Electronic Colloquium on Computational Complexity, Report No. 70 (2011)

Composition of semi-LTCs by two-wise Tensor Products*

Eli Ben-Sasson†
Computer Science Department
Technion — Israel Institute of Technology
Haifa 32000, Israel
eli@cs.technion.ac.il

Michael Viderman
Computer Science Department
Technion — Israel Institute of Technology
Haifa 32000, Israel
viderman@cs.technion.ac.il

May 1, 2011

Abstract

In this paper we obtain a composition theorem that allows us to construct locally testable codes (LTCs) by repeated two-wise tensor products. This is the first composition theorem showing that *repeating* the two-wise tensor operation any constant number of times still results in a locally testable code, improving upon previous results which only worked when the tensor product was applied *once*.

To obtain our results we define a new tester for tensor products. Our tester uses the distribution of the "inner tester" associated with the base-code to sample rows and columns of the product code. This construction differs from previously studied testers for tensor product codes which sampled rows and columns *uniformly*.

We show that if the base-code is any LTC or any expander code, then the code obtained by taking the *repeated* two-wise tensor product of the base-code with itself is locally testable. In particular, this answers a question posed in the paper of Dinur et al. (2006) by expanding the class of allowed base-codes to include all LTCs, and not just so-called *uniform LTCs* whose associated tester queries all codeword entries with equal probability.

1 Introduction

Locally testable codes (LTCs) are error correcting codes for which distinguishing, when given oracle access to a purported word w, between the case that w is a codeword and the case that it is very far from all codewords, can be accomplished by a randomized algorithm, called a *tester*. The tester reads a sublinear amount of information from w. Such codes are of interest in computer science due to their numerous connections to probabilistically checkable proofs (PCPs) and property testing. (See the surveys [26, 16] for more information.) By now several different constructions of LTCs are known including codes based on low-degree polynomials over finite fields [23, 1], constructions based on PCPs of proximity/assignment testers [2, 12], sparse random linear codes [8, 19, 21] and affine invariant codes [20]. Our work studies a different family of LTC constructions, namely, *tensor*

*A preliminary version of this paper appeared in the Proceedings of APPROX-RANDOM 2009 [6].

†The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 240258. Research of both authors supported by grant number 2006104 by the US-Israel Binational Science Foundation and by grant number 679/06 by the Israeli Science Foundation.

ISSN 1433-8092

codes. Given two linear error correcting codes $C \subseteq \mathbf{F}^n, R \subseteq \mathbf{F}^m$ over a finite field $\mathbf{F}$, we define their *tensor product* to be the subspace $R \otimes C \subseteq \mathbf{F}^{n \times m}$ consisting of $n \times m$ matrices M with entries in $\mathbf{F}$ having the property that every row of M is a codeword of R and every column is a codeword of C. If $C = R$ we use C^2 to denote $C \otimes C$ and for $i > 2$ define $C^i = C \otimes C^{i-1}$.

Ben-Sasson and Sudan suggested in [5] to use tensor product codes as a means to construct LTCs combinatorially. They showed that taking the *three-wise tensor* C^3 of any code $C \subseteq \mathbf{F}^n$ with sufficiently large distance results in a *robust* locally testable code. By *robust* we informally mean that the tester associated with C^3 has the property that given any word w that is far from C^3, the *local view* selected by the tester will be far, on average, from being consistent with a local view of a codeword of C^3. More formally, denoting by $w|_I$ the projection of w onto the set of queries $I \subset \{1, \ldots, n\}^3$ picked by the tester, and denoting by $C^3|_I = \left\{c|_I \;\middle|\; c \in C^3\right\}$ the set of views that are *consistent* with C^3, the *robustness* of C^3 means that, on average, $w|_I$ will be far in Hamming distance from all elements of $C^3|_I$. This robustness allowed them to apply *composition* and prove that the *repeated* three-wise tensor product of C, namely, the code C^{3^t}, is locally testable. The ability to take the repeated tensor product is crucial for tensor-based constructions of LTCs. The repeated m-wise tensor product (for $m \geq 3$) was used in [5, 24] to construct new families of LTCs. Ben-Sasson and Sudan also raised the question of whether the repeated *two-wise* tensor product of C also leads to robust LTCs.

There is a surprising difference between two- and three-wise tensor products. For two-wise products, large distance is not sufficient to guarantee robustness (whereas for three-wise products it is). This phenomena was discovered by Paul Valiant who constructed in [27] a pair of codes R, C with large distance whose tensor product is not robust. (See [10, 17] for generalizations of this result.) Nevertheless, in another surprising turn of events, Dinur et al. [13] showed that if C is any so-called *smooth* code, and has sufficiently large distance, then C^2 is robust. The family of smooth codes includes low density parity check (LDPC) codes based on expander graphs with very good expansion properties, even though these codes are not necessarily locally testable [3], and *uniform* LTCs which are LTCs whose associated tester is *equally* likely to query any codeword symbol. (These results were generalized in our earlier work [7] to *weakly smooth* codes which besides the above codes include also unique-neighbor expander codes and locally correctable codes.)

One issue that has remained open in all previous works on two-wise tensor product codes is under what conditions can one compose such codes and apply *repeated* two-wise products. To see the problem consider C^2 where C is an expander code, which is smooth (as well as weakly smooth). The work of Dinur et al. [13] showed that C^2 is robust, however, there is no reason to believe C^2 is smooth or weakly smooth. So one cannot argue that C^4 is a robust LTC and apply composition.[1] In terms of LTC constructions, this means that, using previous techniques, the smallest query complexity we could get in a two-wise tensor based construction would be at least $\Omega(\sqrt{n})$, where n is a blocklength of the constructed code. This contrasts once again with the case of three-wise tensors which can be composed repeatedly provided the base code C has (very) large distance, thus resulting in LTCs with polynomial rate and polylogarithmic query complexity.

Our main result uses a new family of testers for repeated two-wise tensor product codes that allows us to provide a general composition theorem for the two-wise tensor products. Our proof follows by defining a new tester for two-wise tensor codes which differs from previous constructions. Previous testers used only the uniform distribution to sample rows and columns of C^2. The key

[1] Close inspection of [13, 7] reveals that repeated products can result in robust LTCs if the base code is a *strong uniform LTC*, but it was not clear how to obtain similar results for expander codes or for nonuniform LTCs.

difference is that our tester, besides using the uniform distribution, also uses the distribution associated with the base code C to sample rows and columns of C^2. We define *semi LTCs* which play a crucial role in our results together with our new tester. The notion of a semi LTC is a relaxation of a standard LTC. Informally, an error correcting code R is a semi LTC if it has a tester that reads only a few symbols from an input word. This tester always accepts all words in R and rejects with high probability words that are approximately a fixed distance from zero codeword, and not all words that are far from R like testers for LTCs (see formal definition of semi LTCs in Section 3). Semi LTCs contain all LTCs and some expander codes. In particular, our results provide a construction of LTCs with query complexity n^ϵ for any $\epsilon > 0$ based on repeated two-wise tensors, where n is a blocklength of the constructed code. This result holds even for LTCs that are *nonuniform*, i. e., whose associated tester may sample some codeword bits more often than others (some LTCs, most notably those of [2, 4, 11, 24], are indeed nonuniform). This result also answers a question raised in [13, Section 2.2], namely, the question of whether there exist robust testers for two-wise tensors of a nonuniform LTC with some other code.

We end by pointing out that our result does not require the base code to have very large distance, hence it holds even over fields of small cardinality. This contrasts with previous works on iterative combinatorial constructions of LTCs due to Ben-Sasson and Sudan [5] and Meir [24] which required very large base-code distance implying large field size. Moreover, in [5] the required base-code distance (and thus a field cardinality) depends on the number of repeated tensor products that should be applied. In our work, the repeated two-wise tensor product can be applied any constant number of times even over the binary field. Moreover, the initial requirements about the base-codes are independent of the number of times that repeated tensor products should be applied.

Organization of the rest of the paper After presenting the necessary definitions in the next section we state our main results in Section 3. In particular, Section 3 presents the notion of *semi LTC* and our suggested tester which are crucial for our proofs. This is followed by the proof of our main technical theorem (Theorem 3.3) in Section 4. In Section 5 we show that the property "strong semi LTC" is preserved after a tensor product is applied. We conclude in Section 6 with formal proofs of our main corollaries. Some auxiliary material is postponed to the appendix.

2 Preliminary Definitions

Throughout this paper, $\mathbf{F}$ is a finite field, $[n]$ denotes the set $\{1, \ldots, n\}$ and $\mathbf{F}^n$ denotes $\mathbf{F}^{[n]}$. All codes discussed in this paper will be a linear. Let $C \subseteq \mathbf{F}^n$ be a linear code over $\mathbf{F}$.

For $w \in \mathbf{F}^n$ let $\mathrm{supp}(w) = \{i | w_i \neq 0\}$, $|w| = |\mathrm{supp}(w)|$ and $\mathrm{wt}(w) = \frac{|w|}{n}$. We define the *distance* between two words $x, y \in \mathbf{F}^n$ to be $\Delta(x, y) = |\{i \mid x_i \neq y_i\}|$ and the relative distance to be $\delta(x, y) = \frac{\Delta(x,y)}{n}$. The distance of a code is defined by $\Delta(C) = \min_{x \neq y \in C} \Delta(x, y)$ and its the relative distance is denoted $\delta(C) = \frac{\Delta(C)}{n}$. A $[n, k, d]_{\mathbf{F}}$-code is a k-dimensional subspace $C \subseteq \mathbf{F}^n$ of distance d. The rate of the code C is defined by $\mathrm{rate}(C) = \frac{\dim(C)}{n}$. For $x \in \mathbf{F}^n$ and $C \subseteq \mathbf{F}^n$, let $\delta(x, C) = \delta_C(x) = \min_{y \in C} \{\delta(x, y)\}$ to denote the relative distance of x from the code C. We note that $\Delta(C) = \min_{c \in C \setminus \{0\}} \{\mathrm{wt}(c)\}$. If $\delta(x, C) \geq \epsilon$ we say that x is ϵ-far from C and otherwise x is ϵ-close to C. We let $\dim(C)$ denote the dimension of C. The vector inner product between $u = (u_1, u_2, \ldots, u_n) \in \mathbf{F}^n$ and $v = (v_1, v_2, \ldots, v_n) \in \mathbf{F}^n$ is defined to be $\langle u, v \rangle = \sum_{i \in [n]} u_i \cdot v_i$. We

let $C^{\perp} = \{u \in \mathbf{F}^n \mid \forall c \in C : \langle u, c\rangle = 0\}$ be the dual code of C and $C_t^{\perp} = \left\{u \in C^{\perp} \mid |u| = t\right\}$. In a similar way we define $C_{\leq t}^{\perp} = \left\{u \in C^{\perp} \mid |u| \leq t\right\}$. For $t \in \mathbf{F}^n$ and $T \subseteq \mathbf{F}^n$ we say that $t \perp T$ if $\langle t, t'\rangle = 0$ for all $t' \in T$.

For $w \in F^n$ and $S = \{j_1, j_2, \ldots, j_m\} \subseteq [n]$, where $j_1 < j_2 < \ldots < j_m$, we let $w|_S = (w_{j_1}, \ldots, w_{j_m})$ be the *restriction* of w to the subset S. We let $C|_S = \{c|_S \mid c \in C\}$ denote the restriction of the code C to the subset S.

2.1 Tensor Product Codes

The definitions appearing here are standard in the literature on tensor-based LTCs (e. g. [13, 5, 24, 7, 27]).

For $x \in \mathbf{F}^I$ and $y \in \mathbf{F}^J$ we let $x \otimes y$ denote the tensor product of x and y (i. e., the matrix M with entries $M_{(i,j)} = x_i \cdot y_j$ where $(i, j) \in I \times J$). Let $R \subseteq \mathbf{F}^I$ and $C \subseteq \mathbf{F}^J$ be linear codes. We define the tensor product code $R \otimes C$ to be the linear space spanned by words $r \otimes c \in \mathbf{F}^{I \times J}$ for $r \in R$ and $c \in C$. Some known facts regarding the tensor products (see e. g., [13]):

- The code $R \otimes C$ consists of all $I \times J$ matrices over $\mathbf{F}$ whose rows belong to R and whose columns belong to C.
- $\dim(R \otimes C) = \dim(R) \cdot \dim(C)$
- $\delta(R \otimes C) = \delta(R) \cdot \delta(C)$

We let $C^1 = C$ and $C^t = C^{t-1} \otimes C$ for $t > 1$. Note by this definition, $C^{2^0} = C$ and $C^{2^t} = C^{2^{t-1}} \otimes C^{2^{t-1}}$ for $t > 0$.

2.2 Expander Codes

Low density parity check (LDPC) codes were introduced by Gallager more than four decades ago [14, 15]. They have been studied extensively in information theory (cf. [9]). Binary LDPC codes motivated Margulis' explicit construction of graphs of large girth [22], and the work of Sipser and Spielman [25].

In this section we give the definitions of LDPC codes based on expander graphs as appeared in [3]. We define various types of "neighbors" (Definition 2.1) and the associated forms of "expanders" (Definition 2.2).

Definition 2.1 (Neighbors)**.** Let $G = (V, E)$ be a graph. For $S \subseteq V$, let

- $N(S)$ be the set of neighbors of S.
- $N^1(S)$ be the set of unique neighbors of S, i. e., vertices with exactly one neighbor in S.
- $N^{odd}(S)$ be the set of neighbors of S with an odd number of neighbors in S.

Notice that $N^1(S) \subseteq N^{odd}(S)$.

We note that $N(S)$ and $N^1(S)$ are standard notations, while $N^{odd}(S)$ is not standard and was defined in [3].

Definition 2.2 (Expander code)**.** Let $c, d \in N$ and $\gamma, \tau \in (0,1)$ be constants. Let $C \subseteq \mathbf{F}^n$ be a linear code and $S \subseteq C^\perp$ such that $\text{span}(S) = C^\perp$. Note that $x \in C$ if and only if $x \perp S$.

A parity check graph of C is a bipartite graph $G = (L, S, E)$ with vertex sets L, S such that $L = [n]$, $S \subseteq C^\perp$ and for every $l \in L$ and $s \in S$ it holds that $(l, s) \in E$ if and only if $l \in \text{supp}(s)$.

Assume that all vertices in L have degree $\leq c$, and all vertices in S have degree $\leq d$ and let us define expanders.

- G is called a (c, d, γ, τ)-*expander* if for all subsets $L_0 \subseteq L$ such that $|L_0| \leq \tau n$ we have $|N(L_0)| > \gamma \cdot c|S|$
- G is called a (c, d, γ, τ)-*odd expander* if for all subsets $L_0 \subseteq L$ such that $|L_0| \leq \tau n$ we have $|N^{odd}(L_0)| > \gamma \cdot c|L_0|$

We say that a code C is a (c, d, γ, τ)-*odd expander code* if it has a parity check graph that is a (c, d, γ, τ)-odd expander.

We notice that the definition of an odd expander generalizes the definition of a unique neighbor expander, which was already shown in [7] to result in a robustly testable tensor code (see Definition 2.6). However, we do not aware about the use of odd expander codes in information theory.

2.3 Locally testable codes and Robustly Testable Codes

A *standard q-query tester* for a linear code $C \subseteq \mathbf{F}^n$ is a randomized algorithm that reads at most q symbols from an input string $w \in \mathbf{F}^n$ and outputs accept or reject. We can assume without loss of generality (see [3, Theorem 2]) that the q-query tester T for C executes the follows steps. Given a word $w \in \mathbf{F}^n$ the tester T picks (non-adaptively) a subset $I \subseteq [n]$ such that $|I| \leq q$. Then T reads all symbols of $w|_I$ and accepts if $w|_I \in C|_I$, and rejects otherwise.

For purposes of composition we want to define a generalized tester (Definition 2.3) which does not make queries, but returns a "view" (a subset $I \subseteq [n]$) which can be considered as a code by itself ($C|_I$).

Definition 2.3 (Tester of C and Test View)**.** A *q-query tester* $\mathbf{D}$ is a distribution $\mathbf{D}$ over subsets $I \subseteq [n]$ such that $|I| \leq q$. Let $w \in \mathbf{F}^n$ (think of the task of testing whether $w \in C$) and let $I \subseteq [n]$ be a subset. We call $w|_I$ the *view* of a tester. If $w|_I \in C|_I$ we say that this view is *consistent* with C, or when C is clear from the context we simply say $w|_I$ is *consistent*.

When considering a tensor code $R \otimes C \subseteq \mathbf{F}^m \otimes \mathbf{F}^n$, an associated tester will be a distribution over subsets $I \subseteq [n] \times [m]$. Although the tester does not output accept or reject, the way a standard tester does, it can be converted to output accept, reject as follows. Whenever the task is to test whether $w \in C$ and a subset $I \subseteq [n]$ is selected by the tester, the tester can output accept if $w|_I \in C|_I$ and otherwise output reject.

Definition 2.4 (LTCs and strong LTCs)**.** A code $C \subseteq \mathbf{F}^n$ is a (q, ϵ, δ)-LTC if it has a q-query tester $\mathbf{D}$ such that for all $w \in \mathbf{F}^n$, if $\delta(w, C) \geq \delta$ we have $\Pr_{I \sim \mathbf{D}}[w|_I \notin C|_I] \geq \epsilon$.

A code $C \subseteq \mathbf{F}^n$ is a (q, ϵ)-strong LTC if it has a q-query tester $\mathbf{D}$ such that for all $w \in \mathbf{F}^n$, we have $\Pr_{I \sim \mathbf{D}}[w|_I \notin C|_I] \geq \epsilon \cdot \delta(w, C)$.

Note that given a code $C \subseteq \mathbf{F}^n$, the subset $I \subseteq [n]$ uniquely defines $C|_I$. Moreover, the linearity of C implies that $C|_I$ is a linear subspace of $\mathbf{F}^I$. In the rest of this section we formally define the notion of *robustness* (Definition 2.6) as was introduced in [5]. To do that we start from the definition of *local distance* (Definition 2.5), which will be used in Definition 2.6 and later in our proofs.

Definition 2.5 (Local distance)**.** Let C be a code and $w|_I$ be the view on the coordinate set I obtained from the word w. The *local distance* of w from C with respect to I (also called the I-distance of w from C) is $\Delta(w|_I, C|_I) = \min_{c \in C} \{\Delta(w|_I, c|_I)\}$ and similarly the *relative local distance* of w from C with respect to I (relative I-distance of w from C) is $\delta(w|_I, C|_I) = \min_{c \in C} \{\delta(w|_I, c|_I)\}$. When I is clear from context we omit reference to it.

Informally, robustness implies that if a word is far from the code then, on average, a test's view is far from any consistent view that can be accepted on the same coordinate set I. This notion was defined for LTCs following an analogous definition for PCPs [2, 11]. We are now ready to provide a general definition of robustness.

Definition 2.6 (Robustness)**.** Given a tester (i. e., a distribution) $\mathbf{D}$ for the code $C \subseteq \mathbf{F}^n$, we let

$$\rho^{\mathbf{D}}(w) = \mathop{\mathbf{E}}_{I \sim \mathbf{D}} [\delta(w|_I, C|_I)] \text{ be the expected relative local distance of input } w.$$

We say that the tester $\mathbf{D}$ has robustness $\rho^{\mathbf{D}}(C)$ on the code C if for every $w \in \mathbf{F}^n$ it holds that $\rho^{\mathbf{D}}(w) \geq \rho^{\mathbf{D}}(C) \cdot \delta_C(w)$.

Let $\{C_n\}_n$ be a family of codes where C_n is of blocklength n and $\mathbf{D_n}$ is a tester for C_n. A family of codes $\{C_n\}_n$ is *robustly testable* with respect to testers $\{\mathbf{D_n}\}_n$ if there exists a constant $\alpha > 0$ such that for all n we have $\rho^{\mathbf{D_n}}(C_n) \geq \alpha$.

3 Main Results

We start from defining central notions in this paper, called semi LTCs (sLTCs) and strong sLTCs. Then we define our suggested tester for two-wise tensor products. A notion of semi LTC is a relaxation of a standard LTC in the sense that the rejection criterion is relaxed only to the words that are approximately a fixed distance from the zero codeword.

Definition 3.1 (Semi LTCs and strong semi LTCs)**.** Let $0 < \beta < 1$. We say that a code C is a (q, ϵ, β)-semi LTC if there exists a q-query tester $\mathbf{D}$ such that for all $w \in \mathbf{F}^n$ if $\beta\delta(C)/3 \leq \mathrm{wt}(w) \leq \beta\delta(C)$ then $\mathop{\mathbf{Pr}}_{I \sim \mathbf{D}}[w|_I \notin C|_I] \geq \epsilon$.

We say that a code C is a (q, ϵ, β)-strong sLTC if there exists q-tester $\mathbf{D}$ such that for all $w \in \mathbf{F}^n$ if $\mathrm{wt}(w) \leq \beta\delta(C)$ then $\mathop{\mathbf{Pr}}_{I \sim \mathbf{D}}[w|_I \notin C|_I] \geq \epsilon \cdot \mathrm{wt}(w)$.

Remark 3.2. For every $w \in \mathbf{F}^n$ it holds that $\delta(w, C) \leq \delta(w, 0^n) = \mathrm{wt}(w)$. If $\mathrm{wt}(w) \leq \beta \cdot \delta(C)$ for some $0 < \beta < 1/2$ then $\delta(w, C) = \delta(w, 0^n) = \mathrm{wt}(w)$.

We also notice that sLTCs (strong sLTCs) were defined using the weight of an input word w, while LTCs (strong LTCs) were defined using the distance of w from the code.

Now we present our new tester which plays a crucial role in proving the main theorem (Theorem 3.3), stated in Section 3.1. Our starting point is the *uniform row/column tester* used in all previous works on two-wise tensor codes [27, 10, 17, 13, 7]. We describe this tester for $R \otimes C \subseteq \mathbf{F}^m \otimes \mathbf{F}^n$. For $i \in [n]$ and $j \in [m]$ let the i-row $= \{i\} \times [m]$ and j-column $= [n] \times \{j\}$.

Uniform Row/Column Tester

- flip a coin
- **if** "heads," pick $i \in_U [n]$ and choose i-row;
  else pick $j \in_U [m]$ and choose j-column.

The distribution over the tests of this tester is uniform over rows and columns and does not depend on the structure of the base-codes R, C.

Our suggested tester is a combination of the Uniform Row/Column Tester and the $\mathbf{D_C}$-distribution Tester which depends on the structure of the base code. Our tester for a code $R \otimes C$ picks views that will be $M|_S$ where S is either a row ($\{i\} \times [m]$) or a column ($[n] \times \{i\}$) or a *rectangle* ($\mathrm{supp}(u) \times \{i\}$ for small weight $u \in C^\perp$). To define our suggested tester we assume that the code C has some distribution $\mathbf{D_C}$ over $C^\perp_{\leq q}$. The main place where we use our suggested tester is Theorem 3.3, where we assume that the code C is a (q, ϵ, β)-sLTC (see Definition 3.1) and thus has a "corresponding" distribution $\mathbf{D_C}$ over $C^\perp_{\leq q}$ (see Proposition A.1).

Our suggested tester is defined by two sub-testers, the first sub-tester is the already defined Uniform Row/Column Tester and the second is the $\mathbf{D_C}$-distribution Tester which we define below.

Our Suggested Tester

- flip a coin
- **if** "heads," invoke Uniform Row/Column Tester described above;
  else invoke $\mathbf{D_C}$-distribution Tester (to be defined below).

$\mathbf{D_C}$-distribution Tester

- pick $u \in_{\mathbf{D_C}} C^\perp_{\leq q}$
- flip a coin
- **if** "heads," pick $i \in_U \mathrm{supp}(u)$ and choose i-row;
  else pick $j \in_U [m]$ and choose $\mathrm{supp}(u) \times \{j\}$.

3.1 Main Theorem and its Corollaries

The following theorem is our main technical theorem which shows that the tensor product of a sLTC with another code is robust with respect to our tester.

Theorem 3.3 (Main Theorem)**.** *Let $R \subseteq \mathbf{F}^m$ be a code such that $\delta(R) = \delta_R$ and $C \subseteq \mathbf{F}^n$ be a (q, ϵ, β)-sLTC such that $\delta(C) = \delta_C$ and $\beta \leq \frac{3}{4}$. Let T be our suggested tester (defined in Section 3) for the code $R \otimes C$. Then*

$$\rho^T(R \otimes C) \geq \min\left\{\frac{\beta\delta_C\delta_R}{36}, \frac{\epsilon \cdot \delta_R}{32q^2}\right\}.$$

Notice that the distribution of the tester is over rows, columns and dual words of weight at most q. The proof of Theorem 3.3 is postponed to Section 4.

We use Theorem 3.3 to conclude Corollary 3.4 which states that codes obtained by the tensor product of an LTC with any code is robust with respect to our tester. We note that Corollary 3.4 extends the result of Dinur et al. [13], where a similar result was proved for *uniform LTCs*, i. e., LTCs whose tester queries every bit with the same probability.

Corollary 3.4 (Robust Tensor of LTCs)**.** *Let $R \subseteq \mathbf{F}^m$ be a code such that $\delta(R) = \delta_R$. Let $C \subseteq \mathbf{F}^n$ be a (q, ϵ, δ)-LTC such that $\delta(C) = \delta_C$ and $\delta \leq \frac{\delta_C}{4}$. Let T be our suggested tester (defined in Section 3) for the code $R \otimes C$. Then,*

$$\rho^T(R \otimes C) \geq \min\left\{\frac{\delta\delta_R}{12}, \frac{\epsilon \cdot \delta_R}{32q^2}\right\}.$$

Corollary 3.5 states that the tensor product of an odd expander code with any code is robust with respect to our tester. Notice that even a random regular expander code will be the odd expander code with a high probability, although it is not locally testable (see [3]). Corollary 3.5 extends our previous result, which showed that the tensor product of unique-neighbor expander code and other code is robust (see [7]).

Corollary 3.5 (Robust Tensor of Expanders)**.** *Let $R \subseteq \mathbf{F}^m$ be a code such that $\delta(R) = \delta_R$. Let $C \subseteq \mathbf{F}^n$ be a (c, d, γ, τ)-odd expander code. Let T be our suggested tester (defined in Section 3) for the code $R \otimes C$. Then,*

$$\rho^T(R \otimes C) \geq \frac{\gamma\tau\delta_R}{128d^2}.$$

The proofs of Corollary 3.4 and Corollary 3.5 appear in Section 6. Informally, LTCs and odd expander codes are semi LTCs (see Definition 3.1) and thus by Theorem 3.3 result in robust tensor products.

We show that taking repeated two-wise tensor products of either a strong LTC (Corollary 3.6), or an odd expander code (Corollary 3.8), results in a robustly testable LTC. We stress that Corollary 3.6 and Corollary 3.8 improve upon previous works on two-wise tensor products [13, 7] which only worked when the tensor product was applied *once*. The previous works did not achieve the composition via two-wise tensor products since the properties of the codes they defined were not necessary preserved after the tensor products. In this work we achieve such a composition since we require quite simple property (semi LTCs, see Definition 3.1) and prove that this property is preserved after tensor operation (see Section 5).

Recall that $C^{2^0} = C$ and $C^{2^t} = C^{2^{t-1}} \otimes C^{2^{t-1}}$ for $t > 0$.

Corollary 3.6. *Let $t > 0$ be an integer. Let $C \subseteq \mathbf{F}^n$ be a (q, ϵ)-strong LTC such that $\delta(C) = \delta_C$. Then C^{2^t} is a (q, ϵ')-strong LTC, where*

$$\epsilon' = \left(\frac{\epsilon}{48q^2}\right)^{2t}\left(\frac{\delta_C}{4}\right)^{4\cdot 2^t}$$

Remark 3.7. Let $q, \epsilon, t > 0$ be constants. Assume that $C \subseteq \mathbf{F}^n$ is a (q, ϵ)-strong LTC and $\delta(C) = \Omega(1)$. Then, Corollary 3.6 implies that C^{2^t} is a $(q, \Omega_{\epsilon,q,t}(1))$-strong LTC. Moreover, $\delta(C^{2^t}) = \Omega_t(1)$ and $\mathrm{rate}(C^{2^t}) = (\mathrm{rate}(C))^{2^t} = (\mathrm{rate}(C))^{O_t(1)}$.

Given the fact that rate(C) can be $\frac{1}{n^{O(1)}}$ (see [18, Sections 3 and 5]) we conclude that C^{2^t} is a strong LTC with constant query complexity, constant relative distance and inverse polynomial rate.

Corollary 3.8. *Let $t > 0$ be an integer. Let $C \subseteq \mathbf{F}^n$ be a (c, d, γ, τ)-odd expander code such that $\delta(C) = \delta_C$. Then C^{2^t} is a (n, ϵ')-strong LTC, where*

$$\epsilon' = \frac{\gamma^t \cdot (\tau\delta_C)^{2^{t+1}}}{(96d^2)^t \cdot 8^{t^2}}.$$

Remark 3.9. Let $c, d, \gamma, \tau, t > 0$ be constants. Assume that $C \subseteq \mathbf{F}^n$ is a (c, d, γ, τ)-odd expander code. Then Corollary 3.8 implies that C^{2^t} is a $(n, \Omega_{d,\gamma,\tau,t}(1))$-strong LTC. Moreover, $\delta(C^{2^t}) = \Omega_{t,\tau}(1)$ and rate$(C^{2^t}) = (\text{rate}(C))^{2^t} = (\text{rate}(C))^{O_t(1)}$.

Note that $N = n^{2^t}$ is a blocklength of C^{2^t} and we have that $n = N^{\frac{1}{2^t}}$. Given the fact that rate(C) can be $\Omega(1)$ (see [3]) we conclude that C^{2^t} is a strong LTC with sublinear query complexity, constant relative distance and constant rate.

The proofs of Corollary 3.6 and Corollary 3.8 appear in Section 6.

4 Proof of Main Theorem (Theorem 3.3)

We define Rectangle Tester which will be used in the proof of Theorem 3.3. We start with the definition of rectangle.

Definition 4.1 (Rectangle)**.** Let $S_{rows} \subseteq [n]$, $T_{cols} \subseteq [m]$. We call $S_{rows} \times T_{cols}$ a *rectangle coordinate set* or simply a *rectangle*. For $M \in \mathbf{F}^m \otimes \mathbf{F}^n$ we call $M|_{(S_{rows} \times T_{cols})}$ a *rectangle view*.

The rectangles we will use are of the form $\text{supp}(u) \times [n]$ for $u \in C^\perp$. Now we define Rectangle Tester which picks rectangles as views.

Rectangle Tester

- pick $u \in_{\mathbf{D_C}} C^\perp_{\leq q}$
- choose $Rect = \text{supp}(u) \times [m]$.

Notice that $\mathbf{D_C}$-distribution Tester is equivalent to the invocation of Uniform Row/Column Tester on the view chosen by Rectangle Tester, so the view of our suggested tester will be either row, column or support of dual word of weight at most q.

For every word $M \in \mathbf{F}^n \times \mathbf{F}^m$ we let

$$\rho_{rect}(M) = \mathop{\mathbf{E}}_{u \in_{\mathbf{D_C}} C^\perp_{\leq q}} \left[\delta\left(M|_{\text{supp}(u)\times[m]}, (R \otimes C)|_{\text{supp}(u)\times[m]}\right)\right]$$

be the expected relative local distance of input M obtained by the Rectangle Tester.

Similarly, let $\rho_{uniform}(M)$ be the expected relative local distance of input M obtained by the Uniform Row/Column Tester. Let $\delta_R(M)$ be a relative distance of a typical row of M from R and

$\delta_C(M)$ be a relative distance of a typical column of M from C. Then we have $\rho_{uniform}(M) = \frac{\delta_R(M)+\delta_C(M)}{2}$ since with probability $\frac{1}{2}$ the Uniform Row/Column Tester picks a random row and with probability $\frac{1}{2}$ the Uniform Row/Column Tester picks a random column.

Let $\rho_{\mathbf{D_C}}(M)$ be the expected relative local distance of input M obtained by the $\mathbf{D_C}$-distribution Tester. We let $\rho(M)$ the expected relative local distance of input M obtained by our suggested tester. Then we have

$$\rho(M) = \frac{\rho_{uniform}(M) + \rho_{\mathbf{D_C}}(M)}{2} \tag{4.1}$$

since our suggested tester invokes the Uniform Row/Column tester with probability $\frac{1}{2}$ and with probability $\frac{1}{2}$ our suggested tester invokes the $\mathbf{D_C}$-distribution Tester. From (4.1) we have

$$\rho(M) \geq \frac{1}{2}\rho_{\mathbf{D_C}}(M), \text{ and} \tag{4.2}$$

$$\rho(M) \geq \frac{1}{2}\rho_{uniform}(M) \tag{4.3}$$

4.1 High level overview of Theorem 3.3

Recall that we want to prove that $\rho^T(R \otimes C)$ is lower bounded by a positive constant. To do this we fix any $M \in (\mathbf{F}^m \otimes \mathbf{F}^n) \setminus (R \otimes C)$ and assume the contrary, i.e., that $\rho(M)$ is small and $\delta(M, R \otimes C)$ is large. Then we define the error matrix $E \in \mathbf{F}^m \otimes \mathbf{F}^n$ and prove that $\mathrm{wt}(E) \leq 4\rho(M)$ (Equation (4.6)). The assumption that $\rho(M)$ is small implies that $\mathrm{wt}(E)$ is small. Given this observation, in Proposition 4.4 we prove that $\rho_{\mathbf{D_C}}(M)$ is large. By (4.2) we conclude that $\rho(M)$ must be large. Contradiction.

The proof of Proposition 4.4 will follow from two auxiliary propositions: Proposition 4.2 and Proposition 4.3. Proposition 4.2 shows a surprising relation between the constraints of the code C, the error-matrix E and the input word M. It turns out that if $u^T \cdot E \neq 0$ for some $u \in C^\perp$ then the $M|_{\mathrm{supp}(u)\times[m]}$ will be far from consistent (see Definition 2.5). On the other side, Proposition 4.3 implies that for many $u \in C^\perp_{\leq q}$ we have $u^T \cdot E \neq 0$. Proposition 4.4 uses Proposition 4.2 and Proposition 4.3 to imply that with high probability $\mathbf{D_C}$-distribution Tester will pick a constraint $u \in C^\perp$ such that the rectangle $\mathrm{supp}(u) \times [n]$ of M is far from being consistent. This fact will be used to conclude that with high probability the final local view obtained by $\mathbf{D_C}$-distribution Tester is far from being consistent and thus $\rho_{\mathbf{D_C}}(M)$ is large.

We now present Proposition 4.2, Proposition 4.3 and Proposition 4.4. We prove Proposition 4.2 in Section 4.2, Proposition 4.3 in Section 4.3 and Proposition 4.4 in Section 4.4.

Proposition 4.2. *Let $u \in C^\perp_{\leq q}$ and $S = \mathrm{supp}(u) \times [m]$ be a rectangle coordinate set. If $u^T \cdot E \neq 0$ then $\Delta\left(M|_S, (R \otimes C)|_S\right) \geq \frac{\delta_R m}{2}$.*

Proposition 4.3. $\displaystyle\Pr_{u \in_{\mathbf{D_C}} C^\perp_{\leq q}}\left[u^T \cdot E \neq 0\right] \geq \frac{\epsilon}{2}$.

Proposition 4.2 and Proposition 4.3 will be used to conclude

Proposition 4.4. $\rho_{\mathbf{D_C}}(M) \geq \frac{\epsilon \cdot \delta_R}{16q^2}$.

We are ready to prove Theorem 3.3.

Proof of Theorem 3.3. We have $\frac{1}{36}\beta\delta_C\delta_R < \frac{1}{16}$ because $\beta, \delta_C, \delta_R \leq 1$, so it is sufficient to show that for all $M \in (\mathbf{F}^m \otimes \mathbf{F}^n) \setminus (R \otimes C)$ we have

$$\frac{\rho(M)}{\delta_{R\otimes C}(M)} \geq \min\left\{\frac{\beta\delta_C\delta_R}{36}, \frac{\epsilon\cdot\delta_R}{32q^2}, \frac{1}{16}\right\}$$

Fix $M \in (\mathbf{F}^m \otimes \mathbf{F}^n) \setminus (R \otimes C)$ and denote $\delta_{R\otimes C}(M)$ by $\delta(M)$. If $\frac{\rho(M)}{\delta(M)} \geq \frac{1}{16}$ or $\rho(M) \geq \frac{\beta\delta_C\delta_R}{36}$ we are done since $\delta(M) \leq 1$ and hence $\frac{\rho(M)}{\delta(M)} \geq \min\left\{\frac{\beta\delta_C\delta_R}{36}, \frac{1}{16}\right\}$. Thus in what follows we assume that

$$\rho(M) < \frac{\beta\delta_C\delta_R}{36}, \text{ and} \tag{4.4}$$

$$\delta(M) > 16\rho(M) \tag{4.5}$$

We prove that $\rho(M) \geq \frac{\epsilon\cdot\delta_R}{32q^2}$. Let $\delta^{row}(M) = \delta_{R\otimes\mathbf{F}^n}(M)$ denote the distance of M from the space of matrices whose rows are codewords of R, and define $\delta^{col}(M) = \delta_{\mathbf{F}^m\otimes C}(M)$ similarly. For row $i \in [n]$, let $r^{(i)} \in R$ denote the codeword of R closest to the i-th row of M. For column $j \in [m]$, let $c^{(j)} \in C$ denote the codeword of C closest to the j-th column of M. Let M_R denote the $n \times m$ matrix whose i-th row is $r^{(i)}$, and let M_C denote the matrix whose j-th column is $c^{(j)}$. Let $E = M_R - M_C$.

In what follows the matrices M_R, M_C and (especially) E will be the central objects of attention. We refer to E as the *error matrix*. We use the error matrix E for the analysis of robustness; note that the tester does not obtain a view of E but only of M and of course it is possible that some constraints that are unsatisfied on M are satisfied on E and vice versa.

We know that $\delta(M, M_R) = \delta^{row}(M)$, $\delta(M, M_C) = \delta^{col}(M)$ and $\rho_{uniform}(M) = \frac{\delta^{row}(M)+\delta^{col}(M)}{2}$ because the Uniform Row/Column Tester picks with probability $\frac{1}{2}$ a random row and with probability $\frac{1}{2}$ a random column. Let $\mathrm{wt}(E)$ be the relative weight of E, so

$$\mathrm{wt}(E) = \delta(M_R, M_C) \leq \delta(M, M_R) + \delta(M, M_C) = 2\rho_{uniform}(M) \leq 4\rho(M). \tag{4.6}$$

By (4.4) and (4.6) it follows that

$$\mathrm{wt}(E) < 4 \cdot \frac{1}{36}\beta\delta_C\delta_R = \frac{1}{9}\beta\delta_C\delta_R. \tag{4.7}$$

We want to prove that $\rho(M) \geq \frac{\epsilon\cdot\delta_R}{32q^2}$. It is sufficient to show that $\rho_{\mathbf{D_C}}(M) \geq \frac{\epsilon\cdot\delta_R}{16q^2}$ and then from (4.2) we conclude $\rho(M) \geq \frac{\epsilon\cdot\delta_R}{32q^2}$. Theorem 3.3 follows from Proposition 4.4 by the previous discussions. □

4.2 Proof of Proposition 4.2

Proposition 4.2 is the central observation in the Main Theorem (Theorem 3.3). Recall that we use the error matrix E for the analysis of robustness and that the tester does not obtain a view of E but only of M.

We start from a simple claim that will be crucial in the proof of Proposition 4.2. Recall that $R \subseteq \mathbf{F}^m$ is a linear code such that $\delta(R) = \delta_R$.

Claim 4.5. *Let $w \in \mathbf{F}^m$. If $c_1 \in R$ is a closest codeword of R to w then for all $c_2 \in R \setminus \{c_1\}$ we have $\Delta(w, c_2) \geq \frac{\delta_R m}{2}$.*

Proof. Notice that w can have more than one codeword closest to R. Assume by way of contradiction $\Delta(w, c_2) < \frac{\delta_R \cdot m}{2}$. Since c_1 is a closest codeword to w we have $\Delta(w, c_1) \leq \Delta(w, c_2) < \frac{\delta_R m}{2}$ and so $\Delta(R) \leq \Delta(c_1, c_2) \leq \Delta(w, c_1) + \Delta(w, c_2) < \delta_R m$. Contradiction. □

We notice that $u|_{\text{supp}(u)} \cdot (E|_S) \neq 0$ if and only if $u \cdot (E) \neq 0$. Let $\hat{M}|_S$ be the consistent view that is closest to $M|_S$. There are two cases: either $\hat{M}|_S \neq M_R|_S$ or $\hat{M}|_S = M_R|_S$.

Case 1: $\hat{M}|_S \neq M_R|_S$ so, at least one row i of $\hat{M}|_S$ is not equal to row i of $M_R|_S$, but row i of $\hat{M}|_S$ is a codeword of R because $\hat{M}|_S$ is a consistent view and the row i of $M_R|_S$ is a codeword of R by definition of M_R. Row i of M_R is the closest codeword of R to row i of M, thus according to Claim 4.5 row i of M is at least $\frac{\delta_R m}{2}$ far from row i of $\hat{M}|_S$. So, $\Delta\left(\hat{M}|_S, M|_S\right) \geq \frac{\delta_R m}{2}$.

Case 2: $\hat{M}|_S = M_R|_S$ and thus $M_R|_S$ is the consistent view. We argue that this is impossible and show that $M_R|_S$ will not satisfy constraint u (or formally $u|_{\text{supp}(u)}$).
This is true since $0 \neq u^T \cdot E = u^T \cdot (M_R - M_C) = u^T \cdot M_R - u^T \cdot M_C$, every column of M_C satisfies u and so $u^T \cdot M_C = 0$ and thus $0 \neq u^T \cdot E = u^T \cdot M_R = u^T|_{\text{supp}(u)} \cdot M_R|_S = u^T|_{\text{supp}(u)} \cdot \hat{M}|_S$. Contradiction.

4.3 Proof of Proposition 4.3

We start from auxiliary Proposition 4.6 that will be used later in the proof of Proposition 4.3.

Proposition 4.6. *There exists a rectangle $Rect = A \times B$ such that $A \subseteq [n]$, $\delta_C n/2 \leq |A|$ and $B \subseteq [m]$, $\frac{2}{3}\delta_R m \leq |B|$, and all rows and columns of $E|_{Rect}$ are non-zero and every column c of E indexed by a member of B has $\text{wt}(c) < \frac{1}{3}\beta\delta_C$.*

Proof. Proposition 6 of [13] asserts that under our conditions, M is close to $R \otimes C$. The proof first shows that M_R and M_C are close to $R \otimes C$ and then uses this to estimate the distance of M to $R \otimes C$. We slightly change the proof of [13, Proposition 6] to fit our case.

Claim 4.7. *Assume there exist sets $U \subseteq [m]$ and $V \subseteq [n]$, $|U|/m < \delta_R$ and $|V|/n < \delta_C/2$ such that $M_R(i,j) \neq M_C(i,j)$ implies either $j \in U$ or $i \in V$. Then $\delta(M) \leq 16\rho(M)$.*

Proof. It is sufficient to show that $\delta(M) \leq 8\rho_{uniform}(M)$ since from (4.3) we have $\rho_{uniform}(M) \leq 2\rho(M)$. First we note that there exists a matrix $N \in R \otimes C$ that agrees with M_R and M_C on $\bar{V} \times \bar{U}$ (See [5, Proposition 3]). Recall also that $\delta(M, M_R) = \delta^{row}(M) \leq 2\rho_{uniform}(M)$. So it suffices to show $\delta(M_R, N) \leq 6\rho_{uniform}(M)$. We do so in two steps. First we show that $\delta(M_R, N) \leq 2\rho_{uniform}(M_R)$. We then show that $\rho_{uniform}(M_R) \leq 3\rho_{uniform}(M)$ concluding the proof.

For the first part we start by noting that M_R and N agree on every row in $\bar{V}$. This is the case since both rows are codewords of R which may disagree only on entries from the columns of U, but the number of such columns is less that $\delta_R m$. Next we claim that for every column $j \in [m]$ the closest codeword of C to the j-th column of M_R, is the j-th column of N. This is true since $M_R(i,j) \neq N(i,j)$ implies $i \in V$ and so the number of such i is less than $\delta_C n/2$. Thus for every j, the j-th column of N is the (unique) decoding of the j-th column of M_R. Averaging over j, we get

that $\delta^{col}(M_R) = \delta(M_R, N)$. This yields in turn $\rho_{uniform}(M_R) \geq \delta^{col}(M_R)/2 = \delta(M_R, N)/2$. This gives the first of the two desired inequalities:

$$\delta(M_R, N) \leq 2\rho_{uniform}(M_R) \tag{4.8}$$

Now to bound $\rho_{uniform}(M_R)$, note that for any pair of matrices M_1 and M_2 we have $\rho_{uniform}(M_1) \leq \rho_{uniform}(M_2) + \delta(M_1, M_2)$ because

$$\delta^{row}(M_1) \leq \delta^{row}(M_2) + \delta(M_1, M_2) \quad \text{and} \quad \delta^{col}(M_1) \leq \delta^{col}(M_2) + \delta(M_1, M_2).$$

Thus $\frac{\delta^{row}(M_1)+\delta^{col}(M_1)}{2} \leq \frac{\delta^{row}(M_2)+\delta^{col}(M_2)}{2} + \delta(M_1, M_2)$. Applying this inequality to $M_1 = M_R$ and $M_2 = M$ we get

$$\rho_{uniform}(M_R) \leq \rho_{uniform}(M) + \delta(M_R, M) = \rho_{uniform}(M) + \delta^{row}(M) \leq 3\rho_{uniform}(M). \tag{4.9}$$

This yields the second inequality and thus the proof of the claim. □

Corollary 4.8. *For all $U' \subset [n]$, $V' \subset [m]$ with $|U'| > (1 - \delta_C/2)n$ and $|V'| > (1 - \delta_R)m$ there exists $(i, j) \in U' \times V'$ such that $E(i, j) \neq 0$.*

Proof. Follows from Claim 4.7, since otherwise $\delta(M) \leq 16\rho(M)$ contradicting to (4.5). □

We continue the proof of Proposition 4.6. We say that the column c of E is heavy if $\mathrm{wt}(c) \geq \frac{1}{3}\beta\delta_C$. Let $V \subseteq [m]$ be the set of indices of heavy columns of E, then $|V| < \frac{1}{3}\delta_R m$ because otherwise $\mathrm{wt}(E) \geq \frac{1}{3} \cdot \frac{1}{3}\beta\delta_R\delta_C$ contradicting (4.7), and thus $|\bar{V}| \geq m - \frac{1}{3}\delta_R m$, where $\bar{V} = [m] \setminus V$. Every column c of $E_{[n]\times\bar{V}}$ has $\mathrm{wt}(c) < \frac{1}{3}\beta\delta_C$.

Let $B \subseteq \bar{V}$ be the set of indices of all non zero columns of $E|_{[n]\times\bar{V}}$. Then $|B| \geq \frac{2}{3}\delta_R m$ since otherwise we have $|V| + |B| < \delta_R m$ and we would have a large zero rectangle of E, namely $E|_{[n]\times([m]\setminus(V\cup B))}$, contradicting Corollary 4.8. Let $A \subseteq [n]$ be the set of indices of all non-zero rows of $E|_{[n]\times\bar{V}}$. Then $|A| \geq \delta_C n/2$, since otherwise $E|_{\bar{A}\times\bar{V}}$ would be a large zero rectangle of E in contradiction to Corollary 4.8.

We get that $Rect = A \times B$ is the required rectangle, since all rows and columns of $E_{R'}$ are non-zero and every column c of E indexed by a member of B has $\mathrm{wt}(c) < \frac{1}{3}\beta\delta_C$. □

Recall that C is a (q, ϵ, β)-sLTC, therefore by Proposition A.1 it has a distribution $\mathbf{D_C}$ over $C^{\perp}_{\leq q}$ such that Claim 4.9 holds.

Claim 4.9. *Let $w \in \mathbf{F}^n$ such that $(\beta/3)\delta(C) \leq \mathrm{wt}(w) \leq \beta\delta(C)$. Then, $\Pr_{u\in_{\mathbf{D_C}} C^{\perp}_{\leq q}}[\langle u, w\rangle \neq 0] \geq \frac{\epsilon}{2}$.*

Note that in Claim 4.9 the probability lower bound is $\frac{\epsilon}{2}$ and not ϵ. This occurs because the definition of sLTCs (Definition 2.4) guarantees a corresponding distribution over the small subsets of $[n]$. However, when a distribution over subsets $I \subseteq [n]$, $|I| \leq q$ is transformed to a distribution $\mathbf{D_C}$ over $C^{\perp}_{\leq q}$ the rejection probability might decease by a factor of $\frac{1}{2}$ (see Proposition A.1).

Proof of Proposition 4.3. Let us start from the auxiliary Claim 4.10.

Claim 4.10. *Let $v_1, ..., v_m \in \mathbf{F}^n$ such that $|\bigcup_{1\leq i\leq m}(\mathrm{supp}(v_i))| \geq \alpha n$. Let $v \in \mathbf{F}^n$ be obtained by random linear combination of $v_1, ..., v_m$ over $\mathbf{F}$, i. e., $v = \sum_i a_i \cdot v_i$ where $a_1, ..., a_m \in_U \mathbf{F}$. Then $\mathbf{E}[|\mathrm{supp}(v)|] = \frac{|\mathbf{F}|-1}{|\mathbf{F}|} \cdot \alpha n \geq \frac{\alpha n}{2}$.*

Proof. Straight forward by the linearity of expectation, since random linear combination of $b_1, ..., b_m \in \mathbf{F}$ where not all b_i are zero, results in random element of $\mathbf{F}$ and thus with probability $\frac{|\mathbf{F}|-1}{|\mathbf{F}|}$ produces non-zero element of $\mathbf{F}$. □

We say that the column E_j of E is a light column if $0 < \mathrm{wt}(E_j) \leq \frac{1}{3}\beta\delta_C$. Recall that Rectangle Tester obtains views $M|_{\mathrm{supp}(u)\times[n]}$ for $u \in C^{\perp}_{\leq q}$. By Proposition 4.6 there exists non-zero rectangle $A \times B$ of E, namely $E|_{A\times B}$, such that for every column E_i of E indexed by a member of B it holds that E_i is a light column. We argue that $\underset{u\in_{\mathbf{D_C}} C^{\perp}_{\leq q}}{\mathbf{Pr}}[u \cdot E \neq 0] \geq \epsilon$. It is sufficient to show that there exists a linear combination of columns of E, call it E_{res}, such that $\underset{u\in_{\mathbf{D_C}} C^{\perp}_{\leq q}}{\mathbf{Pr}}[\langle u, E_{res}\rangle \neq 0] \geq \epsilon$ because if $\langle u, E_{res}\rangle \neq 0$ then $u^T \cdot E \neq 0$ since for at least one column E_j of E we have $\langle u, E_j\rangle \neq 0$.

Let $LightCols = \{E_1, ..., E_k\}$ be a set of all columns of E indexed by B, note they all are light columns. It holds that $|\bigcup_{E_j\in LightCols}(\mathrm{supp}(E_j))| \geq \delta_C n/2$ because by Proposition 4.6 every row of $E|_{A\times B}$ is non-zero and $|A| \geq \delta_C n/2$. Throw them (E_j) one by one from $LightCols$ reducing their total support $(\bigcup_{E_j\in LightCols}(\mathrm{supp}(E_j)))$, finally obtain set $(LightCols')$ of total support between $(\frac{2}{3})\beta\delta_C n$ and $\beta\delta_C n$, i. e., $\frac{2}{3}\beta\delta_C n \leq |\bigcup_{E_j\in LightCols}(\mathrm{supp}(E_j))| \leq \beta\delta_C n$. By Claim 4.10 there exists a linear combination (over $\mathbf{F}$) of $\{E_j \in LightCols'\}$, call it E_{res}, such that $\mathrm{wt}(E_{res}) \geq (\frac{1}{3})\beta\delta_C$. Moreover, $\mathrm{wt}(E_{res}) \leq \beta\delta_C$ because $|\bigcup_{E_j\in LightCols}(\mathrm{supp}(E_j))| \leq \beta\delta_C$.

By Claim 4.9 it holds that $\underset{u\in_{\mathbf{D_C}}}{\mathbf{Pr}}[\langle u, E_{res}\rangle \neq 0] \geq \frac{\epsilon}{2}$. But we know that if $\langle u, E_{res}\rangle \neq 0$ then $u^T \cdot E \neq 0$. We conclude $\underset{u\in_{\mathbf{D_C}}}{\mathbf{Pr}}\left[u^T \cdot E \neq 0\right] \geq \frac{\epsilon}{2}$. □

4.4 Proof of Proposition 4.4

We proceed as follows. We first show in Proposition 4.11 that $\rho_{rect}(M) \geq \frac{\epsilon\cdot\delta_R}{4q}$. Next we show auxiliary immediate Proposition 4.12. We then show in Proposition 4.13 that if $\rho_{rect}(M) \geq \alpha$ then $\rho_{\mathbf{D_C}}(M) \geq \frac{\alpha}{4q}$. Finally we conclude that $\rho_{\mathbf{D_C}}(M) \geq \frac{\epsilon\cdot\delta_R}{16q^2}$.

Proposition 4.11. $\rho_{rect}(M) \geq \frac{\epsilon\delta_R}{4q}$.

Proof. By Proposition 4.3 we have $\underset{u\in_{\mathbf{D_C}} C^{\perp}_{\leq q}}{\mathbf{Pr}}\left[u^T \cdot E \neq 0\right] \geq \frac{\epsilon}{2}$. By Proposition 4.2 whenever $u^T \cdot E \neq 0$ it holds that $\Delta\left(M|_{\mathrm{supp}(u)\times[m]}, (R \otimes C)|_{\mathrm{supp}(u)\times[m]}\right) \geq \delta_R m/2$. Hence, the expected distance of the view chosen by Rectangle Tester from a consistent view is at least $\frac{\epsilon}{2} \cdot \frac{\delta_R m}{2}$, i. e.,

$$\underset{u\in_{\mathbf{D_C}} C^{\perp}_{\leq q}}{\mathbf{E}}\left[\Delta\left(M|_{\mathrm{supp}(u)\times[m]}, (R \otimes C)|_{\mathrm{supp}(u)\times[m]}\right)\right] \geq \frac{\epsilon}{2} \cdot \frac{\delta_R m}{2}.$$

For any $u \in C^{\perp}_{\leq q}$ we have $|\mathrm{supp}(u) \times [m]| \leq qm$. So,

$$\rho_{rect}(M) = \underset{u\in_{\mathbf{D_C}} C^{\perp}_{\leq q}}{\mathbf{E}}\left[\delta\left(M|_{\mathrm{supp}(u)\times[m]}, (R \otimes C)|_{\mathrm{supp}(u)\times[m]}\right)\right] \geq \frac{\frac{\epsilon}{2} \cdot \frac{\delta_R m}{2}}{qm} = \frac{\epsilon\delta_R}{4q}.$$

□

Proposition 4.12. *Let $u \in C^{\perp}_{\leq q}$, $j \in [m]$ such that $\langle u|_{\mathrm{supp}(u)}, M|_{\mathrm{supp}(u)\times\{j\}}\rangle \neq 0$. Then,*

$$\delta(M|_{\mathrm{supp}(u)\times\{j\}}, C|_{\mathrm{supp}(u)}) \geq \frac{1}{q}.$$

Proof. This is true since $|\{\mathrm{supp}(u)\times\{j\}\}| \leq q$ and $M|_{\mathrm{supp}(u)\times\{j\}} \notin C|_{\mathrm{supp}(u)}$ so at least one entry of $M|_{\mathrm{supp}(u)\times\{j\}}$ should be changed in order to be in $C|_{\mathrm{supp}(u)}$. □

Proposition 4.13. *If $\rho_{rect}(M) \geq \alpha$ then $\rho_{\mathbf{D_C}}(M) \geq \frac{\alpha}{4q}$.*

Note that Proposition 4.11 and Proposition 4.13 imply $\rho_{\mathbf{D_C}}(M) \geq \epsilon \cdot \frac{\delta_R n}{16q^2}$.

Proof of Proposition 4.13. Notice that $\Delta(M|_S, (R\otimes C)|_S) \geq \alpha|\,\mathrm{supp}(u)|m$ because $|S| = |\,\mathrm{supp}(u)|m$. Note that $(M|_S)|_{\{i\}\times[m]} = M|_{\{i\}\times[m]}$ and $(M_R|_S)|_{\{i\}\times[m]} = M_R|_{\{i\}\times[m]}$. For $i \in \mathrm{supp}(u)$ let $RowDiff_i = (M|_{\{i\}\times[m]} - M_R|_{\{i\}\times[m]}$ be the i-row difference between M and the closest consistent row (i-row of M_R). Note that $|\,\mathrm{wt}(RowDiff_i)| = \delta(M|_{\{i\}\times[m]}, R)$.

Note that $\delta(M|_S, M_R|_S)$ shows the expected relative distance of the random row of $M|_S$ from R. If $\delta(M|_S, M_R|_S) \geq \frac{\alpha}{2q}$ we are done since with probability 1/2 Uniform Row/Column Tester (think of the testing $M|_S$) will choose a random row of $M|_S$ and thus $\rho_{uniform}(M|_S) \geq \frac{\alpha}{4q}$ that finishes the proof. Thus we assume that $\delta(M|_S, M_R|_S) < \frac{\alpha}{2q}$.

Let $Bad_r = \bigcup_{i\in\mathrm{supp}(u)}(\mathrm{supp}(RowDiff_i))$ be union of all differences. We have $|Bad_r| < \frac{\alpha|\,\mathrm{supp}(u)|m}{2q} \leq \frac{\alpha m}{2}$ since otherwise $\delta(M|_S, M_R|_S) \geq \frac{\alpha}{2q}$. Let Bad_c be all non-consistent columns of $M|_S$, i. e., $j \in Bad_c$ if and only if $M|_{\mathrm{supp}(u)\times\{j\}} \notin C|_{\mathrm{supp}(u)}$. If $|Bad_c| \geq \frac{\alpha m}{2}$ we are done since with probability 1/2 Uniform Row/Column Tester (think of the testing $M|_S$) will choose a random column of $M|_S$ and thus with probability at least $\frac{1}{2}\cdot\frac{\alpha}{2}$ the tester will pick non-consistent column of $M|_S$ (which does not belong to $C|_{\mathrm{supp}(u)}$) of size $|\,\mathrm{supp}(u)|$. Thus by Proposition 4.12 we have $\rho_{uniform}(M|_S) \geq \frac{\alpha}{4q}$. Hence we assume that $|Bad_c| < \frac{\alpha m}{2}$ and $|Bad_r| < \frac{\alpha m}{2}$ and show the contradiction.

We know that every row of $M|_{S\setminus(\mathrm{supp}(u)\times(Bad_r\cup Bad_c))}$ belongs to $R|_{[m]\setminus(Bad_r\cup Bad_c)}$ and every column of $M|_{S\setminus(\mathrm{supp}(u)\times(Bad_r\cup Bad_c))}$ belongs to $C|_{\mathrm{supp}(u)}$. Proposition B.2 implies that $M|_{S\setminus(\mathrm{supp}(u)\times(Bad_r\cup Bad_c))} \in (R\otimes C)|_{S\setminus(\mathrm{supp}(u)\times(Bad_r\cup Bad_c))}$.

We have $|Bad_r \cup Bad_c| < \alpha m$ and thus $|(\mathrm{supp}(u)\times(Bad_r\cup Bad_c))| < \alpha|\,\mathrm{supp}(u)|m$. Projecting $(\mathrm{supp}(u)\times(Bad_r\cup Bad_c))$ out we obtain the consistent view $(M|_{S\setminus(\mathrm{supp}(u)\times(Bad_r\cup Bad_c))})$ (by Proposition B.2) and thus $\Delta(M|_S, (R\otimes C)|_S) < \alpha|\,\mathrm{supp}(u)|m$. Contradiction. □

Thus by Proposition 4.13 we have that if $\rho_{rect}(M) \geq \alpha$ then $\rho_{\mathbf{D_C}}(M) \geq \frac{\alpha}{4q}$. But by Proposition 4.11 we have that $\rho_{rect}(M) \geq \frac{\epsilon\cdot\delta_R}{4q}$. We conclude that $\rho_{\mathbf{D_C}}(M) \geq \epsilon\cdot\frac{\delta_R}{16q^2}$.

5 Strong sLTC property is preserved after tensor operation

In this section we show that strong sLTC property is preserved after tensor operation.

Proposition 5.1. *Let $R \subseteq \mathbf{F}^m$ be a $(q_1, \epsilon_1, \beta_1)$-strong sLTC and $C \subseteq \mathbf{F}^n$ be a $(q_2, \epsilon_2, \beta_2)$-strong sLTC. Then $R\otimes C$ is a (q, ϵ, β)-strong sLTC where $q = \max\{q_1, q_2\}$, $\epsilon = \frac{3}{8}\min\{\epsilon_1, \epsilon_2\}$ and $\beta = \frac{\beta_1\cdot\beta_2}{4}$.*

Proof. Let $\delta_R = \delta(R)$, $\delta_C = \delta(C)$ and then $\delta(R\otimes C) = \delta_R\delta_C$. Let $\mathbf{D_R}$ and $\mathbf{D_C}$ be the testers (distributions) for R and C respectively. We define a q-tester $T_{R\otimes C}$ (distribution $\mathbf{D_{R\otimes C}}$) as follows

- flip a coin
- **if** "heads," pick $i \in_U [n]$ and invoke T_R on i-row;
  else pick $j \in_U [m]$ and invoke T_C on j-column.

This tester has query complexity at most $q = \max\{q_1, q_2\}$. Let $M \in \mathbf{F}^n \times \mathbf{F}^m$. We say that a row r of M is a heavy row if $\mathrm{wt}(r) > \beta_1 \delta_R$ and a column c of M is heavy column if $\mathrm{wt}(c) > \beta_2 \delta_C$, otherwise we say that r (c) is a light row (column). Notice that if $M|_{\{i\}\times[m]}$ is a light row then

$$\Pr_{I \sim \mathbf{D_R}} \left[(M_{\{i\}\times[m]})|_I \notin R|_I \right] \geq \mathrm{wt}(M|_{\{i\}\times[m]}) \cdot \epsilon_1$$

and if $M|_{[n]\times\{j\}}$ is a light column then

$$\Pr_{I \sim \mathbf{D_C}} \left[(M|_{[n]\times\{j\}})|_I \notin C|_I \right] \geq \mathrm{wt}(M|_{[n]\times\{j\}}) \cdot \epsilon_2.$$

We show that if $\mathrm{wt}(M) \leq \beta \cdot \delta(R \otimes C) = \beta \cdot \delta_R \delta_C$ then

$$\Pr_{I \sim \mathbf{D_{R\otimes C}}} [M|_I \notin (R \otimes C)|_I] \geq \epsilon \cdot \mathrm{wt}(M).$$

Let $W = \mathrm{wt}(M)$ and $\epsilon' = \min\{\epsilon_1, \epsilon_2\}$. We assume that $W \leq \beta \delta_R \delta_C$.

We notice that if there exists $S \subseteq [n]\times[m]$, $\alpha = \frac{|S|}{nm}$ such that for all $(i,j) \in S$ we have $M_{(i,j)} \neq 0$ and either $M|_{\{i\}\times[m]}$ is a light row or $M|_{[n]\times\{j\}}$ is a light column, then

$$\Pr_{I \sim \mathbf{D_{R\otimes C}}} [M|_I \notin (R \otimes C)|_I] \geq \frac{\epsilon' \alpha}{2}.$$

To see this, let

$$\alpha_1 = \frac{\left|\left\{(i,j) \in S \mid M|_{\{i\}\times[m]} \text{ is a light row and } M_{(i,j)} \neq 0\right\}\right|}{nm}, \text{ and}$$

$$\alpha_2 = \frac{\left|\left\{(i,j) \in S \mid M|_{[n]\times\{j\}} \text{ is a light column and } M_{(i,j)} \neq 0\right\}\right|}{nm}.$$

We have $\alpha_1 + \alpha_2 \geq \alpha$. It holds that

$$\Pr_{i \in_U [n], I \sim \mathbf{D_R}} \left[(M|_{\{i\}\times[m]})|_I \notin R|_I \right] \geq \epsilon' \alpha_1 \quad \text{and} \quad \Pr_{j \in_U [m], I \sim \mathbf{D_C}} \left[(M|_{[n]\times\{j\}})|_I \notin C|_I \right] \geq \epsilon' \alpha_2.$$

The explanation of two above inequalities is simple. In the worst case, every light row $M|_{\{i\}\times[m]}$ of M is chosen with probability $\frac{1}{n}$, and given that it was chosen, it is "rejected" by $\mathbf{D_R}$ with probability at least $\epsilon' \cdot \frac{|\mathrm{supp}(M|_{\{i\}\times[m]})|}{m}$. I.e., every non-zero element of a light row contributes $\frac{\epsilon'}{mn}$ to the rejection probability over rows $\left(\mathbf{Pr}_{i \in_U [n], I \sim \mathbf{D_R}} \left[(M|_{\{i\}\times[m]})|_I \notin R|_I \right]\right)$. Since $\alpha_1 \cdot (mn)$ is a number of all non-zero symbols in the light rows the first inequality follows. The intuition behind the second inequality is similar.

So,

$$\Pr_{I \sim \mathbf{D_{R\otimes C}}} [M|_I \notin (R \otimes C)|_I] \geq \frac{\epsilon' \cdot \alpha_1}{2} + \frac{\epsilon' \cdot \alpha_2}{2} \geq \frac{\epsilon' \alpha}{2}.$$

Thus it is sufficient to show that there exists S such that $|S| \geq \frac{3}{4}W$. Let r be a fraction of heavy rows of M and let c be a fraction of heavy columns of M. We know that $r\beta_1\delta_R \leq W$ and $c\beta_2\delta_C \leq W$. So,

$$r \cdot c \leq \frac{W^2}{\beta_1\delta_R\beta_2\delta_C} = \frac{W}{\beta_1\delta_R\beta_2\delta_C} \cdot W \leq \frac{1}{4}W,$$

where the last inequality holds since by assumption $W \leq \beta\delta_R\delta_C = \frac{\beta_1\cdot\beta_2}{4}\delta_R\delta_C$. Hence $\alpha \geq \mathrm{wt}(M) - r \cdot c = W - r \cdot c \geq \frac{3}{4}W$ since $\left|\left\{(i,j) \mid M_{(i,j)} \neq 0 \text{ and } (i,j) \notin S\right\}\right| =$

$$\left|\left\{(i,j) \mid \text{row } i \text{ and column } j \text{ of } M \text{ are heavy and } \ M_{(i,j)} \neq 0\right\}\right| \leq (r \cdot c) \cdot (mn).$$

Thus

$$\Pr_{I\sim\mathbf{D}_{\mathbf{R}\otimes\mathbf{C}}}[M|_I \notin (R \otimes C)|_I] \geq \frac{3\epsilon'}{8} \cdot \mathrm{wt}(M) = \frac{3}{8}\min\{\epsilon_1, \epsilon_2\} \cdot \mathrm{wt}(M).$$

□

Proposition 5.2 immediately follows from Proposition 5.1.

Proposition 5.2. *Let $t > 0$ be an integer. Let C be a $[n,k,d]$ code, which is a (q,ϵ,β)-strong sLTC. Then C^{2^t} is a $[n^{2^t},k^{2^t},d^{2^t}]$ code and a $\left(q,(\frac{3}{8})^t\epsilon,\frac{\beta^{2^t}}{4^{2^t+1}}\right)$-strong sLTC.*

Proof. We prove by induction on $i = 1 \ldots t$ that C^{2^t} is a $[n^{2^t},k^{2^t},d^{2^t}]$ code and a $\left(q,(\frac{3}{8})^t\epsilon,\frac{\beta^{2^t}}{4^{2^t+2^{t-1}+\ldots+2^1}}\right)$-strong sLTC. Since $4^{2^t+2^{t-1}+\ldots+2^1} \leq 4^{2^{t+1}}$ this completes the proof of the Proposition.

We know that C is a $[n,k,d]$ code, which is a (q,ϵ,β)-strong sLTC. Assume C^{2^i} is a $[n^{2^i},k^{2^i},d^{2^i}]$ code, which is a $\left(q,(\frac{3}{8})^i\epsilon,\frac{\beta^{2^i}}{4^{2^i+\ldots+2^1}}\right)$-strong sLTC. Then $C^{2^{i+1}}$ is a $[n^{2^{i+1}},k^{2^{i+1}},d^{2^{i+1}}]$. Furthermore, by Proposition 5.1 $C^{2^{i+1}}$ is a $\left(q,(\frac{3}{8})^{i+1}\epsilon,\frac{\beta^{2^{i+1}}}{4^{2^{i+1}+2^i+\ldots+2^1}}\right)$-strong sLTC. □

6 Proof of Main Corollaries

We state and prove Proposition 6.1 and Proposition 6.2. The proofs of Corollary 3.4 and Corollary 3.5 will follow from Proposition 6.1, Proposition 6.2 and Theorem 3.3.

Proposition 6.1. *Let $C \subseteq \mathbf{F}^n$ be a code.*

- *If C is a (q,ϵ,δ)-LTC, where $\delta \leq \frac{1}{4}\delta(C)$ then C is a $(q,\epsilon,\frac{3\delta}{\delta(C)})$-sLTC.*
- *If C is a (q,ϵ)-strong LTC. Then C is a $(q,\epsilon,\frac{1}{2})$-strong sLTC.*
- *If C is a (q,ϵ,β)-strong sLTC. Then C is a $\left(q,\frac{\epsilon\beta\delta(C)}{3},\beta\right)$-sLTC.*

Proof. For the first bullet, let $\mathbf{D}$ be a distribution over q-tests of C such that for all $w \in \mathbf{F}^n$ if $\delta(w,C) \geq \delta$ then $\Pr_{I\sim\mathbf{D}}[w|_I \notin C|_I] \geq \epsilon$. So, if $\delta = \frac{1}{3}\frac{3\delta}{\delta(C)}\delta(C) \leq \mathrm{wt}(w) \leq \frac{3\delta}{\delta(C)}\delta(C) \leq \frac{3}{4}\delta(C)$ then $\delta(w,C) \geq \delta$. Therefore $\Pr_{I\sim\mathbf{D}}[w|_I \notin C|_I] \geq \epsilon$.

For the second bullet, let $\mathbf{D}$ be a distribution over q-tests of C such that for all $w \in \mathbf{F}^n$ we have $\Pr_{I\sim\mathbf{D}}[w|_I \notin C|_I] \geq \epsilon \cdot \delta(w, C)$. If $0 < \mathrm{wt}(w) \leq \frac{1}{2}\delta(C)$ then $\Pr_{I\sim\mathbf{D}}[w|_I \notin C|_I] \geq \epsilon \cdot \delta(w, C) = \epsilon \cdot \mathrm{wt}(w)$.

For the third bullet, let $\mathbf{D}$ be a distribution of C such that for all $w \in \mathbf{F}^n$ if $\mathrm{wt}(w) \leq \beta\delta(C)$ then $\Pr_{I\sim\mathbf{D}}[w|_I \notin C|_I] \geq \epsilon \cdot \mathrm{wt}(w)$. Then if $(\beta/3)\delta(C) \leq \mathrm{wt}(w) \leq \beta\delta(C)$ it holds that $\Pr_{I\sim\mathbf{D}}[w|_I \notin C|_I] \geq \epsilon\,\mathrm{wt}(w) \geq \dfrac{\epsilon\beta\delta(C)}{3}$. □

Proposition 6.2 shows that odd expander codes are strong sLTCs.

Proposition 6.2 (Odd Expander Codes are strong sLTCs)**.** *Let $C \subseteq \mathbf{F}_2^n$ be a (c, d, γ, τ)-odd expander code. Then $\delta(C) \geq \tau$, C is a $(d, \frac{\gamma\tau}{3}, \frac{\tau}{\delta(C)})$-sLTC and a $(d, \gamma, \frac{\tau}{\delta(C)})$-strong sLTC.*

Proof. By definition, C has the parity check graph $G = ([n], S, E)$ which is a (c, d, γ, τ)-odd expander, where $S \subseteq C^{\perp}_{\leq d}$ and S is also associated to the vertex subset. First note that for every $w \in \mathbf{F}_2^n \backslash 0^n$ such that $\mathrm{wt}(w) \leq \tau$ there exists a constraint $u \in S \subseteq C^{\perp}_{\leq d}$ such that $|\mathrm{supp}(w) \cap \mathrm{supp}(u)|$ is odd and thus $\langle u, w\rangle \neq 0$ and $w \notin C$. This implies that $\delta(C) \geq \tau$.

We argue that C is a $(d, \gamma, \frac{\tau}{\delta(C)})$-strong sLTC and conclude by Proposition 6.1 that C is a $(d, \frac{\gamma\tau}{3}, \frac{\tau}{\delta(C)})$-sLTC. Let $\mathbf{D}$ to be a uniform distribution over S and let $w \in \mathbf{F}_2^n$ be a word such that $\mathrm{wt}(w) \leq \tau = \frac{\tau}{\delta(C)} \cdot \delta(C)$. Note that $N^{odd}(\mathrm{supp}(w)) = \{u \in S \mid \langle u, w\rangle \neq 0\}$ since $\langle u, w\rangle \neq 0$ iff $u \in N^{odd}(\mathrm{supp}(w))$. Then,

$$\Pr_{I\sim\mathbf{D}}[w|_I \notin C|_I] \geq \frac{\left|N^{odd}(\mathrm{supp}(w))\right|}{|S|} \geq \frac{|\mathrm{supp}(w)|c \cdot \gamma}{cn} = \mathrm{wt}(w) \cdot \gamma \geq \delta(w, C) \cdot \gamma,$$

where we used the facts that $|S| \leq cn$ and $\mathrm{wt}(w) = \delta(w, 0^n) \geq \delta(w, C)$ since $0^n \in C$. □

We are ready to prove Corollary 3.4 and Corollary 3.5.

Proof of Corollary 3.4. By Proposition 6.1 we know that C is a $(q, \epsilon, \frac{3\delta}{\delta(C)})$-sLTC. By Theorem 3.3

$$\rho^T(R \otimes C) \geq \min\left\{\frac{\left(\frac{3\delta}{\delta(C)}\right)\delta_C\delta_R}{36}, \frac{\epsilon \cdot \delta_R}{32q^2}\right\} = \min\left\{\frac{3\delta\delta_R}{36}, \frac{\epsilon \cdot \delta_R}{32q^2}\right\}.$$

□

Proof of Corollary 3.5. C is a $(c, d, \gamma, \frac{3}{4}\tau)$-odd expander code and by Proposition 6.2 $\delta(C) \geq \tau$ and thus $\frac{\frac{3}{4}\tau}{\delta(C)} \leq \frac{3}{4}$. By Proposition 6.2 we know that C is a $(d, \gamma\tau/4, \frac{3\tau}{4\delta(C)} \leq \frac{3}{4})$-sLTC. By Theorem 3.3

$$\rho^T(R \otimes C) \geq \min\left\{\frac{\frac{0.75\tau}{\delta(C)}\delta(C)\delta_R}{36}, \frac{(\gamma\tau/4) \cdot \delta_R}{32d^2}\right\} \geq \frac{\gamma\tau\delta_R}{128d^2}$$

where the last inequality holds since $d \geq 1$ and $\gamma \leq 1$. □

In the rest of the section we prove Corollary 3.6 and Corollary 3.8. Before starting the proofs let us explain how the testers, and in particular, our suggested testers can be composed.

6.1 Composition of Testers

We describe how the testers can be composed to define a new (composed) tester. Suppose we want to test $C \subseteq \mathbf{F}^J$.

Let $\mathbf{D_{out}}$ be a tester (i. e., a distribution over $I \subseteq J$) for the code C. For all $I \subseteq J$, $\mathbf{D_{out}}(I) > 0$ let $\mathbf{D^I_{in}}$ be a tester on $\mathbf{F}^I$, i. e., a distribution over $I' \subseteq I$.

Definition 6.3 (Composed Tester)**.** The composed tester for the code C is the distribution $\mathbf{D_{comp}}$ over $\mathbf{F}^J$ where

$$\mathbf{D_{comp}}(I') = \sum_{I \subseteq J} \mathbf{D_{out}}(I) \cdot \mathbf{D^I_{in}}(I').$$

Let the composed tester (distribution $\mathbf{D_{comp}}$) be defined as above from the distributions $\mathbf{D_{out}}$) and $\mathbf{D^I_{in}}$.

Proposition 6.4. *If for all $I \subseteq J$ such that $\mathbf{D_{out}}(I) > 0$ it holds that $\rho^{\mathbf{D^I_{in}}}(C|_I) \geq \rho_{in}$ then*

$$\rho^{\mathbf{D_{comp}}}(C) \geq \rho^{\mathbf{D_{out}}}(C) \cdot \rho_{in}$$

Proof. This holds because

$$\rho^{\mathbf{D_{comp}}}(w) = \mathop{\mathbf{E}}_{I' \sim \mathbf{D_{comp}}} [\delta(w|_{I'}, C|_{I'})] = \mathop{\mathbf{E}}_{I \sim \mathbf{D_{out}}} \left[\mathop{\mathbf{E}}_{I' \sim \mathbf{D^I_{in}}} [\delta(w|_{I'}, C|_{I'})] \right] \geq \delta(w, C) \cdot \rho^{\mathbf{D_{out}}} \cdot \rho_{in}$$

□

Example: Composition of Tensor Codes

Let $C_0 = C \subseteq \mathbf{F}^J$ be a code with a q-query tester $\mathbf{D_0}$ with robustness $\rho^{\mathbf{D_0}}(C_0)$. Let $C_i = C^{2^i}$ for $i \geq 0$. Let $J_0 = J$ and $J_i = J_{i-1} \times J_{i-1}$. Then $C_i \subseteq \mathbf{F}^{J_i}$ for all $i \geq 0$. For $j = 1...m$ let and $\mathbf{D_j}$ be a uniform row/column tester of C_j with robustness $\rho^{\mathbf{D_j}}(C_j)$.

Let $\mathbf{D'_1} = \mathbf{D_1}$ and $\mathbf{D'_j}$ be the composed tester of $\mathbf{D_j}$ and $\mathbf{D'_{j-1}}$. For all j it holds that D'_j has query complexity q. Moreover by Proposition 6.4 we have $\rho^{\mathbf{D'_1}}(C_1) = \rho^{\mathbf{D_1}}(C_1)$ and $\rho^{\mathbf{D'_j}}(C_j) \geq \rho^{\mathbf{D_j}}(C_j) \cdot \rho^{\mathbf{D'_{j-1}}}(C_{j-1}) \geq \rho^{\mathbf{D_1}}(C_1) \cdot \ldots \cdot \rho^{\mathbf{D_j}}(C_j)$.

Composition of our suggested testers. Assume $C \subseteq \mathbf{F}^n$ is a (q, ϵ, β)-strong sLTC code, $C^2 = C \otimes C$ and $C^4 = C^2 \otimes C^2$. So, by Proposition 5.2 C^2 and C^4 are also strong sLTCs with corresponding q-query testers (distributions). Let $\mathbf{D_2}$ be our suggested tester for C^2 and $\mathbf{D_4}$ be our suggested tester for C^4. Suppose we are given a word M and we want to test its membership to C^4. In order to test whether $M \in C^4$ we invoke our suggested tester $\mathbf{D_4}$, which chooses either a row of M or a column of M or support of some u, where $u \in (C^2)^\perp_{\leq q}$.

If support of some u, where $u \in (C^2)^\perp_{\leq q}$ was chosen we will check whether $M|_{\mathrm{supp}(u)} \in C^4|_{\mathrm{supp}(u)}$ (note that $|\mathrm{supp}(u)| \leq q$ resulting in query complexity at most q) and thus we are done.

Otherwise, either a row of M or a column of M was chosen by our suggested tester $\mathbf{D_4}$, and, we assume without loss of generality that it was a row r of M. But then we need to test a membership of r to C^2. Now, we can invoke $\mathbf{D_2}$ which in turn will select either a row of r or a column of r or support of some u', where $u' \in C^\perp_{\leq q}$. If support of some u', where $u' \in C^\perp_{\leq q}$ was chosen then,

similarly, we read at most q entries and we are done. Otherwise we get either a selected row of r or a selected column of r, and the selected row (column) of r can be tested to a membership to C. The robustness of $\mathbf{D_2}$ and $\mathbf{D_4}$ implies that if $\delta(M, C^4) \geq \alpha$ then the expected distance of the finally obtained view from C is $\Omega(\alpha)$.

If C is a strong LTC we know how to test the finally obtained view to a membership to C (with query complexity q) but if C is an expander code we simply read all the entries of the selected row (column) of r, which gives query complexity n.

Notice first of all that in the above example two testers $\mathbf{D_2}$ and $\mathbf{D_4}$ were composed and gave us a tester for C^4 with query complexity at most n where the blocklength of C^4 is n^4, i. e., query complexity of the composed tester is at most (blocklength)$^{1/4}$.

Finally, note that if C is a (q, ϵ)-strong LTC then we have a tester for C^4 with query complexity q. And if C is an odd expander code then we have a tester for C^4 with query complexity n.

Proof of Corollary 3.6. C is a $(q, \epsilon, \frac{1}{2})$-strong sLTC by Proposition 6.1. Let $j > 0$ be an integer, then $\delta(C^{2^j}) = \delta_C^{2^j}$ and C^{2^j} is a $\left(q, (\frac{3}{8})^j \epsilon, \frac{1}{2^{2^j} \cdot 4^j}\right)$-strong sLTC by Proposition 5.2.

Thus by Proposition 6.1 C^{2^j} is a $\left(q, \left(\frac{3}{8}\right)^j \epsilon \cdot \frac{\delta_C^{2^j}}{3 \cdot 4^j \cdot 2^{2^j}}, \frac{1}{4^j \cdot 2^{2^j}}\right)$-sLTC. Since C is a (q, ϵ)-strong LTC it has a q-query tester (distribution) $\mathbf{D_C}$ over $C^\perp_{\leq q}$ (see Corollary A.1). Let $\mathbf{D_{2^j}}$ be our suggested tester (distribution) for $C^{2^j} \otimes C^{2^j}$, then by Theorem 3.3

$$\rho^{\mathbf{D_{2^j}}}(C^{2^j}) \geq \min\left\{\frac{1}{36}\frac{1}{4^j \cdot 2^{2^j}}\delta_C^{2^{j+1}}, \frac{\delta_C^{2^j}}{32q^2}\left(\frac{3}{8}\right)^j \epsilon \cdot \frac{(\frac{\delta_C}{2})^{2^j}}{3 \cdot 4^j}\right\} \geq \frac{\epsilon}{48q^2}\frac{1}{2^{2^j}}\frac{1}{4^{2^j}}\delta_C^{2^{j+1}} \geq \frac{\epsilon}{48q^2}\left(\frac{\delta_C}{4}\right)^{2^{j+1}}$$

So, letting $\mathbf{D_{comp}}$ be the composed n-query tester of $\mathbf{D_1}, ..., \mathbf{D_{2^t}}$ (see Definition 6.3) we get by Proposition 6.4 that $\rho^{\mathbf{D_{comp}}}(C^{2^t}) \geq \left(\frac{\epsilon}{48q^2}\right)^{2t}\left(\frac{\delta_C}{4}\right)^{4 \cdot 2^t}$. Thus letting $\mathbf{D_{final}}$ be a composed q-query tester of $\mathbf{D_C}$ and $\mathbf{D_{comp}}$ we get that if $\delta(w, C^{2^t}) = \delta$ it holds that $\Pr_{I \sim \mathbf{D_{final}}}[w|_I \notin C|_I] \geq \delta \cdot \left(\frac{\epsilon}{48q^2}\right)^{2t}\left(\frac{\delta_C}{4}\right)^{4 \cdot 2^t}$. □

We state and prove a simple proposition and then we prove Corollary 3.8.

Proposition 6.5. *If C has a q-query tester $\mathbf{D_C}$ such that $\rho^{\mathbf{D_C}}(C) \geq \epsilon$ then C is a (q, ϵ)-strong LTC.*

Proof. Let $w \in \mathbf{F}^n$ and $\delta = \delta(w, C)$. Assume by way of contradiction that $\Pr_{I \sim \mathbf{D_C}}[w|_I \notin C|_I] < \epsilon \cdot \delta$. For all I it holds that $\delta(w|_I, C|_I) \leq 1$. Thus $\mathop{\mathbf{E}}_{I \sim \mathbf{D_C}}[\delta(w|_I, C|_I)] < 1 \cdot \epsilon \cdot \delta$. But by assumption $\rho^{\mathbf{D_C}}(C) \geq \epsilon$ and thus $\rho^{\mathbf{D_C}}(w) = \mathop{\mathbf{E}}_{I \sim \mathbf{D_C}}[\delta(w|_I, C|_I)] \geq \epsilon \cdot \delta$. Contradiction. □

Proof of Corollary 3.8. C is a $\left(c, d, \gamma, \frac{3}{4}\tau\right)$-odd expander code. By Proposition 6.2 we have $\delta_C \geq \tau$, and thus $\frac{3\tau}{4\delta_C} \leq \frac{3}{4}$. By Proposition 6.2 C is a $\left(d, \gamma, \frac{0.75\tau}{\delta_C}\right)$-strong sLTC.

Let $j > 0$ be an integer. Proposition 5.2 implies that C^{2^j} is a $\left(d, \left(\frac{3}{8}\right)^j \gamma, \frac{(\frac{3\tau}{4\delta_C})^{2^j}}{4^j}\right)$- strong sLTC and Proposition 6.1 implies that C^{2^j} is a $\left(d, (\frac{3}{8})^j \cdot \frac{\gamma\delta_C^{2^j}}{3} \cdot \frac{(\frac{3\tau}{4\delta_C})^{2^j}}{4^j}, \frac{(\frac{3\tau}{4\delta_C})^{2^j}}{4^j}\right)$-sLTC. We know $\delta(C^{2^j}) = \delta_C^{2^j}$.

Let $\mathbf{D_{2^j}}$ be our suggested tester for $C^{2^j} \otimes C^{2^j}$, then by Theorem 3.3

$$\rho^{\mathbf{D_{2^j}}}(C^{2^j}) \geq \min\left\{\frac{1}{36}\frac{(\frac{3\tau}{4\delta_C})^{2^j}}{4^j}\delta_C^{2^{j+1}}, \frac{\delta_C^{2^j}}{32d^2} \cdot (\frac{3}{8})^j \frac{\gamma\delta_C^{2^j}}{3} \cdot \frac{(\frac{3\tau}{4\delta_C})^{2^j}}{4^j}\right\} \geq \frac{\gamma \cdot (0.75\tau\delta_C)^{2^j}}{96d^2}\frac{1}{8^j}$$

Let $\mathbf{D_{comp}}$ be the composed n-query tester (see Definition 6.3) from $\mathbf{D_1}, ..., \mathbf{D_{2^t}}$. Proposition 6.4 implies $\rho^{\mathbf{D_{comp}}}(C^{2^t}) \geq \frac{\gamma^t \cdot (0.75\tau\delta_C)^{2^{t+1}}}{(96d^2)^t \cdot 8^{t^2}}$. By Proposition 6.5 it holds that C^{2^t} is a $\left(n, \frac{\gamma^t \cdot (0.75\tau\delta_C)^{2^{t+1}}}{(96d^2)^t \cdot 8^{t^2}}\right)$-strong LTC. □

Acknowledgements

We thank Prahladh Harsha for helpful discussions. We would like to thank anonymous referees for many invaluable comments.

References

[1] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, "Proof verification and the hardness of approximation problems," *Journal of the ACM*, vol. 45, no. 3, pp. 501–555, May 1998.

[2] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, and S. P. Vadhan, "Robust PCPs of proximity, shorter PCPs, and applications to coding," *SIAM Journal on Computing*, vol. 36, no. 4, pp. 889–974, 2006.

[3] E. Ben-Sasson, P. Harsha, and S. Raskhodnikova, "Some 3CNF Properties Are Hard to Test," *SIAM Journal on Computing*, vol. 35, no. 1, pp. 1–21, 2005. [Online]. Available: http://epubs.siam.org/SICOMP/volume-35/art_44544.html

[4] E. Ben-Sasson and M. Sudan, "Simple PCPs with poly-log rate and query complexity," in *STOC*. ACM, 2005, pp. 266–275. [Online]. Available: http://doi.acm.org/10.1145/1060590.1060631

[5] ——, "Robust locally testable codes and products of codes," *Random Struct. Algorithms*, vol. 28, no. 4, pp. 387–402, 2006. [Online]. Available: http://dx.doi.org/10.1002/rsa.20120

[6] E. Ben-Sasson and M. Viderman, "Composition of Semi-LTCs by Two-Wise Tensor Products," in *APPROX-RANDOM*, ser. Lecture Notes in Computer Science, I. Dinur, K. Jansen, J. Naor, and J. D. P. Rolim, Eds., vol. 5687. Springer, 2009, pp. 378–391. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-03685-9

[7] ——, "Tensor Products of Weakly Smooth Codes are Robust," *Theory of Computing*, vol. 5, no. 1, pp. 239–255, 2009. [Online]. Available: http://dx.doi.org/10.4086/toc.2009.v005a012

[8] ——, "Low Rate Is Insufficient for Local Testability," in *APPROX-RANDOM*, ser. Lecture Notes in Computer Science, M. J. Serna, R. Shaltiel, K. Jansen, and J. D. P. Rolim, Eds., vol. 6302. Springer, 2010, pp. 420–433. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-15369-3

[9] A. Bennatan and D. Burshtein, "On the Application of LDPC Codes to Arbitrary Discrete-Memoryless Channels," *IEEE Transactions on Information Theory*, vol. 50, no. 3, pp. 417–438, 2004.

[10] D. Coppersmith and A. Rudra, "On the Robust Testability of Product of Codes," *Electronic Colloquium on Computational Complexity (ECCC)*, no. 104, 2005. [Online]. Available: http://eccc.hpi-web.de/eccc-reports/2005/TR05-104/index.html

[11] I. Dinur, "The PCP theorem by gap amplification," *Journal of the ACM*, vol. 54, no. 3, pp. 12:1–12:44, Jun. 2007.

[12] I. Dinur and O. Reingold, "Assignment Testers: Towards a Combinatorial Proof of the PCP Theorem," *SIAM Journal on Computing*, vol. 36, no. 4, pp. 975–1024, 2006. [Online]. Available: http://dx.doi.org/10.1137/S0097539705446962

[13] I. Dinur, M. Sudan, and A. Wigderson, "Robust Local Testability of Tensor Products of LDPC Codes," in *APPROX-RANDOM*, ser. Lecture Notes in Computer Science, vol. 4110. Springer, 2006, pp. 304–315. [Online]. Available: http://dx.doi.org/10.1007/11830924_29

[14] R. G. Gallager, *Low-density Parity Check Codes*. MIT Press, 1963.

[15] ——, *Information Theory and Reliable Communication*. Wiley, New York, 1968.

[16] O. Goldreich, "Short locally testable codes and proofs (survey)," *Electronic Colloquium on Computational Complexity (ECCC)*, no. 014, 2005. [Online]. Available: http://eccc.hpi-web.de/eccc-reports/2005/TR05-014/index.html

[17] O. Goldreich and O. Meir, "The Tensor Product of Two Good Codes Is Not Necessarily Robustly Testable," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 14, no. 062, 2007. [Online]. Available: http://eccc.hpi-web.de/eccc-reports/2007/TR07-062/index.html

[18] O. Goldreich and M. Sudan, "Locally testable codes and PCPs of almost-linear length," *Journal of the ACM*, vol. 53, no. 4, pp. 558–655, Jul. 2006.

[19] T. Kaufman and M. Sudan, "Sparse random linear codes are locally decodable and testable," in *FOCS*. IEEE Computer Society, 2007, pp. 590–600. [Online]. Available: http://doi.ieeecomputersociety.org/10.1109/FOCS.2007.65

[20] ——, "Algebraic property testing: the role of invariance," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*. ACM, 2008, pp. 403–412. [Online]. Available: http://doi.acm.org/10.1145/1374376.1374434

[21] S. Kopparty and S. Saraf, "Local list-decoding and testing of random linear codes from high error," in *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010*, L. J. Schulman, Ed. ACM, 2010, pp. 417–426. [Online]. Available: http://doi.acm.org/10.1145/1806689.1806748

[22] G. A. Margulis, "Explicit constructions of graphs without short cycles and low density codes," *Combinatorica*, vol. 2, no. 1, pp. 71–78, 1982.

[23] M.Blum, M.Luby, and R.Rubinfeld, "Self-Testing/Correcting with Applications to Numerical Problems," *JCSS: Journal of Computer and System Sciences*, vol. 47, 1993.

[24] O. Meir, "Combinatorial Construction of Locally Testable Codes," *SIAM J. Comput*, vol. 39, no. 2, pp. 491–544, 2009. [Online]. Available: http://dx.doi.org/10.1137/080729967

[25] M. Sipser and D. A. Spielman, "Expander Codes," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1710–1722, 1996, preliminary version appeared in FOCS 1994.

[26] L. Trevisan, "Some Applications of Coding Theory in Computational Complexity," in *ECCC: Electronic Colloquium on Computational Complexity, technical reports*, 2004.

[27] P. Valiant, "The Tensor Product of Two Codes Is Not Necessarily Robustly Testable," in *APPROX-RANDOM*, ser. Lecture Notes in Computer Science, vol. 3624. Springer, 2005, pp. 472–481. [Online]. Available: http://dx.doi.org/10.1007/11538462_40

A Distribution over subsets implies a distribution over dual codewords

Sometimes we assume that a tester of a linear code C tests an input word w by picking a small weight dual word $u \in C^\perp$ and accepts if and only if $\langle u, w\rangle = 0$. Proposition A.1 demonstrates that our definition of LTCs (Definition 2.4) implies this property, i. e., a distribution over small subsets of $[n]$ defines a "corresponding" distribution over small weight dual words. Recall that $C \subseteq \mathbf{F}^n$.

Proposition A.1. *1. If C is a (q, ϵ, δ)-LTC then there exists a distribution $\mathbf{D_C}$ over $C^\perp_{\leq q}$ such that for all w, $\delta(w, C) \geq \delta$ we have*

$$\Pr_{u \in_{\mathbf{D_C}} C^\perp_{\leq q}}[\langle u, w\rangle \neq 0] \geq \frac{\epsilon(|\mathbf{F}| - 1)}{|\mathbf{F}|}$$

2. If C is a (q, ϵ)-strong LTC then there exists a distribution $\mathbf{D_C}$ over $C^\perp_{\leq q}$ such that for all w we have

$$\Pr_{u \in_{\mathbf{D_C}} C^\perp_{\leq q}}[\langle u, w\rangle \neq 0] \geq \frac{\epsilon \cdot \delta(w, C)(|\mathbf{F}| - 1)}{|\mathbf{F}|}$$

3. If C is a (q, ϵ, β)-semi LTC then there exists a distribution $\mathbf{D_C}$ over $C^\perp_{\leq q}$ such that for all w, $(\beta/3)\delta(C) \leq \mathrm{wt}(w) \leq \beta\delta(C)$ we have

$$\Pr_{u \in_{\mathbf{D_C}} C^\perp_{\leq q}}[\langle u, w\rangle \neq 0] \geq \frac{\epsilon(|\mathbf{F}| - 1)}{|\mathbf{F}|}$$

4. *If C is a (q,ϵ,β)-strong semi LTC then there exists a distribution $\mathbf{D_C}$ over $C^{\perp}_{\leq q}$ such that for all w, $\mathrm{wt}(w) \leq \beta\delta(C)$ we have*

$$\Pr_{u\in_{\mathbf{D_C}} C^{\perp}_{\leq q}}[\langle u,w\rangle \neq 0] \geq \frac{\epsilon\cdot \mathrm{wt}(w)(|\mathbf{F}|-1)}{|\mathbf{F}|}$$

Proof. We claim the following statement and all bullets of the Proposition will follow immediately from this statement. Let $\mathbf{D}$ be a distribution over $I \subseteq [n]$ such that $|I| \leq q$ and assume that for all $w \in \mathbf{F}^n$ we have $\Pr_{I\sim\mathbf{D}}[w|_I \notin C|_I] \geq \epsilon_w$ where $0 \leq \epsilon_w \leq 1$. Then there exists a distribution $\mathbf{D_C}$ over $C^{\perp}_{\leq q}$ such that for all $w \in \mathbf{F}^n$ it holds that $\Pr_{u\in_{\mathbf{D_C}} C^{\perp}_{\leq q}}[\langle u,w\rangle \neq 0] \geq \frac{|\mathbf{F}|-1}{|\mathbf{F}|}\cdot\epsilon_w$.

Let $\mathbf{U_I}$ be the uniform distribution over $(C|_I)^{\perp}$ for $|I| \leq q$. Let $\mathbf{D_C}$ be the distribution over $C^{\perp}_{\leq q}$ defined as follows: $\mathbf{D_C}(u) = \sum_{I\sim\mathbf{D},\mathrm{supp}(u)\subseteq I} \mathbf{D}(I)\cdot\mathbf{U_I}(u)$. Let $w \in S$. We argue that

$$\Pr_{u\in_{\mathbf{D_C}} C^{\perp}_{\leq q}}[\langle u,w\rangle \neq 0] \geq \frac{|\mathbf{F}|-1}{|\mathbf{F}|}\cdot\epsilon_w.$$

To see this note that

$$\Pr_{I\sim\mathbf{D}}[w|_I \notin C|_I] \geq \epsilon_w$$

and

$$\Pr_{u\in_U (C|_I)^{\perp}}[\langle u,w\rangle \neq 0 \mid w|_I \notin C|_I] = \frac{|\mathbf{F}|-1}{|\mathbf{F}|}$$

because if $w|_I \notin C|_I$ then by linearity for $\frac{|\mathbf{F}|-1}{|\mathbf{F}|}$ fraction $u \in (C|_I)^{\perp}$ we have $\langle u,w\rangle \neq 0$. To see this let $\{u_1,\ldots,u_m\} \subseteq (C|_I)^{\perp}$ be the basis of $(C|_I)^{\perp}$ and then there exists $u_i \in \{u_1,\ldots,u_m\}$ such that $\langle u_i,w\rangle = a \neq 0$, since $w|_I \notin C|_I$. It is sufficient to show that

$$\Pr_{\alpha_1,\ldots,\alpha_m\in_U\mathbf{F}}\left[\langle\sum_j \alpha_j u_j, w\rangle \neq 0\right] = \frac{|\mathbf{F}|-1}{|\mathbf{F}|}$$

which is equivalent to

$$\Pr_{\alpha_1,\ldots,\alpha_m\in_U\mathbf{F}}\left[\langle\sum_{j\neq i} \alpha_j u_j, w\rangle \neq -\alpha_i\cdot\langle u_i,w\rangle\right] = \frac{|\mathbf{F}|-1}{|\mathbf{F}|}.$$

Thus $-\alpha_i\cdot\langle u_i,w\rangle = -\alpha_i\cdot a$ is distributed uniformly in $\mathbf{F}$ where $\alpha_i \in_U \mathbf{F}$ and so with probability $\frac{1}{|\mathbf{F}|}$ it holds that $\langle\sum_{j\neq i}\alpha_j u_j, w\rangle = -\alpha_i\cdot a$ and with probability $\frac{|\mathbf{F}|-1}{|\mathbf{F}|}$ it holds that $\langle\sum_{j\neq i}\alpha_j u_j, w\rangle \neq -\alpha_i\cdot a$. □

B Proposition B.2

In this section we prove Proposition B.2. We first prove an auxiliary Claim B.1.

Claim B.1. *Assume that $w \in \mathbf{F}^n$, $C \subseteq \mathbf{F}^n$ is a linear code and $w \perp \{u \in C^\perp \mid \mathrm{supp}(u) \subseteq [n] \setminus I\}$. Then $w|_{[n]\setminus I} \in C|_{[n]\setminus I}$, i. e., there exists $c \in C$ such that $w|_{[n]\setminus I} = c|_{[n]\setminus I}$ and thus $\delta(w, C) \leq |I|/n$.*

Proof. We show that $w|_{[n]\setminus I} \in C|_{[n]\setminus I}$. Let $Constr_{(I)} = \{u|_{[n]\setminus I} \mid u \in C^\perp \text{ and } \mathrm{supp}(u) \cap I = \emptyset\}$. By assumption, $w|_{[n]\setminus I} \perp Constr_{(I)}$ and thus $w|_{[n]\setminus I} \in (Constr_{(I)})^\perp$. For all $u \in (C|_{[n]\setminus I})^\perp$ it follows that $u = u'|_{[n]\setminus I}$, where $u' \in C^\perp$ and $\mathrm{supp}(u') \cap I = \emptyset$. Thus $u = u'|_{[n]\setminus I} \in Constr_{(I)}$ and $(C|_{[n]\setminus I})^\perp \subseteq Constr_{(I)}$. Therefore $w|_{[n]\setminus I} \in (Constr_{(I)})^\perp = C|_{[n]\setminus I}$. □

Proposition B.2. *Assume $R \subseteq F^m$ and $C \subseteq F^n$ are linear codes. Let $S \subseteq [n]$, $T \subseteq [m]$, $P = S \times T$ and $M \in F^n \times F^m$. If every row of $M|_P$ belongs to $R|_T$ and every column of $M|_P$ belongs to $C|_S$ then $M|_P \in (R \otimes C)|_P$.*

Proof. If $S = [n]$ and $T = [m]$ we are done. Assume without loss of generality that $T = \{1, 2, \ldots, j\} \subset [m]$. To conclude that $M|_P \in (R \otimes C)|_P$ it is sufficient to show the existence of $M' \in R \otimes C$ such that $M|_P = M'|_P$. Note that if all rows of M' belong to R and all columns of M' belong to C then $M' \in R \otimes C$.

Let $T' = T \cup \{j+1\}$. It is sufficient to show how to get M' such that $M|_{S\times T} = M'|_{S\times T}$ and $M'|_{S\times T'} \in (R \otimes C)|_{S\times T'}$. Because in this case we show how to extend $M|_P$ by the column (or a row).

For $k \in [m]$ let $c^{(k)}$ be $M|_{S\times\{k\}}$, i. e., the k-th column of M restricted on S. We are going to fix all entries of $c^{(j+1)}$, call the obtained new matrix M'. Then we show that $M|_{S\times T} = M'|_{S\times T}$ and $M'|_{S\times T'} \in (R \otimes C)|_{S\times T'}$.

If there exists $u \in R^\perp$ such that $(j+1) \in \mathrm{supp}(u)$ and $\mathrm{supp}(u) \subseteq T'$ then pick arbitrarily any such u and assign $c^{(j+1)}$ such that $\sum_{i\in\mathrm{supp}(u)} c^{(i)} \cdot u|_i = 0$. Call the result M'. Then all columns of $M'|_{S\times T'}$ belong to $C|_S$ because $c^{(j+1)}$ is equal to the linear combination of codewords of $C|_S$. By construction, for every row r of $M'|_{S\times T'}$ we have $\langle r, u\rangle = 0$. We argue that every row r of $M'|_{S\times T'}$ satisfies all constraints $u^* \in R^\perp$ such that $\mathrm{supp}(u^*) \subseteq T'$, i. e., $\langle r, u^*\rangle = 0$ and thus by Claim B.1 we conclude all rows of $M'|_{S\times T'}$ belong to $R|_{T'}$. To see this assume by contradiction that for some $u' \in R^\perp$ we have $\mathrm{supp}(u') \subseteq T'$, $(j+1) \in \mathrm{supp}(u')$ and $\langle r, u'\rangle \neq 0$, but then taking a linear combination of u and u' we get $u'' \in R^\perp$ such that $\mathrm{supp}(u'') \subseteq T$ and $\langle r, u''\rangle \neq 0$ and thus row r of $M|_P$ does not belong to $R|_T$. Contradiction.

Otherwise there is no $u \in R^\perp$ such that $(j+1) \in \mathrm{supp}(u)$ and $\mathrm{supp}(u) \subseteq T'$. Then pick any $w \in C$ and assign $c^{(j+1)} = w|_S$. Call the result M'. Then all columns of $M'|_{S\times T'}$ belong to $C|_S$ because $c^{(j+1)} \in C|_S$. And, similarly, every row r of $M'|_{S\times T'}$ satisfies all constraints $u \in R^\perp$ such that $\mathrm{supp}(u) \subseteq T'$, i. e., $\langle r, u\rangle = 0$ and thus by Claim B.1 we conclude all rows of $M'|_{S\times T'}$ belong to $R|_{T'}$. □

ECCC ISSN 1433-8092
http://eccc.hpi-web.de