Об асимптотических хороших семействах классических и квантовых LDPC кодов

Пантелеев П. А.[2], Калачев Г. В.[1]

В работе показывается существование асимптотически хорошего семейства квантовых низкоплотностных кодов, что доказывает qLDPC гипотезу. Также показано существование асимптотически хорошего семейства локально тестируемых кодов с константными параметрами локальности и корректности, что также является положительным решением известной гипотезы в области классических локально тестируемых кодов.

Ключевые слова: локально тестируемы коды, квантовые LDPC коды, асимптотически хорошие коды.

1. Введение

Обозначим через $\mathbb{F}_q$ конечное поле из q элементов. *Классическим линейным* $[n, k, d]_q$ *кодом над* $\mathbb{F}_q$ называют произвольное k-мерное векторное пространство $\mathcal{C} \subseteq \mathbb{F}_q^n$ такое, что $d = \min_{c \in \mathcal{C} \setminus \{0\}} |c|$, где $|c|$ — *вес Хемминга* вектора $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$, т.е. число его ненулевых компонент c_i, $1 \leq i \leq n$. Параметры n, k и d называются соответственно *длинной*, *размерностью* и *минимальным расстоянием* кода $\mathcal{C}$.

Обычно линейный код задается как множество решений однородной системы уравнений $\mathcal{C}(H) := \{c \in \mathbb{F}_q^n \mid Hc = 0\}$, а соответствующая матрица $H \in \mathbb{F}_q^{r \times n}$ называется его *проверочной матрицей*. Бесконечное семейство $\{\mathcal{C}^{(i)}\}_{i \in \mathbb{N}}$ классических линейных кодов над $\mathbb{F}_q$ называется семейством *низкоплотностных кодов* или семейством *LDPC кодов* (англ. Low-Density Parity-Check code) [1], если существует задающее их семейство проверочных матриц $\{H^{(i)}\}_{i \in \mathbb{N}}$, т.е. $\mathcal{C}^{(i)} = \mathcal{C}(H^{(i)})$, такое, что число ненулевых элементов в $H_i \in \mathbb{F}_q^{r_i \times n_i}$ растет как $\Theta(n_i)$ при $i \to \infty$. Часто последнее требование заменяется более сильным требованием, что существует универсальная константа w такая, что все строки и столбцы

[2] *Пантелеев Павел Анатольевич* — к.ф.-м.н., н.с. каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: panpavel@yandex.ru.

Panteleev Pavel Anatolyevich — Candidate of Physical and Mathematical Sciences, Researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

[1] *Калачев Глеб Вячеславович* — к.ф.-м.н., м.н.с. лаборатории проблем теоретической кибернетики мех.-мат. ф-та МГУ, e-mail: gleb.kalachev@yandex.ru.

Kalachev Gleb Vyacheslavovich — Candidate of Physical and Mathematical Sciences, Junior Researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Problems of Theorecical Cybernetics Lab.

матриц из $\{H^{(i)}\}_{i\in\mathbb{N}}$ ограничены сверху числом w. В этом случае семейство LDPC кодов $\{\mathcal{C}^{(i)}\}_{i\in\mathbb{N}}$ называется *w-ограниченным*. Везде далее семейство LDPC кодов понимается именно в этом более узком смысле.

Классический код называется (w,s)-*локально тестируемым кодом* если его можно задать проверочной матрицей $H\in\mathbb{F}_q^{r\times n}$, у которой вес всех строк ограничен w, и для любого вектора $x\in\mathbb{F}_q$ мы получаем

$$\frac{1}{r}|Hx|\geqslant\frac{s}{n}d(x,\mathcal{C}),$$

где $d(x,\mathcal{C}):=\min_{c\in\mathcal{C}}|x-c|$ — *расстояние* от x до кода $\mathcal{C}$. Параметры w и s называются соответственно *локальностью* (англ. locality) и *корректностью* (англ. soundness) проверочной матрицы H. Локально тестируемые коды тесно связаны с вероятностно проверяемыми доказательствами и знаменитой PCP-теоремой, и имеют большое значение для современной теории сложности вычислений [3].

Квантовые коды были введены П. Шором [4] с целью создания устойчивых к ошибкам квантовых компьютеров. Одним из наиболее распространенных классов таких кодов являются коды Кальдербанка-Шора-Стина (CSS коды) [5, 6]. Напомним, что квантовый CSS код $\mathcal{Q}$ с параметрами $[[n,k,d]]_q$ определяется парой классических кодов $\mathcal{C}_X,\mathcal{C}_Z\subseteq\mathbb{F}_q^n$ таких, что $\mathcal{C}_Z^\perp\subseteq\mathcal{C}_X$ и $k=\dim\mathcal{C}_X+\dim\mathcal{C}_Z-n$, где $\mathcal{C}_Z^\perp$ — двойственный код к $\mathcal{C}_Z$, т.е его ортогональное дополнение относительно стандартного скалярного произведения $\langle x,y\rangle:=x_1y_1+\ldots+x_ny_y$ в $\mathbb{F}_q^n$. Параметры n, k и d, как и в случае классических кодов, называются соответственно *длиной*, *размерностью* и *минимальным расстоянием* квантового CSS кода. При этом минимальное расстояние d определено как $d:=\min(d_X,d_Z)$, где d_X и d_Z равны минимальному весу Хемминга векторов из $\mathcal{C}_X\setminus\mathcal{C}_Z^\perp$ и $\mathcal{C}_Z\setminus\mathcal{C}_X^\perp$ соответственно. Бесконечное семейство квантовых CSS кодов, заданных парами классических кодов $\{(\mathcal{C}_X^{(i)},\mathcal{C}_Z^{(i)})\}_{i\in\mathbb{N}}$, называется семейством *квантовых LDPC кодов* если $\{\mathcal{C}_X^{(i)}\}_{i\in\mathbb{N}}$ и $\{\mathcal{C}_Z^{(i)}\}_{i\in\mathbb{N}}$ являются семействами классических LDPC кодов.

Часто, в особенности когда $n\to\infty$, бывает полезно также рассматривать величины k/n и d/n называемые *скоростью* и *относительным минимальным расстоянием* кода (классического или квантового). Бесконечное семейство кодов (классических или квантовых) называется *асимптотически хорошим* если существует такая константа $\varepsilon>0$, что скорость и относительное минимальное расстояние любого кода из этого семейства ограничены снизу величиной ε. Известно [1], что существуют конструкции асимптотически хороших LDPC кодов, причем даже с линейной сложностью декодирования [2]. Однако вопрос о существовании асимптотически хороших семейств классических локально тестируемых

и квантовых LDPC кодов оставался открытым достаточно долгое время. В настоящей работе мы показываем существование данных семейств.

Теорема 1. *Для каждого числа $R \in (0, 1/2)$ и конечного поля $\mathbb{F}_q$ можно найти константы s and w такие, что существует семейство (w, s)-локально тестируемых классических линейных кодов с параметрами $[n, k \geqslant Rn, d = \Theta(n)]_q$ при $n \to \infty$.*

Теорема 2. *Для каждого числа $R \in (0, 1)$ и конечного поля $\mathbb{F}_q$ существует семейство квантовых LDPC кодов с параметрами $[[n, k \geqslant Rn, d = \Theta(n)]]_q$ при $n \to \infty$.*

Замечание. Полная версия данной работы с доказательствами Теорем 1 и 2 может быть найдена в [7]. Отметим также, что чуть более сильная версия Теоремы 1 для случая поля $\mathbb{F}_2$ была также недавно независимо показана в [8].

Список литературы

[1] R. Gallager, "Low-density parity-check codes", *IRE Transactions on Information Theory*, **8**:1 (1962), 21–28.

[2] M. Sipser, D.A. Spielman, "Expander codes", *IEEE Transactions on Information Theory*, **42**:6 (1996), 1710–1722.

[3] Oded Goldreich, *Short Locally Testable Codes and Proofs: A Survey in Two Parts*, Lecture Notes in Computer Science, ed. Oded Goldreich, Springer, Berlin, Heidelberg, 2010, 65–104.

[4] P. Shor, "Scheme for reducing decoherence in quantum computer memory", *Phys. Rev. A*, **52**:4 (1995), R2493–R2496.

[5] A. R. Calderbank, P. Shor, "Good quantum error-correcting codes exist", *Phys. Rev. A*, **54**:2 (1996), 1098–1105.

[6] A. M. Steane, "Error Correcting Codes in Quantum Theory", *Phys. Rev. Lett.*, **77**:5 (1996), 793–797.

[7] Pavel Panteleev, Gleb Kalachev, *Asymptotically Good Quantum and Locally Testable Classical LDPC Codes*, arXiv: 2111.03654.

[8] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, Shahar Mozes, *Locally Testable Codes with constant rate, distance, and locality*, arXiv: 2111.04808.

On asymptotically good families of classical and quantum LDPC codes

Panteleev P.A., Kalachev G.V.

In this work it is shown that there exists an asymptotically good family of quantum LDPC codes, which proves the qLDPC conjecture. We also show that there exists an asymptotically good family of classical locally testable codes with constant query and soundness

parameters, which also gives a positive solution of a well-known conjecture in the field of classical locally testable codes.

Keywords: locally testable codes, quantum LDPC codes, asymptotically good codes.

References

[1] R. Gallager, "Low-density parity-check codes", *IRE Transactions on Information Theory*, **8**:1 (1962), 21–28.

[2] M. Sipser, D.A. Spielman, "Expander codes", *IEEE Transactions on Information Theory*, **42**:6 (1996), 1710–1722.

[3] Oded Goldreich, *Short Locally Testable Codes and Proofs: A Survey in Two Parts*, Lecture Notes in Computer Science, ed. Oded Goldreich, Springer, Berlin, Heidelberg, 2010, 65–104.

[4] P. Shor, "Scheme for reducing decoherence in quantum computer memory", *Phys. Rev. A*, **52**:4 (1995), R2493–R2496.

[5] A. R. Calderbank, P. Shor, "Good quantum error-correcting codes exist", *Phys. Rev. A*, **54**:2 (1996), 1098–1105.

[6] A. M. Steane, "Error Correcting Codes in Quantum Theory", *Phys. Rev. Lett.*, **77**:5 (1996), 793–797.

[7] Pavel Panteleev, Gleb Kalachev, *Asymptotically Good Quantum and Locally Testable Classical LDPC Codes*, arXiv: 2111.03654.

[8] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, Shahar Mozes, *Locally Testable Codes with constant rate, distance, and locality*, arXiv: 2111.04808.