Расширение произведения LDPC кодов

Г. В. Калачев*

Мы изучаем свойство расширения произведения кодов LDPC. Известно, что произведение двух экспандерных кодов LDPC является робастно тестируемым (robustly testable), что в двумерном случае эквивалентно расширению произведения. В данной работе показано, что расширение произведения любого числа LDPC кодов на основе вершинных экспандеров ограничено снизу положительной константой. При подходящем выборе параметров случайные LDPC коды с высокой вероятностью экспандерные, поэтому результат покрывает широкий класс кодов. Ранее для трёх и более двоичных кодов свойство расширения произведения было известно только для локально тестируемых кодов и некоторых их подкодов.

Ключевые слова: тензорное произведение кодов, LDPC коды, экспандерные коды, расширение произведения.

1. Введение

Понятие расширения произведения кодов в таком виде, как мы его будем рассматривать, было введено в [1]. В последние годы оно активно изучалось в связи с построением хороших локально тестируемых и квантовых кодов. Для двух кодов с линейным минимальным расстоянием оно совпадает со свойствами робастной тестируемости и тестируемости на согласованность, а при $m \geqslant 3$ строго сильнее [2]. В общем случае это переформулировка когранічного расширения коцепного комплекса, связанного с тензорным произведением кодов [1, Appendix B].

Для двух экспандерных кодов это свойство следует из [3]. Для $m \geqslant 3$ кодов основные известные на данный момент результаты получены для недвоичных кодов. Исключением являются двоичные локально тестируемые коды (LTC) с линейным расстоянием и некоторые их подкоды, для которых расширение произведения доказано в [4], однако это очень узкий класс кодов. Там же высказана гипотеза о том, что экспандерные LDPC коды также обладают хорошим расширением произведения. В настоящей

* *Калачев Глеб Вячеславович* — канд. физ.-мат. наук, с. н. с. лаборатории проблем теоретической кибернетики мех.-мат. ф-та МГУ, e-mail: gleb.kalachev@yandex.ru, ORCID: 0000-0003-2695-3179.

Kalachev Gleb Vyacheslavovich — Candidate of Physical and Mathematical Sciences, Senior Researcher, Laboratory of Problems of Theoretical Cybernetics, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

работе мы доказываем эту гипотезу, показывая, что произвольное фиксированное число LDPC кодов на основе вершинных экспандеров обладает хорошим расширением произведения.

Приведём определение расширения произведения из [1], где также представлены история и связь с другими формами этого определения. Пусть заданы линейные коды $\mathcal{C}_1, \dots, \mathcal{C}_m \subseteq \mathbb{F}_q^n$. Мы можем определить (*тензорное*) *произведение кодов*

$$\mathcal{C}_1 \otimes \dots \otimes \mathcal{C}_m := \{c \in \mathbb{F}_q^{n^m} \mid \forall i \in [m]\ \forall \ell \in \mathcal{L}_i \colon c|_\ell \in \mathcal{C}_i\},$$

где $\mathbb{F}_q^{n^m}$ — это множество функций $c\colon [n]^m \to \mathbb{F}_q$, а $\mathcal{L}_i$ — множество линий, параллельных i-й оси в m-мерной решётке $[n]^m$, то есть

$$\mathcal{L}_i := \{A_1 \times \dots \times A_m \subseteq [n]^m \mid A_i = [n], \forall j \neq i : |A_j| = 1\}.$$

Здесь и далее мы используем обозначение $[n] := \{1, \dots, n\}$. Также для набора $\mathcal{C} = (\mathcal{C}_i)_{i\in[m]}$ линейных кодов над $\mathbb{F}_q$ нам будет удобно использовать обозначение $\otimes\mathcal{C} := \mathcal{C}_1 \otimes \dots \otimes \mathcal{C}_m$.

Для набора $\mathcal{C} = (\mathcal{C}_i)_{i\in[m]}$ линейных кодов над $\mathbb{F}_q$ определим коды

$$\mathcal{C}^{(i)} := \mathbb{F}_q^n \otimes \dots \otimes \mathcal{C}_i \otimes \dots \otimes \mathbb{F}_q^n = \{c \in \mathbb{F}_q^{n^m} \mid \forall \ell \in \mathcal{L}_i \colon c|_\ell \in \mathcal{C}_i\}.$$

Можно заметить, что в этих обозначениях выполнено

$$\mathcal{C}_1 \otimes \dots \otimes \mathcal{C}_m = \mathcal{C}^{(1)} \cap \dots \cap \mathcal{C}^{(m)}.$$

Определим код

$$\boxplus\mathcal{C} := \mathcal{C}_1 \boxplus \dots \boxplus \mathcal{C}_m := \mathcal{C}^{(1)} + \dots + \mathcal{C}^{(m)}.$$

Нетрудно убедиться, что $\mathcal{C}^{(1)} + \dots + \mathcal{C}^{(m)} = (\mathcal{C}_1^\perp \otimes \dots \otimes \mathcal{C}_m^\perp)^\perp$.

Заметим, что каждый код $\mathcal{C}^{(i)}$ представляет собой прямую сумму $|\mathcal{L}_i| = n^{m-1}$ копий кода $\mathcal{C}_i$. Для $x \in \mathbb{F}_q^{n^m}$ через $|x|$ и $|x|_i$ обозначим соответственно *вес Хэмминга* (то есть количество ненулевых элементов) x и количество линий $\ell \in \mathcal{L}_i$, для которых $x|_\ell \neq 0$. Легко видеть, что введённые нормы связаны неравенством $|x| \leqslant n|x|_i$, $i \in [m]$.

Каждый $x \in \mathcal{C}_1 \boxplus \dots \boxplus \mathcal{C}_m$ может быть представлен несколькими способами как сумма $x = \sum_{i\in[m]} a_i$, где $a_i \in \mathcal{C}^{(i)}$ для всех $i \in [m]$. Введём величину

$$|x|_{\boxplus\mathcal{C}} := \min\Big\{ \sum_{i\in[m]} |a_i|_i \;\Big|\; x = \sum_{i\in[m]} a_i, a_i \in \mathcal{C}^{(i)} \Big\}.$$

Расширением произведения набора кодов $\mathcal{C}$ называется величина

$$\rho(\mathcal{C}) := \frac{1}{n} \min_{x \in \boxplus\mathcal{C}\setminus\{0\}} \frac{|x|}{|x|_{\boxplus\mathcal{C}}},$$

где минимум по пустому множеству считаем равным $+\infty$.

2. Основной результат

Двудольный (δ_L, δ_R)-регулярный граф G с левой долей L назовём (α, ε)-экспандером, если для любого $S \subseteq L$ с $|S| \leqslant \alpha|L|$ выполнено $|N(S)| \geqslant (1-\varepsilon)\delta_L|S|$, где $N(S)$ — множество соседей множества S.

Через $\mathsf{ExpLDPC}(\delta, \alpha, \varepsilon)$ обозначим множество линейных кодов $\mathcal{C}$, которые могут быть представлены как $\mathcal{C} = \ker H$, где H — матрица смежности (δ, δ_R)-регулярного (α, ε)-экспандера для некоторого $\delta_R \in \mathbb{N}$. При $\varepsilon < 1/2$ относительное минимальное расстояние такого кода больше α.

Теорема 1. *Для любых $m, \delta \in \mathbb{N}$, $R_1, \ldots, R_m \in (0,1)$, $\alpha > 0$ и $\varepsilon \in [0, 1/16]$ существует $\rho_0 > 0$, зависящее только от m, α и $\Delta := \lfloor \delta/(1 - \max_i R_i) \rfloor$, такое, что для любого $n \in \mathbb{N}$ и любых кодов $\mathcal{C}_i \in \mathsf{ExpLDPC}(\delta, \alpha, \varepsilon)$ длины n и скорости $\leqslant R_i$, $i \in [m]$, выполнено*

$$\rho(\mathcal{C}_1, \ldots, \mathcal{C}_m) \geqslant \rho_0.$$

Замечание 1. В доказательстве регулярность справа и ограничение на скорость кодов нужны лишь для оценки правых степеней d_i: $d_i \leqslant \lfloor \delta/(1 - R_i) \rfloor \leqslant \Delta$.

Код доказательства теоремы 1 в системе Lean 4 доступен в репозитории: `https://github.com/KalachevGleb/ldpc-prodexp-lean/tree/v1.0`.

Об использовании инструментов ИИ

При работе над доказательством использовалась модель Claude Opus 5.5 в среде Claude Code. С её помощью идеи автора были формализованы и доведены до строгого доказательства теоремы 1 и написан программный код для формальной верификации доказательства в системе Lean 4. Автор несёт полную ответственность за содержание статьи.

Список литературы

[1] G. Kalachev, P. Panteleev, “Two-Sided Robustly Testable Codes”, arXiv: 2206.09973.

[2] Г. В. Калачев, “Многомерное расширение произведений кодов сильнее робастной тестируемости и тестируемости на согласованность”, *Интеллектуальные системы. Теория и приложения*, **30**:2 (2026), 101–119.

[3] I. Dinur, M. Sudan, A. Wigderson, “Robust local testability of tensor products of LDPC codes”, *APPROX-RANDOM 2006, Lecture Notes in Computer Science, vol. 4110*, Springer, 2006, 304–315.

[4] G. Kalachev, P. Panteleev, “Maximally Extendable Product Codes are Good Coboundary Expanders”, *2025 IEEE 66th Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE, Sydney, Australia, 2025, 1512–1524. DOI: 10.1109/FOCS63196.2025.00079.

Статья поступила 18 октября 2026 г.

Product Expansion of LDPC Codes

G. V. Kalachev

We study the product expansion property of LDPC codes. It is known that the product of two expander LDPC codes is robustly testable, which in the two-dimensional case is equivalent to product expansion. In this work, we show that the product expansion of any number of expander LDPC codes is bounded below by a positive constant. Since random LDPC codes with certain parameters are expander codes with high probability, our result covers a wide class of codes. Previously, for three or more binary codes, product expansion was known only for locally testable codes and some of their subcodes.

Keywords: tensor product of codes, LDPC codes, expander codes, product expansion.

References

[1] G. Kalachev, P. Panteleev, “Two-Sided Robustly Testable Codes”, arXiv: 2206.09973.

[2] G. Kalachev, “High-dimensional expansion of product codes is stronger than robust and agreement testability”, *Intelligent Systems. Theory and Applications*, **30**:2 (2026), 101–119.

[3] I. Dinur, M. Sudan, A. Wigderson, “Robust local testability of tensor products of LDPC codes”, *APPROX-RANDOM 2006, Lecture Notes in Computer Science, vol. 4110*, Springer, 2006, 304–315.

[4] G. Kalachev, P. Panteleev, “Maximally Extendable Product Codes are Good Coboundary Expanders”, *2025 IEEE 66th Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE, Sydney, Australia, 2025, 1512–1524. DOI: 10.1109/FOCS63196.2025.00079.

Received on October 18, 2026