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

Gleb Kalachev*

August 20, 2023

Abstract

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 product of many codes with linear distance is equivalent to agreement testability. Second, we provide an example of product of three codes with linear distance which is robustly testable but not product expanding.

1 Introduction

Recent constructions of asymptotically good locally testable codes (LTC) and quantum LDPC (qLDPC) codes [?,?,?,?,?,?,?,?,?] use a special property of product codes that has several names and definitions: robust testability, agreement testability, and product expansion. It was shown [?, Lemma 2.9], [?, Lemma 1] that these definitions are essentially equivalent in the case of the product of two codes. For all known constructions of good qLDPC codes, this property is necessary to get the linear distance and efficient decoders for them. For LTCs there is one exception: in [?] the construction of LTC codes is based on one-sided lossless expanders and does not require local codes satisfying specific property.

In [?, Appendix B] it was shown that product expansion can be understood as a form of high-dimensional expansion called coboundary expansion (for 2-dimensional case see also [?, Section 2.6]). Thus, it seems to be an important property of the product code, as well as robust and agreement testability. Moreover, as product expansion is a form of high-dimensional expansion, it is likely to be useful to construct high-dimensional analogs of codes from [?, ?] which could potentially give good quantum locally testable codes (qLTC).

Also, in [?, Lemma 1] it was shown that product expansion for a pair of codes coincides with agreement testability with the same constant (see also [?, Section 2.6]). The goal of this paper is to clarify the relation between robust testability, agreement testability, and product expansion for the product of more than two codes. In particular, we consider a natural generalization of agreement testability for product of multiple codes and show that in the case of the product of 3 or more codes: 1) product expansion is different from robust and agreement testability; 2) agreement testability is equivalent to robustness of the axis-parallel line test up to a constant factor.

*Gleb Kalachev is with the Faculty of Mechanics and Mathematics, Moscow State University, Moscow, Russia.

1.1 Product expansion

Here we will give the definition of product expansion from [?]. The history and relation with other forms of this definition can also be found in [?]. Given linear codes $\mathcal{C}_1, \ldots, \mathcal{C}_m$ over $\mathbb{F}_q$ we can define the (*tensor*) *product code*

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

where $\mathbb{F}_q^{n_1 \times \cdots \times n_m}$ is the set of functions $c\colon [n_1] \times \cdots \times [n_m] \to \mathbb{F}_q$ and $\mathcal{L}_i$ is the set of lines parallel to the i-th axis in the m-dimensional grid $[n_1] \times \cdots \times [n_m]$, i.e.,

$$\mathcal{L}_i := \{\{x + s \cdot e_i \mid s \in [n_i]\} \mid x \in [n_1] \times \cdots \times [n_m], x_i = 0\}.$$

Here e_i denotes the vector $(0, \ldots, 0, 1, 0 \ldots, 0) \in [n_1] \times \cdots \times [n_m]$ with 1 at the i-th position.

As in [?], for linear codes $\mathcal{C}_1 \subseteq \mathbb{F}_q^{n_1}$, $\mathcal{C}_2 \subseteq \mathbb{F}_q^{n_2}$ we denote by $\mathcal{C}_1 \boxplus \mathcal{C}_2$ the code $(\mathcal{C}_1^\perp \otimes \mathcal{C}_2^\perp)^\perp = \mathcal{C}_1 \otimes \mathbb{F}_q^{n_2} + \mathbb{F}_q^{n_1} \otimes \mathcal{C}_2 \subseteq \mathbb{F}_q^{n_1 \times n_2}$. Given a collection $\mathcal{C} = (\mathcal{C}_i)_{i \in [m]}$ of linear codes over $\mathbb{F}_q$, we can define the codes

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

It is clear that $\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_m = \mathcal{C}^{(1)} \cap \cdots \cap \mathcal{C}^{(m)}$ and $\mathcal{C}_1 \boxplus \cdots \boxplus \mathcal{C}_m = \mathcal{C}^{(1)} + \cdots + \mathcal{C}^{(m)}$. Note that every code $\mathcal{C}^{(i)}$ is the direct sum of $|\mathcal{L}_i| = \frac{1}{n_i} \prod_{i \in [m]} n_i$ copies of the code $\mathcal{C}_i$. For $x \in \mathbb{F}_q^{n_1 \times \cdots \times n_m}$ we denote by $|x|_i$ and $\|x\|_i$, respectively, the number and the fraction of the lines $\ell \in \mathcal{L}_i$ such that $a|_\ell \neq 0$. It is clear that $\|x\|_i = \frac{1}{|\mathcal{L}_i|}|x|_i$. By $|x|$ and $\|x\|$ we denote, respectively, the *Hamming weight* (i.e., the number of non-zero entries) and the *normalized Hamming weight* (i.e., the fraction of non-zero entries) of x. We will also use the following notations: the normalized distance $\delta(x, y) := \|x - y\|$, the normalized distance to code $\delta(x, \mathcal{C}) := \min_{y \in \mathcal{C}} \|x - y\|$, and the normalized minimum distance $\delta(\mathcal{C}) := \min_{x \in \mathcal{C}} \|x\|$ for a code $\mathcal{C} \subseteq \mathbb{F}_q^n$.

Definition (Product-expansion [?]). Given a collection $\mathcal{C} = (\mathcal{C}_i)_{i \in [m]}$ of linear codes $\mathcal{C}_i \subseteq \mathbb{F}_q^{n_i}$, we say that $\mathcal{C}$ is *ρ-product-expanding* if every codeword $c \in \mathcal{C}_1 \boxplus \cdots \boxplus \mathcal{C}_m$ can be represented as a sum $c = \sum_{i \in [m]} a_i$, where $a_i \in \mathcal{C}^{(i)}$ for all $i \in [m]$ and the following inequality holds:

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

We denote as $\rho(\mathcal{C})$ the maximal ρ such that $\mathcal{C}$ is ρ-product-expanding. In [?, Appendix B] it was shown that $\rho(\mathcal{C})$, up to the constant factor $1/m$, is equal to the Cheeger constant of the chain complex naturally associated with the product code $\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_m$.

1.2 Robust and agreement testability

Let X be some finite index set, which we will use to enumerate bits of the code. So, a code $\mathcal{C} \subseteq \mathbb{F}_q^X$ is a set of functions $f : X \to \mathbb{F}_q$. If $I \subseteq X$, then $\mathcal{C}|_I := \{c|_I \mid c \in \mathcal{C}\}$ is punctured code $\mathcal{C}$ consisting of restrictions of codewords from the code $\mathcal{C}$ to the index set I.

Definition. A *test for a code* $\mathcal{C} \subseteq \mathbb{F}_q^X$ is a set $T \subseteq 2^X$ equipped with probability measure P on it.

In this paper, we will always use the following probability distribution:

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

The tester for the pair (code $\mathcal{C} \subseteq \mathbb{F}_q^X$ and a test T) works as follows: for a given word $c \in \mathbb{F}_q^X$ we randomly choose a set $I \in T$ and accept c if $c|_I \in \mathcal{C}|_I$ and reject otherwise. Thus, if $c \in \mathcal{C}$, then any tester accepts it with probability 1.

Definition (Test robustness)**.** The test T for a code $\mathcal{C} \subseteq \mathbb{F}_q^X$ is α-*robust* if for all $c \in \mathbb{F}_q^X$ we have

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

where E denotes expectation.

Let us define the maximal robustness:

$$\rho_r(T, \mathcal{C}) := \max \{\alpha \mid \text{Test } T \text{ is } \alpha\text{-robust for the code } \mathcal{C}\}.$$

Usually, when the code $\mathcal{C}$ is defined by a set of local codes, the natural test contains supports of all these local codes. For example, product code $\mathcal{C}_1 \otimes \mathcal{C}_2$ can be defined by local codes on axis-parallel lines of the set $X = [n_1] \times [n_2]$:

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

Thus, the natural test for the code $\mathcal{C}_1 \otimes \mathcal{C}_2$ is the set of all axis-parallel lines:

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

and P defined in (**??**) corresponds to the following procedure: choose a random direction, then choose a random line along this direction. This test is called the *axis-parallel line test*. For product of $m \geqslant 3$ codes, there exist different natural tests, since we can consider axis-parallel subspaces of different dimensions from 1 to $m-1$. The following definition gives a straightforward generalization of the 2-flat test from [**?**, Algorithm 12.2].

Definition (Axis-parallel k-flat test)**.** Let $X = [n_1] \times \cdots \times [n_m]$, $k \in [m-1]$. Then, the *axis-parallel k-flat test* is defined as the set T_m^k of all k-dimensional axis-parallel subspaces (k-*flats*) in X:

$$T_m^k(X) = \bigcup_{I \subseteq [m], |I| = k} \mathcal{L}_I, \quad \mathcal{L}_I = \left\{ \left\{ x + \sum_{i \in I} s_i e_i \;\middle|\; s_i \in [n_i] \text{ for } i \in I \right\} \;\middle|\; x \in X, x_i = 0 \text{ for } i \in I \right\}.$$

We will omit the argument of T_m^k where it is not important or is clear from context.

Here we follow the terminology from [**?**]. The test T_2^1 is the standard axis-parallel line test, T_m^1 is its multidimensional version, and T_m^{m-1} is the *axis-parallel hyperplane test*. In [**?**, Theorem 12.5] it was shown that $\rho_r(T_m^2, \mathcal{C}^{\otimes m}) \geqslant \alpha \delta(\mathcal{C})$ for $m \geqslant 3$ and some function $\alpha(\epsilon, m) > 0$.[1] This result shows that the requirement of constant robustness of the test T_m^2 for a family of codes $\mathcal{C}_i^{\otimes m}$ is equivalent to the requirement of linear minimum distance of codes in this family. So, the only

[1]From the proof of [**?**, Theorem 12.5] it follows that $\alpha(\epsilon, m) = \epsilon^{\frac{1}{2}(m-2)(m+3)} 24^{2-m}$.

test that gives a non-trivial requirement on the code $\mathcal{C}$ is the axis-parallel line test T^1_m. The test T^1_m can be considered as the composition of tests T^2_m for $\mathcal{C}^{\otimes m}$ and T^1_2 for $\mathcal{C}^{\otimes 2}$. As it will be shown more formally in Lemma ??,

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

that is, the constant robustness of T^1_m for $\mathcal{C}^{\otimes m}$ is equivalent to the constant robustness of T^1_2 for $\mathcal{C}^{\otimes 2}$.

The following definition of agreement testability for product of several codes is a straightforward generalization of agreement testability for product of 2 codes [?, Definition 2.8].

Definition (Agreement testability for product code)**.** Let $\mathcal{C} = (\mathcal{C}_1, \dots, \mathcal{C}_m)$ be a collection of codes. Product code $\otimes\mathcal{C}$ is *α-agreement testable* if for each $c_1 \in \mathcal{C}^{(1)}, \dots, c_m \in \mathcal{C}^{(m)}$ there exists $c \in \otimes\mathcal{C}$ such that

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

where the uniform distribution on $[m]$ is assumed. Let us define the maximal agreement testability:

$$\rho_a(\otimes\mathcal{C}) := \max\{\alpha \mid \text{product code } \otimes\mathcal{C} \text{ is } \alpha\text{-agreement testable}\}.$$

Note that $\rho_a(\otimes\mathcal{C}) \leqslant 2$, since $\|c_i - c_j\| \leqslant \|c_i - c\| + \|c_j - c\| \leqslant \|c_i - c\|_i + \|c_j - c\|_j$.

Lemma 1 (Robust testability + Linear distance = Agreement testability)**.** *Let $\mathcal{C} = (\mathcal{C}_1, \dots, \mathcal{C}_m)$ be a collection of codes $\mathcal{C}_i \subseteq \mathbb{F}_q^{n_i}$, $\rho_r := \rho_r(T^1_m, \otimes\mathcal{C})$, $\rho_a := \rho_a(\otimes\mathcal{C})$. Then*

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

The proof is given in Appendix ??. It is essentially the same as the proof for the product of two codes [?, Lemma 2.9]. From Lemma ?? we see that robust and agreement testability are essentially the same. Our main result is that product expansion of a collection of codes is different from robust and agreement testability of the product of these codes.

Theorem 1. *Let C_t be the primitive Reed-Solomon $[n_t, \frac{n_t}{3}]$ code over the field $\mathbb{F}_{2^{2t}}$ defined by the check polynomial $(x-1)(x-\omega)\dots(x-\omega^{\frac{n_t}{3}-1})$, where $t \in \mathbb{N}$, $n_t = 2^{2t} - 1$, ω is a primitive element of $\mathbb{F}_q$. For each $m \geqslant 3$ there exist $\alpha_r > 0$ and $\alpha_a > 0$ such that for all $t \in \mathbb{N}$ the following inequalities hold:*

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

Moreover, product expansion implies robustness of the test T^1_m for $\mathcal{C}^{\otimes m}$.

Proposition 1. *Let $\mathcal{C} \subsetneq \mathbb{F}_q^n$ and $m \geqslant 2$. Then there exists a function α such that $\alpha(x) > 0$ for $x > 0$ and*

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

This proposition together with Theorem ?? shows that the product expansion property imposes a stronger constraint on the code $\mathcal{C}$ than robust testability. Theorem ?? and Proposition ?? are proved in the next section.

2 The proofs

Let us fix $t \in \mathbb{N}$ and consider the primitive Reed-Solomon $[n, k]$ code C over the field $\mathbb{F}_q$, where $q = 2^{2t}$, $n = q - 1$, and $k = n/3$. This code can be defined by the check polynomial $p(x) = (x-1)(x-\omega)\dots(x-\omega^{k-1})$, where ω is a primitive element of $\mathbb{F}_q$:

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

First, we will show that $\rho(C, C, C) \leqslant 1/n$.

First, let us describe the dual of the product of cyclic codes in terms of check polynomials. Consider cyclic codes $\mathcal{C}_1, \dots, \mathcal{C}_m \in \mathbb{F}_q^n$ defined, respectively, by check polynomials $p_1, \dots, p_m \in \mathbb{F}_q[x]$ such that $p_i | (x^n - 1)$:

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

Here for codes $\mathcal{C}_1 \subseteq V_1$, $\mathcal{C}_2 \subseteq V_2$ we say that $\mathcal{C}_1 \cong \mathcal{C}_2$ if there is a linear isomorphism $\varphi : V_1 \to V_2$ preserving the Hamming distance[2] such that $\varphi(\mathcal{C}_1) = \mathcal{C}_2$.

Lemma 2. *Let $\mathcal{C} = \mathcal{C}_1 \boxplus \dots \boxplus \mathcal{C}_m$. Consider the ideal $\mathcal{I} = (x_1^n - 1, \dots, x_m^n - 1) \subseteq \mathbb{F}_q[x_1, ..., x_m]$. Then*

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

Proof. For a polynomial $p(x_1, ..., x_k)$ define $p^*(x_1, ..., x_k) := p(x_1^{n-1}, ..., x_k^{n-1}) \mod \mathcal{I}$.

Since $p_i(x)$ is a check polynomial for $\mathcal{C}_i$, then $p_i^*(x)$ is a generator polynomial for $\mathcal{C}_i^\perp$, i.e.

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

Hence, the tensor product of $\mathcal{C}_1^\perp, \dots, \mathcal{C}_m^\perp$ is generated by $p_1^*(x_1) \cdots p_m^*(x_m) \in \mathbb{F}_q[x_1, \dots, x_m]$:

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

Therefore, $(p_1^*(x_1) \cdots p_m^*(x_m))^* = p_1(x_1) \cdots p_m(x_m)$ is a check polynomial for $(\mathcal{C}_1^\perp \otimes \dots \otimes \mathcal{C}_m^\perp)^\perp = \mathcal{C}_1 \boxplus \dots \boxplus \mathcal{C}_m$. □

Lemma 3. *Let C be the primitive Reed-Solomon $[n, k]$ code C over the field $\mathbb{F}_q$ defined by the check polynomial $p(x) = (x-1)(x-\omega)\dots(x-\omega^{k-1})$, where $q = 2^{2t}$, $n = q - 1$, $k = n/3$. Then*

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

[2] Distinguished bases in V_1, V_2 are necessary to define the Hamming distance and the minimum distance of $\mathcal{C}_1, \mathcal{C}_2$. In the space of polynomials of degree at most k the distinguished basis is $\{1, x, \dots, x^k\}$.

Proof. A codeword of the code $C \boxplus C \boxplus C$ can be defined as a polynomial $f(x, y, z)$ such that

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

Consider the polynomials

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

where

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

First, we will show that a is a codeword of the code $C \boxplus C \boxplus C$. We need to show that

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

Consider the polynomials

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

We have $a(x,y,z)p(x)p(y)p(z) = a'(x, \omega^{-k}y, \omega^{-2k}z)p(x)r(\omega^{-k}y)s(\omega^{-2k}z)$, $\omega^n = 1$, hence by the replacement $y \mapsto \omega^{-k}y$, $z \mapsto \omega^{-2k}z$ the condition (**??**) can be rewritten as

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

Since ω is a primitive element of $\mathbb{F}_q$, we have $p(x)r(x)s(x) = \omega^{3k^2}\prod_{i=0}^{n-1}(x - \omega^i) = x^n - 1$. Let $p(x) = \sum_{i=1}^n p_i x^i$, $r(x) = \sum_{i=1}^n r_i x^i$, $s(x) = \sum_{i=1}^n s_i x^i$. From $p(x)r(x)s(x) \equiv 0 \mod (x^n - 1)$ we have

$$0 = \sum_{d=0}^{n} \sum_{i+j+l \equiv d} p_i r_j s_l x^d \implies \sum_{i+j+l\equiv d} p_i r_j s_l = 0 \text{ for all } d \leqslant n-1.$$

Therefore, modulo $(x^n - 1, y^n - 1, z^n - 1)$ we have

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

(In the last line we used the substitutions $i'' := i - i'$, $j'' := j - j'$, $k'' := k - k'$). Thus, (**??**) holds, hence (**??**) holds, therefore a is a codeword of $C \boxplus C \boxplus C$ by Lemma **??**.

By definition, $|a| = n^2$. Suppose $a = a_1 + a_2 + a_3$, where $a_1 \in C \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$, $a_2 \in \mathbb{F}_q^n \otimes C \otimes \mathbb{F}_q^n$, $a_3 \in \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes C$. Since each axis-parallel line in the cube $[n]^3$ covers only one non-zero element of a_{ijl}, we have $|a_1|_1 + |a_2|_2 + |a_3|_3 \geqslant |a| = n^2$. Taking into account $\|a\| = \frac{1}{n^3}|a| = \frac{1}{n}$, $\|a_i\|_i = \frac{1}{n^2}|a_i|_i$, we obtain

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

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

Lemma ?? just proved shows that product expansion of the triple (C, C, C) tends to zero as code length $n \to \infty$. Now let us combine known results to show that all tests T_m^k are constantly robust for the code $C^{\otimes m}$ and $k \in [m-1]$ as $n \to \infty$. First, we will show that the test T_2^1 is robust for code $C \otimes C$. Let us reformulate the theorem about robust testability of Reed-Solomon codes from [?] for our case.

Lemma 4 (Corollary of [?, Theorem 9]). *Let C be the $[n, k]$ primitive Reed-Solomon code over $\mathbb{F}_q$ defined by the check polynomial $(x-1)(x-\omega)\dots(x-\omega^{k-1})$, where $n = q-1$, $k < n/2$, and ω is a primitive element of $\mathbb{F}_q$. Then for each $c_1 \in C \otimes \mathbb{F}_q^n$, $c_2 \in \mathbb{F}_q^n \otimes C$ if*

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

then

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

Proof. Using discrete Fourier transform [?, Theorem 6.1.5], it is not hard to show that each codeword $c \in C$ can be defined as the vector of values of some polynomial $p_c \in \mathbb{F}_q[x]$ of degree at most $d = k-1$ at points $(1, \omega^{-1}, \omega^{-2}, \dots, \omega^{1-n})$. We will use [?, Theorem 9] for $X = Y = \{1, \omega, ..., \omega^{n-1}\}$, $d = k-1$, $\delta \in I$, where I is the interval $\left(\sqrt{\delta(c_1, c_2)}, \frac{1}{2} - \frac{d}{n}\right)$. Since $\sqrt{\delta(c_1, c_2)} \leqslant \frac{1}{2} - \frac{k}{n} < \frac{1}{2} - \frac{d}{n}$, the interval I is not empty.

Each codeword $c_1 \in C \otimes \mathbb{F}_q^n$ (resp. $c_2 \in \mathbb{F}_q^n \otimes C$) is defined by the vector of values on $X \times Y$ of some bivariate polynomial $p_{c_1}(x, y)$ of degree[3] (d, n) (resp. $p_{c_2}(x, y)$ of degree (n, d)). For $c, c' \in \mathbb{F}_q^n \otimes \mathbb{F}_q^n$, we can interpret $\delta(c, c')$ as $\mathsf{P}_{(x,y)\in X\times Y}\{p_c(x, y) \neq p_{c'}(x, y)\}$. Since $\delta \in I$, the conditions of [?, Theorem 9] hold. Applying this theorem to p_{c_1} and p_{c_2} there exist p_c of degree (d, d) such that

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

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

The corresponding word c belongs to the product code $C \otimes C$, since the degree of p_c in each variable is bounded by d. Therefore, we have

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

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

Taking the infinum over all $\delta \in I$, we have $\delta(c_1, C \otimes C) \leqslant 2\delta(c_1, c_2)$. Similarly, $\delta(c_2, C \otimes C) \leqslant 2\delta(c_1, c_2)$. $\square$

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

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

[3]We say that a polynomial $p(x, y)$ has degree (a, b) if it has degree at most a in x and degree at most b in y

[3]We say that a polynomial $p(x, y)$ has degree (a, b) if it has degree at most a in x and degree at most b in y

Proof. Consider a word $x \in \mathbb{F}_q^{n\times n}$. Let c_1 and c_2 be the nearest words to x from $C \otimes \mathbb{F}_q^n$ and $\mathbb{F}_q^n \otimes C$, respectively. Let $\alpha := \delta(x, c_1) + \delta(x, c_2)$. We want to show that

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

By definition of c_1 and c_2 we have $\delta(x, c_1) = \delta(x, C \otimes \mathbb{F}_q^n)$, $\delta(x, c_2) = \delta(x, \mathbb{F}_q^n \otimes C)$, hence we need to prove that

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

If $\alpha \geqslant \frac{1}{36}$, then (??) holds. Now consider the main case $\alpha < \frac{1}{36}$. Since C is $[n, k]$ code with $k = n/3$, in this case by the triangle inequality we have $\delta(c_1, c_2) \leqslant \alpha < \frac{1}{36} \leqslant \frac{1}{2}\left(\frac{1}{2} - \frac{k}{n}\right)^2$. Hence, by Lemma ?? we have

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

Thus, in this case (??) holds as well, and the proof is complete. □

Lemma 5 (Robustness of test composition)**.** *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ and $1 \leqslant k_1 < k_2 < m$. Then*

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

Proof. Fix $x \in (\mathbb{F}_q^n)^{\otimes m}$. For each $k \in [m-1]$ and $\pi \in T_m^k$ we have $\mathcal{C}^{\otimes m}|_\pi \cong \mathcal{C}^{\otimes k}$, hence

$$\mathop{\mathsf{E}}_{\pi \in T_m^k} \delta(x|_\pi, \mathcal{C}^{\otimes m}|_\pi) = \mathop{\mathsf{E}}_{\pi \in T_m^k} \delta(x|_\pi, \mathcal{C}^{\otimes k_1}).$$

Therefore,

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

Lemma 6. *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$. Denote $M := \frac{1}{2}(m-2)(m+3) = \sum_{k=3}^m k$. Then*

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

Proof. From [?, Theorem 2.6] we have a lower bound on robustness of axis-parallel hyperplane test:

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

Applying Lemma ?? repeatedly $m-2$ times, then using the inequality (??), we obtain:

$$\rho_r(T_m^1, \mathcal{C}^{\otimes m}) \geqslant \rho_r(T_2^1, \mathcal{C}^{\otimes 2}) \prod_{k=3}^m \rho_r(T_k^{k-1}, \mathcal{C}^{\otimes k}) \geqslant \frac{1}{12^{m-2}} \cdot \rho_r(T_2^1, \mathcal{C}^{\otimes 2}) \cdot \delta(\mathcal{C})^M.$$
□

Now we are ready to prove Theorem ?? and Proposition ??.

Theorem ??. *Let C_t be the primitive Reed-Solomon $[n_t, \frac{n_t}{3}]$ code over the field $\mathbb{F}_{2^{2t}}$ defined by the check polynomial $(x-1)(x-\omega)\dots(x-\omega^{\frac{n_t}{3}-1})$, where $t \in \mathbb{N}$, $n_t = 2^{2t}-1$, ω is a primitive element of $\mathbb{F}_q$. For each $m \geqslant 3$ there exist $d_r > 0$ and $\alpha > 0$ such that for all $t \in \mathbb{N}$ the following inequalities hold:*

1. $\rho(\underbrace{C_t,\dots,C_t}_{m\text{ times}}) \leqslant \frac{1}{n_t}$;

2. $\rho_r(T_m^k, C_t^{\otimes m}) \geqslant \alpha_r$ *for all* $k \in [m-1]$;

3. $\rho_a(C_t^{\otimes m}) \geqslant \alpha_a$.

Proof. Claim 1 of the theorem follows from Lemma **??** and [**?**, Lemma 11]:

$$\rho(\underbrace{C,\dots,C}_{m\geqslant 3\text{ times}}) \leqslant \rho(C,C,C) \leqslant 1/n.$$

Claim 2 of the theorem follows from Lemma **??** and Corollary **??**. Recall that C is $[n, \frac{n}{3}, \frac{2}{3}n+1]$ Reed-Solomom code, therefore $\delta(C) = \frac{2}{3} + \frac{1}{n}$. Put $\alpha_r := \frac{1}{72\cdot 12^{m-2}} \cdot \left(\frac{2}{3}\right)^{\frac{1}{2}(m-2)(m+3)}$. By Lemma **??** and Corollary **??** we have

$$\rho_r(T_m^1, C^{\otimes m}) \geqslant \rho_r(T_2^1, C^{\otimes 2}) \cdot \frac{1}{12^{m-2}} \cdot \delta(C)^{\frac{1}{2}(m-2)(m+3)} > \frac{1}{72} \cdot \frac{1}{12^{m-2}} \cdot \left(\frac{2}{3}\right)^{\frac{1}{2}(m-2)(m+3)} = \alpha_r.$$

Claim 3 of the theorem with $\alpha_a := \frac{2}{3}\frac{\alpha_r}{1+\alpha_r}$ follows from Claim 2 and Lemma **??**. ☐

Proposition ??. *Let* $\mathcal{C} \subsetneq \mathbb{F}_q^n$ *and* $m \geqslant 2$. *Then there exists a function* α *such that* $\alpha(x) > 0$ *for* $x > 0$ *and*

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

Proof. Let $\rho := \rho(\underbrace{\mathcal{C},\dots,\mathcal{C}}_{m\text{ times}})$. The proof is the sequence of following steps.

- By [**?**, Lemma 11] we have $\rho(\mathcal{C},\mathcal{C}) \geqslant \rho$, $\delta(\mathcal{C}) = \rho(\mathcal{C}) \geqslant \rho$.
- Using [**?**, Lemma 1], we obtain $\rho_a(\mathcal{C}^{\otimes 2}) \geqslant \rho(\mathcal{C},\mathcal{C}) \geqslant \rho$.
- From [**?**, Lemma 2.9] we have

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

- Finally, by Lemma **??** we have

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

Thus, we obtain the required inequality with $\alpha(\rho) = \frac{1}{4\cdot 12^{m-2}}\rho^{\frac{1}{2}(m-2)(m+3)+1}$. ☐

Acknowledgment

This work was supported by the Ministry of Science and Higher Education of the Russian Federation (Grant 075-15-2020-801).

A Relation between robust and agreement testability

In this section we prove Lemma ??, which states that robust and agreement testability are the same up to a constant factor for the axis-parallel line test for product codes.

Lemma ?? (Robust testability + Linear distance = Agreement testability)**.** *Let* $\mathcal{C} = (\mathcal{C}_1, \dots, \mathcal{C}_m)$ *be a collection of codes* $\mathcal{C}_i \in \mathbb{F}_q^{n_i}$, $\rho_r := \rho_r(T_m^1, \otimes\mathcal{C})$, $\rho_a := \rho_a(\otimes\mathcal{C})$. *Then*

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

Proof. **1. Agreement testability implies robust testability.** Consider arbitrary $x \in \mathbb{F}_q^{n_1 \times \dots \times n_m}$. Let $y_i := \operatorname{argmin}_{y \in \mathcal{C}^{(i)}} \|y - x\|$ for all $i \in [m]$. There exists $z \in \otimes\mathcal{C}$ such that

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

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

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

Hence

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

Therefore, $\rho_r \geqslant \rho_a / 4$.

2. Robust testability implies agreement testability. Consider arbitrary words $c_i \in \mathcal{C}^{(i)}$ for $i \in [m]$. Let

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

Thus we have

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

Since the test T_m^1 is ρ_r-robust for $\otimes\mathcal{C}$, there exists $c \in \otimes\mathcal{C}$ such that

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

Let $\delta_* := \min_{i \in [m]} \delta(\mathcal{C}_i)$. For $i \in [m]$, $x \in \mathcal{C}^{(i)}$ we have $\delta(\mathcal{C}_i)\|x\|_i \leqslant \|x\|$. Hence, applying the triangle inequality followed by (??) and (8), we get:

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

Therefore, $\rho_a(T_m^k, \mathcal{C}^{\otimes m}) \geqslant \delta_* (1 + \frac{1}{\rho_r})^{-1}$. ∎