# Многомерное расширение произведений кодов сильнее робастной тестируемости и тестируемости на согласованность

Г. В. Калачев*

Мы изучаем свойство когранично расширения (coboundary expansion) для произведений кодов, называемое расширением произведения, которое сыграло ключевую роль во многих построениях хороших квантовых LDPC кодов. Ранее было показано, что это свойство эквивалентно робастной тестируемости (robust testability) и тестируемости на согласованность (agreement testability) для произведений двух кодов с линейным расстоянием. Во-первых, мы показываем, что робастная тестируемость по линиям для произведения нескольких кодов с линейным расстоянием эквивалентна тестируемости на согласованность. Во-вторых, мы приводим пример произведения трёх кодов с линейным расстоянием, которое является робастно тестируемым, но не обладает свойством расширения произведения.

**Ключевые слова:** тензорное произведение кодов, кограничное расширение, робастная тестируемость, тестируемость на согласованность.

## 1. Введение

Недавние конструкции асимптотически хороших локально тестируемых кодов (LTC) и квантовых LDPC (qLDPC) кодов [1–7] используют специальное свойство произведений кодов, которое имеет несколько названий и определений: робастная тестируемость (robust testability), тестируемость на согласованность (agreement testability) и расширение произведения (product expansion). Было показано [2, Lemma 2.9], [8, Lemma 1], что эти определения по существу эквивалентны в случае произведения двух кодов. Для всех известных конструкций хороших qLDPC кодов это свойство необходимо для обеспечения линейного расстояния и построения эффективных декодеров. Для LTC существует одно исключение: в работе [9]

* *Калачев Глеб Вячеславович* — канд. физ.-мат. наук, науч. сотр. каф. математической теории интеллектуальных систем 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, Researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

конструкция LTC кодов основывается на односторонних вершинных экспандерах и не требует локальных кодов, удовлетворяющих специальному свойству.

В [8, Appendix B] было показано, что свойство расширения произведения кодов может быть интерпретировано как форма многомерного расширения, называемая когранichным расширением[1] (coboundary expansion). Таким образом, это представляется важным свойством произведений кодов наряду с робастной тестируемостью и тестируемостью на согласованность. Более того, поскольку расширение произведения кодов является формой когранichного расширения, то вероятно, что оно будет полезно для построения многомерных аналогов кодов из [1, 2], которые потенциально могут дать хорошие квантовые локально тестируемые коды (qLTC).

В [8, Lemma 1] также было показано, что расширение произведения двух кодов совпадает с тестируемостью на согласованность с той же константой (см. также [3, Section 2.6]). Цель нашей статьи — прояснить взаимосвязь между робастной тестируемостью, тестируемостью на согласованность и расширением произведения для произведений более чем двух кодов. В частности, мы рассматриваем естественное обобщение тестируемости на согласованность для произведений нескольких кодов и показываем, что в случае произведений 3 и более кодов: 1) расширение произведения отличается от робастной тестируемости и тестируемости на согласованность; 2) тестируемость на согласованность эквивалентна робастной тестируемости для теста по осепараллельным линиям (axis-parallel line test), с точностью до константного множителя.

### 1.1. Расширение произведения кодов

Приведём определение расширения произведения из [8], где также представлены история и связь с другими формами этого определения. Пусть заданы линейные коды $\mathcal{C}_1, \dots, \mathcal{C}_m$ над $\mathbb{F}_q$. Мы можем определить (*тензорное*) *произведение кодов*

$$\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_m := \{c \in \mathbb{F}_q^{n_1 \times \cdots \times n_m} \mid \forall i \in [m]\ \forall \ell \in \mathcal{L}_i \colon c|_\ell \in \mathcal{C}_i\},$$

где $\mathbb{F}_q^{n_1 \times \cdots \times n_m}$ — это множество функций $c\colon [n_1] \times \cdots \times [n_m] \to \mathbb{F}_q$, а $\mathcal{L}_i$ — множество линий, параллельных $i$-й оси в $m$-мерной решётке $[n_1] \times \cdots \times [n_m]$, то есть

$$\mathcal{L}_i := \{A_1 \times \cdots \times A_m \subseteq [n_1] \times \cdots \times [n_m] \mid A_i = [n_i], \forall j \neq i : |A_j| = 1\}.$$

[1] Для двухмерного случая см. также [3, Section 2.6]

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 $\otimes\mathcal{C} := \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_m$.

Как и в [8], для линейных кодов $\mathcal{C}_1 \subseteq \mathbb{F}_q^{n_1}$, $\mathcal{C}_2 \subseteq \mathbb{F}_q^{n_2}$ мы обозначаем $\mathcal{C}_1 \boxplus \mathcal{C}_2$ как код $(\mathcal{C}_1^\perp \otimes \mathcal{C}_2^\perp)^\perp = \mathcal{C}_1 \otimes \mathbb{F}_q^{n_2} + \mathbb{F}_q^{n_1} \otimes \mathcal{C}_2 \subseteq \mathbb{F}_q^{n_1\times n_2}$. Для набора $\mathcal{C} = (\mathcal{C}_i)_{i\in[m]}$ линейных кодов над $\mathbb{F}_q$ мы можем определить коды

$$\mathcal{C}^{(i)} := \mathbb{F}_q^{n_1} \otimes \cdots \otimes \mathcal{C}_i \otimes \cdots \otimes \mathbb{F}_q^{n_m} = \{c \in \mathbb{F}_q^{n_1\times\cdots\times n_m} \mid \forall \ell \in \mathcal{L}_i \colon c|_\ell \in \mathcal{C}_i\}.$$

Легко видеть, что

$$\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_m = \mathcal{C}^{(1)} \cap \cdots \cap \mathcal{C}^{(m)}, \qquad \mathcal{C}_1 \boxplus \cdots \boxplus \mathcal{C}_m = \mathcal{C}^{(1)} + \cdots + \mathcal{C}^{(m)}.$$

Заметим, что каждый код $\mathcal{C}^{(i)}$ представляет собой прямую сумму $|\mathcal{L}_i| = \frac{1}{n_i}\prod_{j\in[m]} n_j$ копий кода $\mathcal{C}_i$. Для $x \in \mathbb{F}_q^{n_1\times\cdots\times n_m}$ обозначим $|x|_i$ и $\|x\|_i$ соответственно как количество и долю линий $\ell \in \mathcal{L}_i$, для которых $x|_\ell \neq 0$. Очевидно, что $\|x\|_i = \frac{1}{|\mathcal{L}_i|}|x|_i$. $|x|$ и $\|x\|$ обозначают соответственно *вес Хэмминга* (то есть количество ненулевых элементов) и *нормализованный вес Хэмминга* (то есть долю ненулевых элементов) в $x$. Легко видеть, что введённые нормы связаны неравенством $\|x\| \leqslant \|x\|_i$, $i \in [m]$. Мы также будем использовать следующие обозначения: нормализованное расстояние $\delta(x, y) := \|x - y\|$, нормализованное расстояние до кода $\delta(x, \mathcal{C}) := \min_{y\in\mathcal{C}} \|x - y\|$ и нормализованное минимальное расстояние $\delta(\mathcal{C}) := \min_{x\in\mathcal{C}\setminus\{0\}} \|x\|$ для кода $\mathcal{C} \subseteq \mathbb{F}_q^n$.

**Определение 1** (Расширение произведения кодов [8])**.** Пусть задан набор $\mathcal{C} = (\mathcal{C}_i)_{i\in[m]}$ линейных кодов $\mathcal{C}_i \subseteq \mathbb{F}_q^{n_i}$. Мы говорим, что $\mathcal{C}$ является *$\rho$-расширяющим*, если каждое кодовое слово $c \in \mathcal{C}_1 \boxplus \cdots \boxplus \mathcal{C}_m$ может быть представлено как сумма $c = \sum_{i\in[m]} a_i$, где $a_i \in \mathcal{C}^{(i)}$ для всех $i \in [m]$ и выполнено следующее неравенство:

$$\rho \sum_{i\in[m]} \|a_i\|_i \leqslant \|c\|. \tag{1}$$

Через $\rho(\mathcal{C})$ обозначим наибольшее значение $\rho$, для которого $\mathcal{C}$ является $\rho$-расширяющим. В [8, Appendix B] было показано, что $\rho(\mathcal{C})$ с точностью до множителя $1/m$ равен константе Чигера цепного комплекса, естественно ассоциированного с произведением кодов $\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_m$.

## 1.2. Робастная тестируемость и тестируемость на согласованность

Пусть $X$ — некоторое конечное индексное множество, которое мы будем использовать для нумерации символов кода. Тогда код $\mathcal{C} \subseteq \mathbb{F}_q^X$ можно

интерпретировать как множество функций $f : X \to \mathbb{F}_q$. Если $I \subseteq X$, то $\mathcal{C}|_I := \{c|_I \mid c \in \mathcal{C}\}$ — это перфорированный код (punctured code) $\mathcal{C}$, состоящий из ограничений кодовых слов из $\mathcal{C}$ на индексное множество $I$.

**Определение 2.** *Тест для кода* $\mathcal{C} \subseteq \mathbb{F}_q^X$ — это множество $T \subseteq 2^X$ с вероятностной мерой $\mathsf{P}$, определённой на нём.

В этой статье мы всегда будем использовать следующую вероятностную меру:

$$\mathsf{P}(I) = \frac{|I|}{\sum_{J \in T} |J|} \quad \text{для} \quad I \in T. \tag{2}$$

Тестер для пары (код $\mathcal{C} \subseteq \mathbb{F}_q^X$ и тест $T$) работает следующим образом: для заданного слова $c \in \mathbb{F}_q^X$ мы случайным образом выбираем множество $I \in T$ и принимаем $c$, если $c|_I \in \mathcal{C}|_I$, и отвергаем в противном случае. Таким образом, если $c \in \mathcal{C}$, то тестер всегда принимает это слово.

**Определение 3** (Робастность теста)**.** Тест $T$ для кода $\mathcal{C} \subseteq \mathbb{F}_q^X$ называется *$\alpha$-робастным*, если для всех $c \in \mathbb{F}_q^X$ выполнено

$$\mathop{\mathsf{E}}_{I \in T} \delta(c|_I, \mathcal{C}|_I) \geqslant \alpha \delta(c, \mathcal{C}),$$

где $\mathsf{E}$ обозначает математическое ожидание.

Обозначим максимальную робастность как:

$$\rho_r(T, \mathcal{C}) := \max\{\alpha \mid \text{тест } T \text{ является } \alpha\text{-робастным для кода } \mathcal{C}\}.$$

Обычно, когда код $\mathcal{C}$ определяется множеством локальных кодов, естественный тест содержит носители всех этих локальных кодов. Например, произведение кодов $\mathcal{C}_1 \otimes \mathcal{C}_2$ можно определить локальными кодами на линиях, параллельных осям множества $X = [n_1] \times [n_2]$:

$$\mathcal{C}_1 \otimes \mathcal{C}_2 = \left\{ f \in \mathbb{F}_q^{[n_1] \times [n_2]} \;\middle|\; f(\cdot, j) \in \mathcal{C}_1 \text{ для } j \in [n_2], f(i, \cdot) \in \mathcal{C}_2 \text{ для } i \in [n_1] \right\}.$$

Таким образом, естественный тест для кода $\mathcal{C}_1 \otimes \mathcal{C}_2$ — это множество всех линий, параллельных осям:

$$T = \mathcal{L}_1 \cup \mathcal{L}_2 = \{[n_1] \times \{j\} \mid j \in [n_2]\} \cup \{\{i\} \times [n_2] \mid i \in [n_1]\},$$

и $\mathsf{P}$, определённое в (2), соответствует следующему процессу: выбирается случайное направление, затем случайная линия вдоль этого направления. Этот тест называется *тестом по осепараллельным линиям* (*axis-parallel line test*). Для произведения $m \geqslant 3$ кодов существуют различные естественные тесты, так как можно рассматривать подпространства, параллельные осям, различных размеров от 1 до $m - 1$. Следующее определение даёт прямое обобщение 2-flat test из [10, Algorithm 12.2].

**Определение 4** (Тест по осепараллельным $k$-плоскостям)**.** Пусть $X = [n_1]\times\cdots\times[n_m]$, $k \in [m-1]$. Тогда *тест по осепараллельным $k$-плоскостям* (*axis-parallel $k$-flat test*) определяется как множество $T^k_m$ всех $k$-мерных параллельных координатным осям подпространств (*$k$-плоскостей*) в $X$:

$$T^k_m(X) = \bigcup_{I\subseteq[m],|I|=k} \mathcal{L}_I,$$

$$\mathcal{L}_I = \Big\{ A_1 \times\cdots\times A_m \subseteq [n_1]\times\cdots\times[n_m] \;\Big|\; \forall j \in I : A_j = [n_j], \quad \forall j \in [m]\setminus I : |A_j| = 1 \Big\}.$$

Мы будем опускать аргумент $T^k_m$ там, где это не важно или очевидно из контекста.

Здесь мы следуем терминологии из [10]. Тест $T^1_2$ — это стандартный тест по осепараллельным линиям, $T^1_m$ — его многомерная версия, а $T^{m-1}_m$ — *тест по осепараллельным гиперплоскостям*. В [10, Theorem 12.5] было показано, что $\rho_r(T^2_m, \mathcal{C}^{\otimes m}) \geqslant \alpha(\delta(\mathcal{C}), m)$ для $m \geqslant 3$ и некоторой функции[2] $\alpha(\epsilon, m) > 0$. Этот результат показывает, что требование постоянной робастности теста $T^2_m$ для семейства кодов $(\mathcal{C}_i^{\otimes m})_{i\in\mathbb{N}}$ эквивалентно требованию линейного минимального расстояния для кодов в этом семействе: $\delta(\mathcal{C}_i) = \Omega(1)$ при $i \to \infty$. Таким образом, единственный тест, который накладывает нетривиальное ограничение на код $\mathcal{C}$, — это тест по осепараллельным линиям $T^1_m$.

Тест $T^1_m$ можно рассматривать как композицию тестов $T^2_m$ для $\mathcal{C}^{\otimes m}$ и $T^1_2$ для $\mathcal{C}^{\otimes 2}$. Как будет формально показано в лемме 5,

$$\rho_r(T^1_m, \mathcal{C}^{\otimes m}) \geqslant \rho_r(T^2_m, \mathcal{C}^{\otimes m})\rho_r(T^1_2, \mathcal{C}^{\otimes 2}),$$

то есть константная робастность теста $T^1_m$ для $\mathcal{C}^{\otimes m}$ эквивалентна константной робастности теста $T^1_2$ для $\mathcal{C}^{\otimes 2}$, если $\delta(\mathcal{C}) = \Omega(1)$.

Следующее определение тестируемости на согласованность для произведения нескольких кодов является непосредственным обобщением тестируемости на согласованность для произведения двух кодов [2, Definition 2.8].

**Определение 5** (Тестируемость на согласованность для произведений кодов)**.** Пусть $\mathcal{C} = (\mathcal{C}_1, \ldots, \mathcal{C}_m)$ — коллекция кодов. Произведение кодов

[2] Из доказательства [10, Theorem 12.5] следует, что $\alpha(\epsilon, m) = \epsilon^{\frac{1}{2}(m-2)(m+3)} \cdot 24^{2-m}$.

$\otimes\mathcal{C}$ является *$\alpha$-тестируемым на согласованность*, если для каждого $c_1 \in \mathcal{C}^{(1)}, \ldots, c_m \in \mathcal{C}^{(m)}$ существует $c \in \otimes\mathcal{C}$ такое, что

$$\alpha \mathop{\mathsf{E}}_{i\in[m]} \|c_i - c\|_i \leqslant \mathop{\mathsf{E}}_{i,j\in[m]} \|c_i - c_j\|,$$

где предполагается равномерное распределение на $[m]$. Определим максимальную тестируемость на согласованность:

$$\rho_a(\otimes\mathcal{C}) := \max\{\alpha \mid \otimes\mathcal{C} \text{ является } \alpha\text{-тестируемым на согласованность}\}.$$

Заметим, что $\rho_a(\otimes\mathcal{C}) \leqslant 2$, поскольку для любого $c$ выполнено $\|c_i - c_j\| \leqslant \|c_i - c\| + \|c_j - c\| \leqslant \|c_i - c\|_i + \|c_j - c\|_j$.

**Лемма 1** (Робастная тестируемость + линейное расстояние = тестируемость на согласованность)**.** *Пусть $\mathcal{C} = (\mathcal{C}_1, \ldots, \mathcal{C}_m)$ — набор кодов $\mathcal{C}_i \subseteq \mathbb{F}_q^{n_i}$, $\rho_r := \rho_r(T_m^1, \otimes\mathcal{C})$, $\rho_a := \rho_a(\otimes\mathcal{C})$. Тогда*

$$\rho_r \geqslant \frac{1}{4}\rho_a, \qquad \rho_a \geqslant \frac{\rho_r}{\rho_r + 1} \min_{i\in[m]} \delta(\mathcal{C}_i).$$

Доказательство приведено в разделе 3. Оно в целом совпадает с доказательством для произведения двух кодов [2, Lemma 2.9]. Из леммы 1 следует, что робастная тестируемость и тестируемость на согласованность по существу эквивалентны.

Основной результат данной работы состоит в том, что расширение произведения набора кодов отличается от робастной тестируемости и тестируемости на согласованность произведения этих кодов.

**Теорема 1.** *Пусть $C_t$ — примитивный $[n_t, \frac{n_t}{3}]$ код Рида-Соломона над полем $\mathbb{F}_{2^{2t}}$, определённый проверочным многочленом $(x-1)(x-\omega)\ldots(x-\omega^{\frac{n_t}{3}-1})$, где $t \in \mathbb{N}$, $n_t = 2^{2t} - 1$, $\omega$ — примитивный элемент $\mathbb{F}_{2^{2t}}$. Для каждого $m \geqslant 3$ существуют $\alpha_r > 0$ и $\alpha_a > 0$, такие, что для всех $t \in \mathbb{N}$ выполняются следующие неравенства:*

1. $\rho(\underbrace{C_t, \ldots, C_t}_{m \text{ раз}}) \leqslant \dfrac{1}{n_t}$;
2. $\rho_r(T_m^k, C_t^{\otimes m}) \geqslant \alpha_r$ *для всех* $k \in [m-1]$;
3. $\rho_a(C_t^{\otimes m}) \geqslant \alpha_a$.

Более того, расширение произведения влечёт робастность теста $T_m^1$ для кода $\mathcal{C}^{\otimes m}$.

**Утверждение 1.** *Пусть* $\mathcal{C} \subsetneq \mathbb{F}_q^n$ *и* $m \geqslant 2$. *Тогда существует функция* $\alpha$ *такая, что* $\alpha(x) > 0$ *при* $x > 0$ *и*

$$\rho_r(T_m^1, \mathcal{C}^{\otimes m}) \geqslant \alpha(\rho(\underbrace{\mathcal{C}, \ldots, \mathcal{C}}_{m \text{ раз}})).$$

Это утверждение вместе с теоремой 1 показывает, что свойство расширения произведения накладывает более сильное ограничение на код $\mathcal{C}$, чем робастная тестируемость. Теорема 1 и утверждение 1 доказаны в следующем разделе.

## 2. Доказательства

Зафиксируем $t \in \mathbb{N}$ и рассмотрим примитивный $[n, k]$ код Рида-Соломона $C$ над полем $\mathbb{F}_q$, где $q = 2^{2t}$, $n = q - 1$, и $k = n/3$. Этот код может быть определён проверочным многочленом $p(x) = (x-1)(x-\omega)\ldots(x-\omega^{k-1})$, где $\omega$ — примитивный элемент $\mathbb{F}_q$:

$$C = \left\{ (a_i)_{i=0}^{n-1} \in \mathbb{F}_q^n \;\middle|\; p(x) \sum_{i=0}^{n-1} a_i x^i \equiv 0 \mod (x^n - 1) \right\}.$$

Сначала мы покажем, что $\rho(C, C, C) \leqslant 1/n$.

Начнём с описания двойственного кода к произведению циклических кодов в терминах проверочных многочленов. Рассмотрим циклические коды $\mathcal{C}_1, \ldots, \mathcal{C}_m \subseteq \mathbb{F}_q^n$, определённые соответственно проверочными многочленами $p_1, \ldots, p_m \in \mathbb{F}_q[x]$ такими, что $p_i | (x^n - 1)$:

$$\begin{aligned} \mathcal{C}_i &= \left\{ (a_j)_{j=0}^{n-1} \in \mathbb{F}_q^n \;\middle|\; p_i(x) \sum_{j=0}^{n-1} a_j x^j \equiv 0 \mod (x^n - 1) \right\} \\ &\cong \left\{ a \in \mathbb{F}_q[x] \;\middle|\; \deg a < n,\ p_i(x) a(x) \equiv 0 \mod (x^n - 1) \right\}. \end{aligned}$$

Здесь для кодов $\mathcal{C}_1 \subseteq V_1, \mathcal{C}_2 \subseteq V_2$ мы говорим, что $\mathcal{C}_1 \cong \mathcal{C}_2$, если существует линейный изоморфизм $\varphi : V_1 \to V_2$, сохраняющий расстояние Хэмминга, такой, что $\varphi(\mathcal{C}_1) = \mathcal{C}_2$.

**Лемма 2.** *Пусть* $\mathcal{C} = \mathcal{C}_1 \boxplus \cdots \boxplus \mathcal{C}_m$. *Рассмотрим идеал*

$$\mathcal{I} = (x_1^n - 1, \ldots, x_m^n - 1) \subseteq \mathbb{F}_q[x_1, \ldots, x_m].$$

*Тогда*

$$\mathcal{C} = \left\{ a \in \mathbb{F}_q[x_1, \ldots, x_m] \;\middle|\; \deg_{x_i} a < n \text{ для всех } i \in [m] \right. \\ \left. \text{и } a(x_1, \ldots, x_m) \prod_{i=1}^{m} p_i(x_i) \equiv 0 \mod \mathcal{I} \right\}.$$

*Доказательство.* Для многочлена $p(x_1, \ldots, x_k)$ определим

$$p^*(x_1, \ldots, x_k) := p(x_1^{n-1}, \ldots, x_k^{n-1}) \mod \mathcal{I}.$$

Поскольку $p_i(x)$ является проверочным многочленом для $\mathcal{C}_i$, то $p_i^*(x)$ является порождающим многочленом для $\mathcal{C}_i^\perp$, то есть

$$\mathcal{C}_i^\perp = \big\{p_i^*(x)q(x) \;\big|\; \deg q < n - \deg p_i\big\} = \big\{a \in \mathbb{F}_q[x] \;\big|\; \deg a < n \text{ и } p_i^* | a\big\}.$$

Следовательно, тензорное произведение $\mathcal{C}_1^\perp, \ldots, \mathcal{C}_m^\perp$ порождается полиномом

$$p_1^*(x_1) \cdots p_m^*(x_m) \in \mathbb{F}_q[x_1, \ldots, x_m],$$

а именно:

$$\mathcal{C}_1^\perp \otimes \cdots \otimes \mathcal{C}_m^\perp = \big\{a \in \mathbb{F}_q[x_1, \ldots, x_m] \;\big|\; \deg_{x_i} a < n \text{ и } p_i^*(x_i) | a\big\}.$$

Значит $(p_1^*(x_1) \cdots p_m^*(x_m))^* = p_1(x_1) \cdots p_m(x_m)$ является проверочным многочленом для $(\mathcal{C}_1^\perp \otimes \cdots \otimes \mathcal{C}_m^\perp)^\perp = \mathcal{C}_1 \boxplus \cdots \boxplus \mathcal{C}_m$. □

**Лемма 3.** *Пусть $C$ — примитивный код Рида-Соломона $[n, k]$ над полем $\mathbb{F}_q$, определённый проверочным многочленом $p(x) = (x-1)(x-\omega)\ldots(x-\omega^{k-1})$, где $q = 2^{2t}$, $n = q - 1$, $k = n/3$. Тогда*

$$\rho(C, C, C) \leqslant 1/n.$$

*Доказательство.* Кодовое слово кода $C \boxplus C \boxplus C$ может быть задано как многочлен $f(x, y, z)$, такой что

$$f(x, y, z)p(x)p(y)p(z) \equiv 0 \mod (x^n - 1, y^n - 1, z^n - 1).$$

Рассмотрим многочлены

$$a'(x, y, z) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \sum_{l=0}^{n-1} a'_{ijl} x^i y^j z^l, \quad \text{и} \quad a(x, y, z) := a'(x, \omega^{-k} y, \omega^{-2k} z),$$

где

$$a'_{ijl} = \begin{cases} 1, & i + j + l \equiv 0 \mod n \\ 0, & \text{иначе.} \end{cases}$$

Сначала покажем, что $a$ — это кодовое слово кода $C \boxplus C \boxplus C$. Нам нужно показать, что

$$a(x, y, z)p(x)p(y)p(z) = 0 \mod (x^n - 1, y^n - 1, z^n - 1). \tag{3}$$

Рассмотрим многочлены

$$r(x) := p(\omega^k x) = \omega^{k^2} \prod_{i=2k}^{3k-1} (x - \omega^i), \qquad s(x) := p(\omega^{2k} x) = \omega^{2k^2} \prod_{i=k}^{2k-1} (x - \omega^i).$$

Мы имеем

$$a(x, y, z)p(x)p(y)p(z) = a'(x, \omega^{-k} y, \omega^{-2k} z)p(x)r(\omega^{-k} y)s(\omega^{-2k} z), \quad \omega^n = 1,$$

таким образом, заменяя $y \mapsto \omega^{-k} y$, $z \mapsto \omega^{-2k} z$, мы можем переписать условие (3) как

$$a'(x, y, z)p(x)r(y)s(z) = 0 \mod (x^n - 1, y^n - 1, z^n - 1). \tag{4}$$

Поскольку $\omega$ — примитивный элемент $\mathbb{F}_q$, то

$$p(x)r(x)s(x) = \underbrace{\omega^{3k^2}}_{=1} \prod_{i=0}^{n-1} (x - \omega^i) = x^n - 1.$$

Пусть $p(x) = \sum_{i=0}^{n-1} p_i x^i$, $r(x) = \sum_{i=0}^{n-1} r_i x^i$, $s(x) = \sum_{i=0}^{n-1} s_i x^i$. Из

$$p(x)r(x)s(x) \equiv 0 \mod (x^n - 1)$$

следует

$$0 = \sum_{d=0}^{n-1} \sum_{i+j+l \equiv d} p_i r_j s_l x^d \quad \Longrightarrow \quad \sum_{i+j+l \equiv d} p_i r_j s_l = 0 \text{ для всех } d \leqslant n - 1.$$

Следовательно, по модулю $(x^n - 1, y^n - 1, z^n - 1)$ мы имеем

$$\begin{aligned}
a'(x, y, z)p(x)r(y)s(z) &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \sum_{l=0}^{n-1} x^i y^j z^l \sum_{i'=0}^{n-1} \sum_{j'=0}^{n-1} \sum_{l'=0}^{n-1} p_{i-i'} r_{j-j'} s_{l-l'} a'_{i'j'l'} \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \sum_{l=0}^{n-1} x^i y^j z^l \sum_{i'+j'+l' \equiv 0 \bmod n} p_{i-i'} r_{j-j'} s_{l-l'} \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \sum_{l=0}^{n-1} x^i y^j z^l \underbrace{\sum_{i''+j''+l'' \equiv i+j+l \bmod n} p_{i''} r_{j''} s_{l''}}_{=0} \\
&= 0,
\end{aligned}$$

где во второй строке были использованы подстановки $i'' := i - i'$, $j'' := j - j'$, $l'' := l - l'$, все индексы считаются по модулю $n$. Таким образом, (4) выполняется, а значит, выполняется и (3), и, следовательно, $a$ является кодовым словом $C \boxplus C \boxplus C$ по лемме 2.

По определению выполнено $|a| = n^2$. Предположим, что $a = a_1 + a_2 + a_3$, где $a_1 \in C \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$, $a_2 \in \mathbb{F}_q^n \otimes C \otimes \mathbb{F}_q^n$, $a_3 \in \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes C$. Поскольку каждая линия, параллельная осям в кубе $[n]^3$, покрывает только один ненулевой элемент $a_{ijl}$, мы имеем $|a_1|_1 + |a_2|_2 + |a_3|_3 \geqslant |a| = n^2$. Учитывая, что $\|a\| = \frac{1}{n^3}|a| = \frac{1}{n}$ и $\|a_i\|_i = \frac{1}{n^2}|a_i|_i$, получаем

$$\sum_{i \in [3]} \|a_i\|_i = \frac{1}{n^2} \sum_{i \in [3]} |a_i|_i \geqslant 1 = n\|a\|.$$

Таким образом, $\rho(C, C, C) \leqslant 1/n$. □

Только что доказанная лемма 3 показывает, что расширение произведения тройки $(C, C, C)$ стремится к нулю при $n \to \infty$. Теперь объединим известные результаты, чтобы показать, что все тесты $T_m^k$ имеют константную робастность для кода $C^{\otimes m}$ и $k \in [m-1]$ при $n \to \infty$.

Сначала покажем, что тест $T_2^1$ робастный для кода $C \otimes C$. Переформулируем теорему о робастной тестируемости кодов Рида-Соломона из [11] для нашего случая.

**Теорема 2** (Theorem 9 in [11]). *Пусть $\mathbb{F}$ — поле, $X = \{x_1, \ldots, x_n\} \subseteq \mathbb{F}$, $Y = \{y_1, \ldots, y_n\} \subseteq \mathbb{F}$. Пусть $R(x, y)$ — полином над $\mathbb{F}$ степени $(d, n)$, $C(x, y)$ — полином над $\mathbb{F}$ степени $(n, d)$. Если*

$$\mathsf{P}_{(x,y) \in X \times Y} \{R(x, y) \neq C(x, y)\} < \tau^2,$$

*и $n > 2\tau n + 2d$, то существует полином $Q(x, y)$ степени $(d, d)$ такой, что*

$$\mathsf{P}_{(x,y) \in X \times Y} \{R(x, y) \neq Q(x, y) \text{ или } C(x, y) \neq Q(x, y)\} < 2\tau^2.$$

**Лемма 4** (Следствие из теоремы 2). *Пусть $C$ — это $[n, k]$ примитивный код Рида-Соломона над $\mathbb{F}_q$, определённый проверочным многочленом $(x - 1)(x - \omega) \ldots (x - \omega^{k-1})$, где $n = q - 1$, $k < n/2$, а $\omega$ — примитивный элемент $\mathbb{F}_q$. Тогда для любого $c_1 \in C \otimes \mathbb{F}_q^n$, $c_2 \in \mathbb{F}_q^n \otimes C$, если*

$$\delta(c_1, c_2) \leqslant \left(\frac{1}{2} - \frac{k}{n}\right)^2,$$

*то*

$$\delta(c_1, C \otimes C) \leqslant 2\delta(c_1, c_2), \qquad \delta(c_2, C \otimes C) \leqslant 2\delta(c_1, c_2).$$

*Доказательство.* Используя дискретное преобразование Фурье (см., например, [12, Theorem 6.1.5]), можно показать, что каждое кодовое слово $c \in C$ может быть определено как вектор значений некоторого многочлена $p_c \in \mathbb{F}_q[x]$ степени не более $d = k - 1$ в точках $\{1, \omega^{-1}, \omega^{-2}, \ldots, \omega^{1-n}\}$.

Применим теорему 2 к $X = Y = \{1, \omega, \ldots, \omega^{n-1}\}$, $d = k - 1$, $\tau \in I$, где $I$ — это интервал $\left(\sqrt{\delta(c_1, c_2)}, \frac{1}{2} - \frac{d}{n}\right)$. Так как $\sqrt{\delta(c_1, c_2)} \leqslant \frac{1}{2} - \frac{k}{n} < \frac{1}{2} - \frac{d}{n}$, интервал $I$ непуст.

Каждое кодовое слово $c_1 \in C \otimes \mathbb{F}_q^n$ (соответственно, $c_2 \in \mathbb{F}_q^n \otimes C$) определяется вектором значений на $X \times Y$ некоторого многочлена $p_{c_1}(x, y)$ от двух переменных степени не выше[3] $(d, n)$ (соответственно, $p_{c_2}(x, y)$ степени не выше $(n, d)$). Расстояние $\delta(c, c')$ для $c, c' \in \mathbb{F}_q^n \otimes \mathbb{F}_q^n$ можно интерпретировать как $\mathsf{P}_{(x,y)\in X\times Y}\{p_c(x, y) \neq p_{c'}(x, y)\}$.

Поскольку $\tau \in I$, то выполнены условия теоремы 2. Применяя эту теорему к $p_{c_1}$ и $p_{c_2}$, получаем, что существует многочлен $p_c$ степени не выше $(d, d)$ такой, что

$$\mathsf{P}_{(x,y)\in X\times Y}\{p_{c_1}(x, y) \neq p_c(x, y) \text{ или } p_{c_2}(x, y) \neq p_c(x, y)\} \leqslant 2\tau^2.$$

Соответствующее слово $c$ принадлежит произведению кодов $C \otimes C$, так как степень $p_c$ по каждой переменной не превосходит $d$. Следовательно, имеем

$$\delta(c_1, C \otimes C) \leqslant \delta(c_1, c) = \mathsf{P}_{(x,y)\in X\times Y}\{p_{c_1}(x, y) \neq p_c(x, y)\} \leqslant 2\tau^2.$$

Беря инфинум по всем $\tau \in I$, получаем $\delta(c_1, C \otimes C) \leqslant 2\delta(c_1, c_2)$. Аналогично $\delta(c_2, C \otimes C) \leqslant 2\delta(c_1, c_2)$. □

**Следствие 1.** $\rho_r(T_2^1, C \otimes C) \geqslant \frac{1}{72}$.

*Доказательство.* Рассмотрим слово $x \in \mathbb{F}_q^{n\times n}$. Пусть $c_1$ и $c_2$ — ближайшие слова к $x$ из $C \otimes \mathbb{F}_q^n$ и $\mathbb{F}_q^n \otimes C$, соответственно. Пусть $\alpha := \delta(x, c_1) + \delta(x, c_2)$. Нам нужно показать, что

$$\delta(x, C \otimes C) \leqslant 36\left(\delta(x, C \otimes \mathbb{F}_q^n) + \delta(x, \mathbb{F}_q^n \otimes C)\right).$$

По определению $c_1$ и $c_2$ мы имеем $\delta(x, c_1) = \delta(x, C \otimes \mathbb{F}_q^n)$, $\delta(x, c_2) = \delta(x, \mathbb{F}_q^n \otimes C)$. Поэтому требуется доказать, что

$$\delta(x, C \otimes C) \leqslant 36\alpha. \tag{5}$$

Если $\alpha \geqslant \frac{1}{36}$, то (5) выполняется. Теперь рассмотрим основной случай $\alpha < \frac{1}{36}$. Поскольку $C$ — это $[n, k]$ код с $k = n/3$, то по неравенству

[3] Мы говорим, что многочлен $p(x, y)$ от двух переменных степени не выше $(a, b)$, если каждый его моном имеет степень по $x$ не выше $a$ и степень по $y$ не выше $b$

треугольника мы имеем $\delta(c_1, c_2) \leqslant \alpha < \frac{1}{36} = \left(\frac{1}{2} - \frac{k}{n}\right)^2$. Применяя лемму 4, получаем

$$\delta(x, C \otimes C) \leqslant \delta(x, c_1) + \delta(c_1, C \otimes C) \leqslant \alpha + 2\delta(c_1, c_2) \leqslant 3\alpha.$$

Таким образом, в данном случае (5) также выполняется, что завершает доказательство. □

**Лемма 5** (Робастность композиции тестов)**.** *Пусть* $\mathcal{C} \subseteq \mathbb{F}_q^n$ *и* $1 \leqslant k_1 < k_2 < m$*. Тогда*

$$\rho_r(T_m^{k_1}, \mathcal{C}^{\otimes m}) \geqslant \rho_r(T_m^{k_2}, \mathcal{C}^{\otimes m})\rho_r(T_{k_2}^{k_1}, \mathcal{C}^{\otimes k_2}).$$

*Доказательство.* Зафиксируем $x \in (\mathbb{F}_q^n)^{\otimes m}$. Для каждого $k \in [m-1]$ и $\pi \in T_m^k$ мы имеем $\mathcal{C}^{\otimes m}|_\pi \cong \mathcal{C}^{\otimes k}$. Следовательно,

$$\mathop{\mathsf{E}}_{\pi \in T_m^k} \delta(x|_\pi, \mathcal{C}^{\otimes m}|_\pi) = \mathop{\mathsf{E}}_{\pi \in T_m^k} \delta(x|_\pi, \mathcal{C}^{\otimes k}).$$

Таким образом,

$$\begin{aligned}\delta(x, \mathcal{C}^{\otimes m})\rho_r(T_m^{k_2}, \mathcal{C}^{\otimes m})\rho_r(T_{k_2}^{k_1}, \mathcal{C}^{\otimes k_2}) &\leqslant \mathop{\mathsf{E}}_{\pi \in T_m^{k_2}} \delta(x|_\pi, \mathcal{C}^{\otimes k_2})\rho_r(T_{k_2}^{k_1}, \mathcal{C}^{\otimes k_2}) \leqslant \\ &\leqslant \mathop{\mathsf{E}}_{\pi \in T_m^{k_2}} \mathop{\mathsf{E}}_{\pi' \in T_{k_2}^{k_1}(\pi)} \delta(x|_{\pi'}, \mathcal{C}^{\otimes k_1}) = \mathop{\mathsf{E}}_{\pi' \in T_m^{k_1}} \delta(x|_{\pi'}, \mathcal{C}^{\otimes k_1}).\end{aligned}$$

□

**Лемма 6.** *Пусть* $\mathcal{C} \subseteq \mathbb{F}_q^n$*,* $m \geqslant 2$*. Обозначим* $M := \frac{1}{2}(m-2)(m+3) = \sum_{k=3}^m k$*. Тогда для* $k' \in [m-1]$ *выполнено*

$$\rho_r(T_m^{k'}, \mathcal{C}^{\otimes m}) \geqslant \frac{1}{12^{m-2}} \cdot \rho_r(T_2^1, \mathcal{C}^{\otimes 2}) \cdot \delta(\mathcal{C})^M.$$

*Доказательство.* Заметим, что при $m = 2$ утверждение леммы тавтологично. Поэтому далее рассматриваем случай $m \geqslant 3$. Из [13, Theorem 2.6] мы знаем нижнюю границу робастности теста $T_k^{k-1}$:

$$\rho_r(T_k^{k-1}, \mathcal{C}^{\otimes k}) \geqslant \frac{1}{12}\delta(\mathcal{C})^k. \tag{6}$$

Если $k' \geqslant 2$, то, применяя $m - k'$ раз лемму 5, получим

$$\begin{aligned}\rho_r(T_m^{k'}, \mathcal{C}^{\otimes m}) &\geqslant \prod_{k=k'+1}^{m} \rho_r(T_k^{k-1}, \mathcal{C}^{\otimes k}) \geqslant \\ &\geqslant \frac{1}{12^{m-k'}} \cdot \delta(\mathcal{C})^{\sum_{k=k'+1}^m k} \geqslant \frac{1}{12^{m-2}} \cdot \delta(\mathcal{C})^M.\end{aligned}$$

Для $T^1_m$, применяя предыдущее неравенство с $k' = 2$ и лемму 5, получаем:

$$\rho_r(T^1_m, \mathcal{C}^{\otimes m}) \geqslant \rho_r(T^1_2, \mathcal{C}^{\otimes 2})\rho_r(T^2_m, \mathcal{C}^{\otimes m}) \geqslant \frac{1}{12^{m-2}} \cdot \rho_r(T^1_2, \mathcal{C}^{\otimes 2}) \cdot \delta(\mathcal{C})^M. \quad \square$$

Теперь мы готовы доказать основную теорему и утверждение 1.

**Теорема 1.** *Пусть $C_t$ — примитивный $[n_t, \frac{n_t}{3}]$ код Рида-Соломона над полем $\mathbb{F}_{2^{2t}}$, определённый проверочным многочленом $(x-1)(x-\omega)\dots(x-\omega^{\frac{n_t}{3}-1})$, где $t \in \mathbb{N}$, $n_t = 2^{2t}-1$, $\omega$ — примитивный элемент $\mathbb{F}_{2^{2t}}$. Для каждого $m \geqslant 3$ существуют $\alpha_r > 0$ и $\alpha_a > 0$, такие, что для всех $t \in \mathbb{N}$ выполняются следующие неравенства:*

1. $\rho(\underbrace{C_t, \dots, C_t}_{m \text{ раз}}) \leqslant \dfrac{1}{n_t}$;
2. $\rho_r(T^k_m, C_t^{\otimes m}) \geqslant \alpha_r$ *для всех* $k \in [m-1]$;
3. $\rho_a(C_t^{\otimes m}) \geqslant \alpha_a$.

*Доказательство.* Пункт 1 теоремы следует из леммы 3 и [8, Lemma 11]:

$$\rho(\underbrace{C_t, \dots, C_t}_{m \geqslant 3 \text{ раз}}) \leqslant \rho(C_t, C_t, C_t) \leqslant 1/n_t.$$

Пункт 2 теоремы следует из леммы 6 и следствия 1. Поскольку $C_t$ — это $[n_t, \frac{n_t}{3}, \frac{2}{3}n_t + 1]$ код Рида-Соломона, мы имеем $\delta(C_t) = \frac{2}{3} + \frac{1}{n_t}$. Обозначим $\alpha_r := \frac{1}{72 \cdot 12^{m-2}} \cdot \left(\frac{2}{3}\right)^{\frac{1}{2}(m-2)(m+3)}$. По лемме 6 и следствию 1 для всех $k \in [m-1]$ имеем

$$\rho_r(T^k_m, C_t^{\otimes m}) \geqslant \rho_r(T^1_2, C_t^{\otimes 2}) \cdot \frac{1}{12^{m-2}} \cdot \delta(C_t)^{\frac{1}{2}(m-2)(m+3)} > \\ > \frac{1}{72} \cdot \frac{1}{12^{m-2}} \cdot \left(\frac{2}{3}\right)^{\frac{1}{2}(m-2)(m+3)} = \alpha_r.$$

Пункт 3 теоремы с $\alpha_a := \frac{2}{3}\frac{\alpha_r}{1+\alpha_r}$ следует из пункта 2 и леммы 1. $\square$

**Утверждение 1.** *Пусть $\mathcal{C} \subsetneq \mathbb{F}_q^n$ и $m \geqslant 2$. Тогда существует функция $\alpha$ такая, что $\alpha(x) > 0$ при $x > 0$ и*

$$\rho_r(T^1_m, \mathcal{C}^{\otimes m}) \geqslant \alpha(\rho(\underbrace{\mathcal{C}, \dots, \mathcal{C}}_{m \text{ раз}})).$$

*Доказательство.* Пусть $\rho := \rho(\underbrace{\mathcal{C}, \dots, \mathcal{C}}_{m \text{ раз}})$. Доказательство состоит из следующих шагов:

- Из [8, Lemma 11] следует $\rho(\mathcal{C},\mathcal{C}) \geqslant \rho$ и $\delta(\mathcal{C}) = \rho(\mathcal{C}) \geqslant \rho$.
- Используя [8, Lemma 1], мы имеем $\rho_a(\mathcal{C}^{\otimes 2}) \geqslant \rho(\mathcal{C},\mathcal{C}) \geqslant \rho$.
- Из [2, Lemma 2.9] следует

$$\rho_r(T_2^1, \mathcal{C}^{\otimes 2}) \geqslant \frac{\rho_a(\mathcal{C}^{\otimes 2})}{2(1+\rho_a(\mathcal{C}^{\otimes 2}))} \geqslant \frac{\rho}{2(\rho+1)} \geqslant \frac{1}{4}\rho.$$

- Наконец, по лемме 6 имеем

$$\rho_r(T_m^1, \mathcal{C}^{\otimes m}) \geqslant \left(\frac{1}{12}\right)^{m-2} \rho_r(T_2^1, \mathcal{C}^{\otimes 2}) \cdot \delta(\mathcal{C})^{\frac{1}{2}(m-2)(m+3)} \geqslant$$
$$\geqslant \frac{1}{12^{m-2}} \cdot \frac{1}{4}\rho \cdot \rho^{\frac{1}{2}(m-2)(m+3)}.$$

Таким образом, получаем требуемое неравенство с

$$\alpha(\rho) = \frac{1}{4 \cdot 12^{m-2}} \rho^{\frac{1}{2}(m-2)(m+3)+1}.$$

□

## 3. Связь между робастной тестируемостью и тестируемостью на согласованность

В этом разделе мы доказываем лемму 1, которая утверждает, что робастная тестируемость и тестируемость на согласованность произведений кодов эквивалентны с точностью до постоянного множителя для теста $T_m^1$ (тест по линиям, параллельным координатным осям).

**Лемма 1** (Робастная тестируемость + линейное расстояние = тестируемость на согласованность)**.** *Пусть* $\mathcal{C} = (\mathcal{C}_1, \ldots, \mathcal{C}_m)$ — *набор кодов* $\mathcal{C}_i \subseteq \mathbb{F}_q^{n_i}$, $\rho_r := \rho_r(T_m^1, \otimes\mathcal{C})$, $\rho_a := \rho_a(\otimes\mathcal{C})$. *Тогда*

$$\rho_r \geqslant \frac{1}{4}\rho_a, \qquad \rho_a \geqslant \frac{\rho_r}{\rho_r+1} \min_{i\in[m]} \delta(\mathcal{C}_i).$$

*Доказательство.*

**1. Тестируемость на согласованность влечёт робастную тестируемость.** Рассмотрим произвольное $x \in \mathbb{F}_q^{n_1\times\cdots\times n_m}$. Пусть $y_i := \operatorname{argmin}_{y\in\mathcal{C}^{(i)}} \|y - x\|$ для всех $i \in [m]$. Существует $z \in \otimes\mathcal{C}$ такое, что

$$\rho_a \mathop{\mathsf{E}}_{i\in[m]} \|y_i - z\|_i \leqslant \mathop{\mathsf{E}}_{i,j\in[m]} \|y_i - y_j\|.$$

Обозначим $d_x := \mathsf{E}_{\ell \in T_m^1}\, \delta(x|_\ell, \otimes\mathcal{C}|_\ell)$. Мы имеем

$$d_x = \mathop{\mathsf{E}}_{i\in[m]} \mathop{\mathsf{E}}_{\ell\in\mathcal{L}_i} \delta(x|_\ell, \mathcal{C}_i) = \mathop{\mathsf{E}}_{i\in[m]} \delta(x, \mathcal{C}^{(i)}) = \mathop{\mathsf{E}}_{i\in[m]} \|x - y_i\|.$$

Следовательно,

$$\begin{aligned}\|x - z\| &\leqslant \mathop{\mathsf{E}}_{i\in[m]} (\|x - y_i\| + \underbrace{\|y_i - z\|}_{\leqslant \|y_i - z\|_i}) \leqslant d_x + \frac{1}{\rho_a} \mathop{\mathsf{E}}_{i,j\in[m]} \|y_i - y_j\| \\ &\leqslant d_x + \frac{1}{\rho_a}\cdot 2 \mathop{\mathsf{E}}_{i\in[m]} \|x - y_i\| = d_x \left(1 + \frac{2}{\rho_a}\right) \leqslant \frac{4}{\rho_a} d_x.\end{aligned}$$

Таким образом, $\rho_r \geqslant \rho_a/4$.

**2. Робастная тестируемость влечёт тестируемость на согласованность.** Рассмотрим произвольные слова $c_i \in \mathcal{C}^{(i)}$ для $i \in [m]$. Пусть

$$i_0 := \operatorname*{argmin}_{i\in[m]} \mathop{\mathsf{E}}_{j\in[m]} \delta(c_i, c_j).$$

Тогда

$$\mathop{\mathsf{E}}_{j\in[m]} \|c_{i_0} - c_j\| \leqslant \mathop{\mathsf{E}}_{i,j\in[m]} \|c_i - c_j\|. \tag{7}$$

Поскольку тест $T_m^1$ является $\rho_r$-робастным для $\otimes\mathcal{C}$, то существует $c \in \otimes\mathcal{C}$ такое, что

$$\begin{aligned}\rho_r \|c_{i_0} - c\| \leqslant \mathop{\mathsf{E}}_{\ell\in T_m^1} \delta(c_{i_0}|_\ell, \otimes\mathcal{C}|_\ell) = \mathop{\mathsf{E}}_{j\in[m]} \delta(c_{i_0}, \mathcal{C}^{(j)}) \leqslant \\ \leqslant \mathop{\mathsf{E}}_{j\in[m]} \|c_{i_0} - c_j\| \leqslant \mathop{\mathsf{E}}_{i,j\in[m]} \|c_i - c_j\|. \end{aligned} \tag{8}$$

Пусть $\delta_* := \min_{i\in[m]} \delta(\mathcal{C}_i)$. Для $i \in [m]$, $x \in \mathcal{C}^{(i)}$ имеем $\delta(\mathcal{C}_i)\|x\|_i \leqslant \|x\|$. Следовательно, применяя неравенство треугольника, затем (7) и (8), получаем:

$$\begin{aligned}\delta_* \mathop{\mathsf{E}}_{i\in[m]} \|c_i - c\|_i \leqslant \mathop{\mathsf{E}}_{i\in[m]} \|c_i - c\| \leqslant \|c_{i_0} - c\| + \mathop{\mathsf{E}}_{i\in[m]} \|c_i - c_{i_0}\| \leqslant \\ \leqslant \left(1 + \frac{1}{\rho_r}\right) \mathop{\mathsf{E}}_{i,j\in[m]} \|c_i - c_j\|.\end{aligned}$$

Следовательно, $\rho_a(\otimes\mathcal{C}) \geqslant \delta_*(1 + \frac{1}{\rho_r})^{-1}$. □

## Благодарности

Эта работа поддержана Министерством науки и высшего образования Российской Федерации (грант 075-15-2020-801).

## Список литературы

[1] P. Panteleev, G. Kalachev, “Asymptotically good quantum and locally testable classical LDPC codes”, *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2022, 375–388. DOI: 10.1145/3519935.3520017.

[2] I. Dinur, S. Evra, R. Livne, A. Lubotzky, S. Mozes, “Locally testable codes with constant rate, distance, and locality”, *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2022, 357–374. DOI: 10.1145/3519935.3520024.

[3] I. Dinur, M.-H. Hsieh, T.-C. Lin, T. Vidick, “Good Quantum LDPC Codes with Linear Time Decoders”, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2023, 905–918. DOI: 10.1145/3564246.3585101.

[4] A. Leverrier, G. Zémor, “Quantum Tanner codes”, *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE Computer Society, Los Alamitos, CA, USA, 2022, 872–883. DOI: 10.1109/FOCS54457.2022.00117.

[5] A. Leverrier, G. Zémor, “Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes”, *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2023, 1216–1244. DOI: 10.1137/1.9781611977554.ch45.

[6] A. Leverrier, G. Zémor, “Decoding Quantum Tanner Codes”, *IEEE Transactions on Information Theory*, **69**:8 (2023), 5100–5115. DOI: 10.1109/TIT.2023.3267945.

[7] S. Gu, C. A. Pattison, E. Tang, “An Efficient Decoder for a Linear Distance Quantum LDPC Code”, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2023, 919–932. DOI: 10.1145/3564246.3585169.

[8] G. Kalachev, P. Panteleev, *Two-Sided Robustly Testable Codes*, 2022. DOI: 10.48550/arXiv.2206.09973.

[9] T.-C. Lin, M.-H. Hsieh, "$c^3$-Locally Testable Codes from Lossless Expanders", *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022, 1175–1180. DOI: 10.1109/ISIT50566.2022.9834679.

[10] A. Bhattacharyya, Y. Yoshida, "Linear Properties of Functions", *Property Testing: Problems and Techniques*, Springer Singapore, Singapore, 2022, 323–368. DOI: 10.1007/978-981-16-8622-1_12.

[11] A. Polishchuk, D. A. Spielman, "Nearly-Linear Size Holographic Proofs", *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 1994, 194–203. DOI: 10.1145/195058.195132.

[12] R. E. Blahut, *Algebraic codes for data transmission*, Cambridge University Press, Cambridge, 2003, ISBN: 9780521553742,0521553741. DOI: 10.1017/CBO9780511800467, 482 pp.

[13] A. Chiesa, P. Manohar, I. Shinkar, "On Axis-Parallel Tests for Tensor Product Codes", *Theory of Computing*, **16**:5 (2020), 1–34. DOI: 10.4086/toc.2020.v016a005.

Статья поступила 6 марта 2026 г.

## High-Dimensional Expansion of Product Codes is Stronger than Robust and Agreement Testability

G. V. Kalachev

We study the coboundary expansion property of product codes called product expansion, which played a key role in all recent constructions of good qLDPC codes. It was shown before that this property is equivalent to robust testability and agreement testability for products of two codes with linear distance. First, we show that robust testability for the product of many codes with linear distance is equivalent to agreement testability. Second, we provide an example of the product of three codes with linear distance that is robustly testable but not product expanding.

**Keywords:** tensor product code, coboundary expansion, robust testability, agreement testability.

## References


[1] P. Panteleev, G. Kalachev, "Asymptotically good quantum and locally testable classical LDPC codes", *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2022, 375–388. DOI: 10.1145/3519935.3520017.

[2] I. Dinur, S. Evra, R. Livne, A. Lubotzky, S. Mozes, "Locally testable codes with constant rate, distance, and locality", *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2022, 357–374. DOI: 10.1145/3519935.3520024.

[3] I. Dinur, M.-H. Hsieh, T.-C. Lin, T. Vidick, "Good Quantum LDPC Codes with Linear Time Decoders", *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2023, 905–918. DOI: 10.1145/3564246.3585101.

[4] A. Leverrier, G. Zémor, "Quantum Tanner codes", *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE Computer Society, Los Alamitos, CA, USA, 2022, 872–883. DOI: 10.1109/FOCS54457.2022.00117.

[5] A. Leverrier, G. Zémor, "Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes", *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2023, 1216–1244. DOI: 10.1137/1.9781611977554.ch45.

[6] A. Leverrier, G. Zémor, "Decoding Quantum Tanner Codes", *IEEE Transactions on Information Theory*, **69**:8 (2023), 5100–5115. DOI: 10.1109/TIT.2023.3267945.

[7] S. Gu, C. A. Pattison, E. Tang, "An Efficient Decoder for a Linear Distance Quantum LDPC Code", *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2023, 919–932. DOI: 10.1145/3564246.3585169.

[8] G. Kalachev, P. Panteleev, *Two-Sided Robustly Testable Codes*, 2022. DOI: 10.48550/arXiv.2206.09973.

[9] T.-C. Lin, M.-H. Hsieh, "$c^3$-Locally Testable Codes from Lossless Expanders", *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022, 1175–1180. DOI: 10.1109/ISIT50566.2022.9834679.

[10] A. Bhattacharyya, Y. Yoshida, "Linear Properties of Functions", *Property Testing: Problems and Techniques*, Springer Singapore, Singapore, 2022, 323–368. DOI: 10.1007/978-981-16-8622-1_12.

[11] A. Polishchuk, D. A. Spielman, "Nearly-Linear Size Holographic Proofs", *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 1994, 194–203. DOI: 10.1145/195058.195132.

[12] R. E. Blahut, *Algebraic codes for data transmission*, Cambridge University Press, Cambridge, 2003, ISBN: 9780521553742,0521553741. DOI: 10.1017/CBO9780511800467, 482 pp.

[13] A. Chiesa, P. Manohar, I. Shinkar, "On Axis-Parallel Tests for Tensor Product Codes", *Theory of Computing*, **16**:5 (2020), 1–34. DOI: 10.4086/toc.2020.v016a005.

Received on March 6, 2026