o_n(1).$$

В 1977 году он улучшил свой результат до верхней оценки

$$\mathbb{P}_n < O\left(\frac{1}{\sqrt{n}}\right).$$

В 1995 году Kahn J., Komlós J. и Szemerédi E. добились экспоненциального убывания верхней оценки: $(0.999 + o_n(1))^n$. В 2007 году Tao T. и Vu V. получили оценку $\left(\frac{3}{4} + o_n(1)\right)^n$, а в 2009 году Bourgain J., Vu V. H. и Wood P. M. улучшили ее до $\left(\frac{\sqrt{2}}{2} + o_n(1)\right)^n$. В 2018 году К. Тихомировым было показано, что

$$\mathbb{P}_n = \left(\frac{1}{2} + o_n(1)\right)^n.$$

В докладе будет исследовано представление числа пороговых функций в комбинаторно-топологических терминах, вытекающего из работ L. Schläfli, Zaslavsky T., Hall P. и Folkman J., и показана связь числа $P(2, n)$ с числом вырожденных ± 1 -матриц, позволяющая установить следующие асимптотики.

Теорема 1. *Асимптотика вероятности \mathbb{P}_n равна:*

$$\mathbb{P}_n \sim (n-1)^2 2^{1-n}, n \rightarrow \infty.$$

Теорема 2. *Асимптотика числа пороговых функций равна:*

$$P(2, n) \sim 2 \binom{2^n - 1}{n}, n \rightarrow \infty.$$

Полное изложение результатов можно найти по адресу <https://arxiv.org/pdf/2004.03400v3.pdf>

14 сентября 2022 года

Параметро-эффективная расшифровка булевых функций

м.н.с. Быстрыгова А. В.

Расшифровка функций (learning theory) — направление математики, которое началось развиваться практически полвека назад. Эта область остается актуальной и по сей день, поскольку связана с восстановлением оптимальным образом информации об исследуемом объекте на основе частичных сведений о нем. Более формально, под расшифровкой функции из заданного класса F понимают игру между “учеником” и “учителем”, в которой учитель загадывает одну функцию из класса F , а ученик, зная этот класс F полностью, но не зная выбор учителя, задает учителю запросы разрешенного типа, получает ответы от учителя и на основе этих ответов восстанавливает какую-то информацию про выбранную функцию.

Чтобы оценить, насколько быстро можно расшифровать функции из того или иного класса, вводят понятие сложности расшифровки как максимальное число запросов, которое ученик должен задать учителю для расшифровки самой “плохой” функции. Иными словами, ученик выбирает “лучшую” стратегию восстановления функции. Затем проверяется, сколько запросов потребуется задать ученику, использующему эту стратегию, чтобы восстановить каждую функцию из класса. За сложность расшифровки принимают максимум среди этих значений.

В докладе будут представлены результаты сложности расшифровки булевых функций ограниченного веса для четырех типов запросов (запросы на значение, запросы на сравнение, запросы на ограниченную и расширенную эквивалентность), а также оценки сложности расшифровки всех замкнутых классов решетки Поста для двух типов запросов (запросы на значение, запросы на сравнение).

19 октября 2022 года

Булевы биюнктивные функции и порождаемые ими системы булевых уравнений

доц. Тарасов А. В.

Доклад посвящен результатам из области исследования булевых биюнктивных функций. Класс биюнктивных функций (функций, представимых в виде 2-КНФ) является одним из классов Шефера, порождающих полиномиально решаемые системы булевых уравнений.

Ряд задач, связанных с этими функциями, является труднорешаемыми. К таковым относится, в частности, задача нахождения веса функции по её 2-КНФ, известная как задача #2-SAT. Вместе с тем, 2-КНФ, представляющие бионктивные функции, допускают компактное представление в виде ориентированных графов. В докладе обсуждаются методы эффективного оценивания веса бионктивных функций. Данная задача фактически эквивалентна задаче оценки числа решений булевой двучленной системы уравнений.

Поскольку класс бионктивных функций относится к классам Шефера, в докладе обсуждаются вопросы связи класса бионктивных функций с другими классами Шефера. Центральным результатом здесь является описание групп преобразований n -мерного векторного пространства, стабилизирующих множество бионктивных функций от n переменных и ряд его подмножеств.

Третья часть доклада посвящена изучению параметров метода максимального правдоподобия для решения систем булевых уравнений, порожденных дважды бионктивными функциями, то есть такими бионктивными функциями, отрицание которых также является бионктивной функцией.

26 октября 2022 года

Цифровая подпись на основе кодов, определяющих изображения с точностью до аффинных преобразований

проф. Козлов В. Н.

Первый “допотопный” вариант защиты документа от подделки (используется, однако, и поныне) — это так называемая “живая” подпись (или факсимиле), и канцелярская печать. Но в наши дни документооборот большей частью электронный, и, зачастую, с очень большим числом документов (электронные торги, банковские платежные системы, сделки в криптовалютах, и пр.). Факсимиле в этом случае неудобно, а главное — крайне ненадежно. Здесь работает возникшая около тридцати лет назад цифровая подпись (или электронная цифровая подпись — ЭЦП). Как правило, сердцевиной этой конструкции, т.е. ЭЦП, является функция, у которой ее значение при заданном значении аргумента, вычисляется легко, а обратное, т.е. вычисление значения аргумента при известном значении функции, очень трудно. В докладе описывается аналог цифровой подписи на другой принципиальной основе — на использовании кодов, определяющих изображения с точностью до аффинных преобразований. Это способ защиты электронного изображения от подделки и проверки

подлинности полученной информации. Способ предназначен для работы с любыми изображениями (потенциально и с трехмерными), или с информацией, приводимой к изображениям (например, со звуком). В целом способ может быть использован для защиты канала связи между отправителем информации в виде изображения и получателем от попыток третьих сторон отправить получателю информацию под видом информации от отправителя, а также аутентификации полученного изображения или информации, приводимой к виду изображения.

9 ноября 2022 года

Об укладках схем из функциональных элементов на плоскости и в пространстве

м.н.с. Калачев Г. В.

В докладе будет рассказано о различных моделях схем, учитывающих ограничения на размещение элементов на плоскости или в пространстве. Первая часть доклада будет посвящена обзору различных результатов о сложности реализации булевых функций (и операторов) клеточными схемами, известные асимптотические оценки для клеточных схем. Во второй части доклада будет кратко рассказано о связи сложности клеточных схем со сложностью в других схожих моделях, таких как планарные схемы, клеточные схемы ограниченной ширины, трехмерные клеточные схемы, многослойные схемы. Рассматривается функция сложности преобразования схемы из одной модели в другую, и в терминах этой функции формулируются результаты о связи сложности в различных моделях. В связи с этим естественным образом возникает класс задач, где для данной пары моделей нужно оценить функцию сложности преобразования из одной модели в другую. Несмотря на то, что иногда эта функция оценивается с использованием уже известных результатов, для многих пар моделей вопрос остаётся открытым.

16 ноября 2022 года

Активность в различных моделях схем

м.н.с. Калачев Г. В.

В докладе речь пойдёт о различных мерах активности для схем из функциональных элементов и клеточных схем. Различные меры сложности схем моделируют различные характеристики чипов. Например, сложность схемы отражает площадь чипа, глубина схемы отражает задержку сигнала на выходе, что в свою очередь определяет тактовую частоту устройства. Активность (также называемая мощностью) схемы

- мера сложности, отражающая энергопотребление физического устройства. Одним из наиболее естественных способов определить активность схемы — посчитать максимальное (или среднее) число единиц на выходах элементов, где максимум (или среднее) берётся по всевозможным входным наборам. Это наиболее исследованная мера активности схем, однако есть и другие способы определять активность, о которых будет рассказано в первой части доклада. Также будет дан обзор известных результатов об активности схем из функциональных элементов.

Во второй доклада части речь пойдёт об активности плоских и объёмных клеточных схем. Будут рассказаны результаты о связи мер сложности и активности, а также результаты о поведении функции Шеннона активности плоских и объёмных клеточных схем для класса частичных операторов. На примере класса всех булевых функций от n переменных будут проиллюстрированы несколько основных идей, используемых в доказательствах этих результатов.

23, 30 ноября 2022 года

О проблеме выполнимости булевых формул

доц. Боков Г. В.

Доклад посвящен проблеме выполнимости булевых формул и подходам к ее решению. Будет рассказано о различных моделях формальных систем, представляющих как общий, так и частные случаи проблемы выполнимости. В докладе рассматриваются ограничения на класс допустимых формул и перечень используемых тактик. Будет представлен сравнительный обзор известных результатов по этой теме.

7 декабря 2022 года

Тензорные сети для эффективной симуляции квантовых вычислений

н.с. Пантелеев П. А.

Тензорные сети являются важным инструментом, позволяющим в некоторых частных случаях значительно понижать сложность задач, для которых в общем случае не имеется эффективного алгоритма решения. Одним из многочисленных примеров подобных задач является задача симуляции квантовых схем маленькой глубины на классическом компьютере. В докладе предполагается рассказать об эффективных методах симуляции на основе тензорных сетей, а также о применении данных методов к случайным схемам, возникающим в экспериментах по демонстрации квантового превосходства.

14 декабря 2022 года

A -предпредполные классы в классе линейных автоматов

доц. Часовских А. А., асп. Бирюкова В. А.

В. А. Буевич ввел понятие аппроксимационного замыкания (A -замыкания) в классе конечных автоматов над двухэлементной логикой $P_{0,d}^2$, что, по сравнению с замыканием по операциям композиции (K -замыкания), позволило увеличивать выразительные возможности его подмножеств. Вячеслав Александрович показал, что мощность множества A -предполных классов в $P_{0,d}^2$ счетна, а не континуальна, как для оператора K -замыкания (В. Б. Кудрявцев). Несмотря на это, задача проверки A -полноты конечных подмножеств конечных автоматов, как и в случае K -замыкания, осталась алгоритмически неразрешимой (М. И. Кратко).

Для подкласса $L_{0,d}^2$ класса $P_{0,d}^2$, состоящего из линейных автоматов, количество K -предполных классов счетно, количество A -предполных классов конечно, задачи проверки K -полноты и A -полноты конечных подмножеств алгоритмически разрешимы. Эти же утверждения справедливы для классов линейных автоматов над конечными полями.

Доклад посвящен изучению A -предполных классов в $L_{0,d}^2$. Для них построены A -базисы, найдены все их A -предполные подклассы. Таким образом, в решетке A -замкнутых классов $L_{0,d}^2$ определены два слоя максимальных собственных подклассов. Несмотря на континуальность A -замкнутых подклассов в классе $L_{0,d}^2$, количество A -предполных и A -предпредполных классов в нем конечно, что располагает к дальнейшим исследованиям задачи A -выразимости в $L_{0,d}^2$.

Доклады семинара «Вопросы сложности алгоритмов поиска»

В 2022 году на научном семинаре «Вопросы сложности алгоритмов поиска» под руководством профессора Эльяра Эльдаровича Гасанова состоялось 8 докладов.

7 сентября 2022 года

Параметро-эффективная расшифровка булевых функций

м.н.с. Быстрыгова А. В.

В докладе представлены результаты сложности расшифровки булевых функций ограниченного веса для четырех типов запросов (запросы на значение, запросы на сравнение, запросы на ограниченную и расширенную эквивалентность), а также оценки сложности расшифровки всех замкнутых классов решетки Поста для двух типов запросов (запросы на значение, запросы на сравнение).

14 сентября 2022 года

Число состояний клеточного автомата, реализующего двунаправленное движение на луче со скоростью движения вперёд $1/3$

м.н.с. Кузнецова Е. В.

В докладе рассматривается движение точки на экране, который реализован, как клеточный автомат на бесконечной в правую сторону полосе шириной в одну клетку. Изучается класс S законов движения этого автомата, для которых движение вперёд возможно со скоростью, не большей, чем $1/3$. Движение вперёд на одну клетку осуществляется с двумя остановками. Возможно движение назад со скоростью 1, также точка может стоять на месте произвольное количество тактов.

Определён класс клеточных автоматов — толкатели. Ранее в классе толкателей реализованы законы движения со скоростью движения вперёд $1/4$ и скоростью движения назад $1/2$, а так же законы движения со

скоростью движения вперёд $1/3$, скоростью движения назад 1 и чётным количеством остановок.

В данной работе доказано, что в классе толкателей невозможно построить клеточный автомат с количеством состояний, меньшим пяти, реализующий законы движения из рассматриваемого класса S . Результат получен для случая, когда до появления точки на экране все клетки находятся в состоянии покоя.

19 октября 2022 года

Верхняя оценка переключательной мощности плоских схем, реализующих один класс автоматов

м.н.с. Воротников А. С.

Плоские схемы (или схемы из клеточных элементов) - это в некотором смысле укладка схемы из функциональных элементов на плоскость. Данные объект рассматривали многие авторы, в частности получен порядок потенциала и переключательной мощности для плоской схемы, реализующей булеву функцию от n переменных, составляющий $2^{n/2}$.

В данной работе рассматривается расширенное понятие: плоские автоматные схемы. Это схемы, чей базис клеточных элементов составляют, помимо привычных булевых функций с не более чем четырьмя входами и выходами, задержки — автоматы с одним состоянием, подающие на выход в следующий такт то, что пришло на вход в предыдущий. Корректные схемы теперь в каждом ориентированном цикле должны содержать не менее одной задержки. Функционирует данная конструкция как структурный автомат.

В работе показано, что некоторый класс автоматов можно реализовать плоскими автоматными схемами со средней переключательной мощностью на такт не более чем $2^{n/2} / \log_2 n$. Приводится схема с обозначенными параметрами.

9 ноября 2022 года

Распознавание автоматом свойства графа быть графом-кактусом

асп. Демидова А. А.

Графом-кактусом является такой связный граф, в котором любое ребро принадлежит не более чем одному циклу (и любые два цикла могут иметь не более одной общей вершины). В работе рассматриваются автоматы, осуществляющие обход связных плоских простых неориентированных графов с целью определения того, являются ли эти графы графами-кактусами. Автомату доступно некоторое количество стираемых красок, которые он наносит на рёбра в течение обхода графа. Во время обхода автомат обладает частичной информацией о вершинах, которые он посещает, и инцидентных им рёбрах. В частности, в любой момент времени автомату известно, красил ли он только что некоторое ребро, благодаря чему он может обнаруживать циклы в графе. В работе исследуется возможность автоматов с 3 стираемыми красками оставлять на рёбрах такие метки, которые помогли бы установить, является ли граф кактусом или нет.

16 ноября 2022 года

Вопросы выразимости в классах кусочно-линейных функций

доц. Миронов А. М.

В докладе представлены новая математическая модель криптографических протоколов и примеры применения этой модели для решения задач верификации криптографических протоколов. Криптографические протоколы — это распределенные алгоритмы, предназначенные для обеспечения передачи конфиденциальной информации в небезопасной среде. Они используются, например, в электронных платежах, электронных процедурах голосования, системах доступа к конфиденциальным данным, и т.д. Ошибки в криптографических протоколах могут привести к большому ущербу, поэтому необходимо использовать математические методы для обоснования различных свойств корректности и безопасности криптографических протоколов. В докладе изложены новые методы формальной верификации криптографических протоколов.

23 ноября 2022 года

Реализация сложения чисел клеточными автоматами и клеточными автоматами с локаторами

проф. Гасанов Э. Э.

Было рассказано, как можно реализовать сложение натуральных чисел клеточными автоматами и клеточными автоматами с локаторами в одномерном и двумерном случаях.

30 ноября 2022 года

Нижняя оценка сложности расшифровки булевых функций веса 3 запросами на сравнение

м.н.с. Быстрыгова А. В.

Рассматривается задача точной расшифровки запросами на сравнение булевых функций веса 3. Два игрока “учитель” и “ученик” играют в следующую игру. В начале игры учитель выбирает любую булеву функцию n -местности n веса 3. Ученик не знает выбор учителя, но знает n . Ученик последовательно задает запросы на сравнение, учитель на них безошибочно отвечает. Запрос на сравнение — упорядоченная пара n -местных наборов, ответ на запрос — разность значений выбранной учителем функции на этих наборах. Цель ученика — понять выбор учителя, задав как можно меньше запросов. В докладе представлено доказательство наилучшей нижней оценки этого количества.

7 декабря 2022 года

Алгоритм достижения консенсуса «Лотерея» и методы борьбы со злоумышленниками

асп. Суюнбекова М. Б.

Рассматривается задача выбора одного игрока среди множества участников в качестве победителя, для решения которой приводится алгоритм “Лотерея”. Определяются классы злоумышленников, которые пытаются сорвать игру на основном этапе алгоритма. Для некоторых из этих классов приводятся протоколы их поимки.

К сведению авторов публикаций в журнале «Интеллектуальные системы. Теория и приложения»

В соответствии с требованиями ВАК РФ к изданиям, входящим в перечень ведущих рецензируемых научных журналов и изданий, в которых могут быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук, статьи в журнал «Интеллектуальные системы. Теория и приложения» предоставляются авторами в следующей форме:

1. Статьи, набранные в пакете \LaTeX , предоставляются к загрузке через WEB-форму http://intsysjournal.org/generator_form.
2. К статье прилагаются файлы, содержащие название статьи на русском и английском языках, аннотацию на русском и английском языках (не более 50 слов), список ключевых слов на русском и английском языках (не более 20 слов), информация об авторах: Ф.И.О. полностью, место работы, должность, ученая степень и/или звание (если имеется), контактные телефоны (с кодом города и страны), e-mail, почтовый адрес с индексом города (домашний или служебный).
3. Список литературы оформляется в едином формате, установленном системой Российского индекса научного цитирования.
4. За публикацию статей в журнале «Интеллектуальные системы. Теория и приложения» с авторов (в том числе аспирантов высших учебных заведений) статей, рекомендованных к публикации, плата не взимается. Оттиски статей авторам не предоставляются. Журнал распространяется по подписке, экземпляры журнала рассылаются подписчикам наложенным платежом. Условия подписки публикуются в каталоге НТИ «Роспечать», индекс журнала 64559.
5. Доступ к электронной версии последнего вышедшего номера осуществляется через НЭБ «Российский индекс научного цитирования». Номера, вышедшие ранее, размещаются на сайте <http://intsysjournal.org>, и доступ к ним бесплатный. Там же будут размещены аннотации всех публикуемых статей.

Подписано в печать: 13.03.2023

Дата выхода: 27.03.2023

Тираж: 200 экз.

Цена свободная

Свидетельство о регистрации СМИ: ПИ № ФС77–58444 от 25 июня 2014 г.,
выдано Федеральной службой по надзору в сфере связи, информационных
технологий и массовых коммуникаций(Роскомнадзор).