О РОБАСТНОЙ ТЕСТИРУЕМОСТИ ПРОИЗВЕДЕНИЯ СЛУЧАЙНЫХ КОДОВ

Г. В. Калачев, П. А. Пантелеев (Москва)

Линейным $[n, k]$ кодом над конечным полем $\mathbb{F}_q$ из q элементов называется произвольное k-мерное подпространство $C \subseteq \mathbb{F}_q^n$. Тензорное произведение линейных кодов $C_1 \subseteq \mathbb{F}_q^{n_1}$ и $C_2 \subseteq \mathbb{F}_q^{n_2}$ можно представлять [1, Глава 18] как пространство $C_1 \otimes C_2 \subseteq \mathbb{F}_q^{n_1} \otimes \mathbb{F}_q^{n_2}$ таких $n_1 \times n_2$ матриц над $\mathbb{F}_q$, у которых любой столбец лежит в C_1 и любая строка лежит в C_2.

Определение. Пусть $C_1 \subseteq \mathbb{F}_q^{n_1}$, $C_2 \subseteq \mathbb{F}_q^{n_2}$ — линейные коды. Тогда произведение $C_1 \otimes C_2$ называется *ρ-робастно тестируемым*, если для любого элемента $x \in \mathbb{F}_q^{n_1} \otimes \mathbb{F}_q^{n_2}$ выполнено неравенство

$$\frac{d(x, C_1 \otimes \mathbb{F}_q^{n_2}) + d(x, \mathbb{F}_q^{n_1} \otimes C_2)}{2d(x, C_1 \otimes C_2)} \geq \rho,$$

где $d(u, C)$ означает минимальное расстояние Хэмминга от вектора u до кода C.

Понятие робастно тестируемых кодов (англ. robustly testable codes) возникло в связи с задачами из теории сложности, где нужно, прочитав константное число случайных бит, проверить некоторое свойство [2]. Одним из примеров является использование робастно тестируемых кодов для построения локально тестируемых кодов (LTC) — кодов, расстояние до которых от любого слова можно оценить, прочитав константное число случайных бит этого слова. Вопрос о существовании асимптотически хороших LTC кодов долгое время оставался открытым, и совмсем недавно в работах [3, 4] были построены примеры таких семейств. В обеих работах в том или ином виде использовалось свойство робастной тестируемости произведения некоторых кодов. В работе [3] использовался результат о том, что произведение случайного LDPC кода на код с большим минимальным расстоянием является робастно тестируемым [5].

В работе [4] была предложена конструкция кодов, которая кроме LTC позволяет также построить семейство асимптотически хороших квантовых LDPC кодов, и для этого требуется свойство робастной тестируемости не только для произведения кодов $C_1 \otimes C_2$, но и для произведения двойственных кодов $C_1^\perp \otimes C_2^\perp$. Ни одна из известных конструкций робастно тестируемых кодов [2, 5, 6] не гарантирует существование пары кодов с таким «двусторонним» свойством. Поэтому в [4] было доказано более слабое свойство, которое

можно интерпретировать, как робастная тестируемость с робастностью $\rho = \Theta(n^{-\varepsilon-1/2})$ для произвольного $\varepsilon > 0$, то есть параметр робастности уменьшается с ростом длины кода. Позднее появилось ещё одно доказательство существования асимптотически хороших квантовых LDPC кодов на основе новой конструкции [7], полученной путем упрощения конструкции из [4], но в нём использовался тот же ослабленный вариант робастно тестируемых кодов. Несмотря на то, что ослабленного свойства оказалось достаточно для доказательства линейного минимального расстояния квантовых кодов, оно вносит существенные технические трудности в доказательство. Кроме того, для имеющихся конструкций асимптотически хороших квантовых LDPC кодов пока не известен эффективный алгоритм декодирования. Трудность в построении такого алгоритма связана и с тем, что используется ослабленная версия робастно тестируемых кодов.

В данной работе показано, что произведение двух случайных кодов с большой вероятностью является робастно тестируемым. Сформулируем этот результат формально. Через $\mathrm{Gr}(n,k)$ обозначим множество k-мерных подпространств n-мерного пространства $\mathbb{F}_q^n$. Когда мы выбираем случайным код $C \in \mathrm{Gr}(n,k)$ будем подразумевать, что на $\mathrm{Gr}(n,k)$ задано равномерное распределение вероятностей.

Теорема. *Пусть $R_1 \in (0,1)$, $R_2 \in (0,1)$. Тогда существует $\rho > 0$ такое, что для случайных $C_1 \in \mathrm{Gr}(n_1,k_1)$, $C_2 \in \mathrm{Gr}(n_2,k_2)$ вероятность, что код $C_1 \otimes C_2$ — ρ-робастно тестируемый, стремится к 1 при $\min(n_1,n_2) \to \infty$, $k_i/n_i \to R_i$.*

Нетрудно убедиться, что если случайный код $C \in \mathrm{Gr}(n,k)$ имеет равномерное распределение, то двойственный код $C^\perp \in \mathrm{Gr}(n,n-k)$ имеет также равномерное распределение. Поэтому, для случайных кодов C_1, C_2 теорему можно применить и к произведению двойственных кодов $C_1^\perp \otimes C_2^\perp$. Таким образом, для почти всех пар кодов (C_1,C_2) со скоростями R_1 и R_2 оба кода $C_1 \otimes C_2$ и $C_1^\perp \otimes C_2^\perp$ являются ρ-робастно тестируемыми для некоторого $\rho = \rho(R_1,R_2) > 0$, не зависящего от длины кода. В [7] показано, что при условии существования такой пары кодов можно улучшить константу в оценке минимального расстояния квантовых кодов Таннера. Кроме того, полученный результат позволит существенно упростить имеющиеся доказательства линейного расстояния квантовых кодов [4, 7], а также, возможно, позволит для таких кодов построить декодер, эффективно исправляющий число ошибок, линейно зависящее от длины кода.

Список литературы

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.

2. Ben-Sasson E., Sudan M. Robust locally testable codes and products of codes // Random Structures & Algorithms. — 2006. — Vol. 28, no. 4. — P. 387–402.

3. Dinur I., Evra S., Livne R., Lubotzky A., Mozes S. Locally Testable Codes with constant rate, distance, and locality // ArXiv e-prints. — 2021. — https://arxiv.org/abs/2111.04808

4. Panteleev P. A., Kalachev G. V. Asymptotically good quantum and locally testable classical ldpc codes // ArXiv e-prints. — 2021. — https://arxiv.org/abs/2111.03654

5. Dinur I., Sudan M., Wigderson A. Robust local testability of tensor products of LDPC codes // Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. — 2006. — P. 304–315.

6. Polishchuk A., Spielman D. Nearly linear size holographic proofs // 26th ACM Symp. on Theory of Computing. — 1994. — P. 194–203.

7. Leverrier A., Zémor G. Quantum Tanner codes // ArXiv e-prints. — 2022. — https://arxiv.org/abs/2202.13641

DOI: 10.20948/dms-2022-84

НОВЫЕ КОНСТРУКЦИИ И НИЖНЯЯ ОЦЕНКА ЧИСЛА САМОДУАЛЬНЫХ БЕНТ-ФУНКЦИЙ

А. В. Куценко (Новосибирск)

В данной работе рассматриваются бент-функции — максимально нелинейные булевы функции от чётного числа переменных. Они представляют большой интерес для теоретических исследований и имеют приложения в ряде областей, включая алгебру, теорию кодирования и криптографию. Данные математические объекты впервые изучались в 60-х годах XX века, понятие *бент-функции* было введено О. Ротхаусом позднее в работе [1]. Известно, что функции,