THEORY OF COMPUTING, Volume 5 (2009), pp. 239–255
www.theoryofcomputing.org

Tensor Products of Weakly Smooth Codes are Robust*

Eli Ben-Sasson† Michael Viderman†

Received: October 2, 2008; published: December 3, 2009.

Abstract: We continue the study of *robustly testable* tensor codes and expand the class of base codes that can be used as a starting point for the construction of locally testable codes via robustly testable tensor products. In particular, we show that all unique-neighbor expander codes and all locally correctable codes, when tensored with any other good-distance code, are robustly testable and hence can be used to construct locally testable codes. Previous work by Dinur et al. (2006) required stronger expansion properties to obtain locally testable codes.

Our proofs follow by defining the notion of *weakly smooth* codes that generalize the *smooth* codes of Dinur et al. We show that weakly smooth codes are sufficient for constructing robustly testable tensor codes. Using the weaker definition, we are able to expand the family of base codes to include the aforementioned ones.

ACM Classification: E.4

AMS Classification: 68Q99

Key words and phrases: Linear code, tensor code, expander code

1 Introduction

A linear code over a finite field F is a linear subspace $C \subseteq F^n$. A code is *locally testable* if given a word $x \in F^n$ one can verify whether $x \in C$ by reading only a few (randomly chosen) symbols from x. More precisely such a code has a *tester*, which is a randomized algorithm with oracle access to the received

*A preliminary version of this paper appeared in the Proceedings of APPROX-RANDOM 2008 [3].

†Research of both authors supported in part by a European Community International Reintegration Grant, an Alon Fellowship, and grants by the Israeli Science Foundation (grant number 679/06) and by the US-Israel Binational Science Foundation (grant number 2006104).

 DOI: 10.4086/toc.2009.v005a012

word x. The tester reads at most q symbols from x and based on this "local view" decides if $x \in C$ or not. It should accept codewords with probability one, and reject words that are "far" (in Hamming distance) with "noticeable" probability.

Locally Testable Codes (LTCs) are intimately related to PCPs and were implicit already in [1] (cf. [9, Sec. 2.4]). This connection was explicitly studied by Goldreich and Sudan [11]. Since then, several constructions of LTCs have been suggested. (See [9] for an extensive survey of those constructions.) All known efficient constructions of LTCs, i. e., those which achieve subexponential (i. e., $\exp(o(n))$) code length, rely on some form of "composition" of two (or more) codes. One of the simplest ways to compose codes for the construction of LTCs is by use of the tensor product, as suggested by Ben-Sasson and Sudan [2]. They introduced the notion of *robust* LTCs: An LTC is called *robustly testable* if whenever the received word is far from the code, the "view" of the tester is *far* from an accepting view with noticeable probability (see Definition 2.1). Ben-Sasson and Sudan showed in [2] that a code obtained by tensoring three or more codes is robustly testable when the distances of the codes are big enough, and used this result to construct LTCs. Then they considered the tensor product of two codes. Given two linear codes R, C their tensor product $R \otimes C$ consists of all matrices whose rows are codewords of R and whose columns are codewords of C. If R and C are locally testable, we would like $R \otimes C$ to be locally testable. [2] suggested using the following test for the testing of the tensor product $R \otimes C$ and asked whether the tensor product was robustly testable.

Test for $R \otimes C$:

- flip a coin
- **if** "heads," select a random row; **else** select a random column
- accept if the row (column) belongs to R (or C, respectively).

Paul Valiant [16] showed a surprising example of two linear codes R and C for which the test above is not robust, by exhibiting a word x that is far from $R \otimes C$ but such that the rows of x are very close to R and the columns of x are very close to C. Additional examples give a code whose tensor product with itself is not robust [5] and two good codes (with constant rate) whose tensor product is not robust [10].

Despite these examples, Dinur et al. showed in [6] that the above test is robust as long as one of the base codes is *smooth*, according to a definition of the term introduced there (see Definition 5.1). The family of smooth codes includes locally testable codes and certain codes constructed from expander graphs with very good expansion properties. In this work we continue this line of research and enlarge the family of base codes that result in robustly testable tensor codes and do this by working with a weaker definition of smoothness (Definition 3.4). Using the weaker definition, we still manage to get similar results as in [6] and do this using the same proof strategy as there. We are not aware of codes that are weakly smooth but not smooth, although we conjecture such codes do exist. However, our weaker definition allows us to argue—in what we view as the main technical contributions of this paper (Section 6 and Section 7)—that a larger family of codes is suitable for forming robustly testable tensor codes. One notable example is that our definition allows us to argue that any expander code with unique-neighbor expansion (i. e., with expansion parameter $\gamma < 1/2$ as per Definition 2.3) is also weakly smooth, hence can be used to construct robustly testable tensor products. We stress that unique-neighbor expansion is the minimal requirement in terms of expansion needed to argue an expander code has good (i. e., constant relative) distance, using currently known techniques, so our work shows all "combinatorially good" expander codes[1] can be used for the construction of robustly testable tensor products. In comparison, [6] required stronger expansion parameters ($\gamma < 1/4$) of the kind needed to ensure an expander code is not merely good in terms of its distance, but can also be decoded in linear time [15].

Another family of codes shown here to result in robustly testable tensor products of pairs of codes is the family of locally correctable codes (LCCs), see Definition 7.1.

We end this section by pointing out that recently, tensor codes have played a role in the combinatorial construction by Meir [13] of quasilinear length locally testable codes. Better base codes may result in LTCs with improved rate, hence the importance in broadening the class of base codes that can be used to construct robustly testable tensor codes.

Organization of the paper.

In the following section we provide the now-standard definitions regarding robustly testable tensor codes. In Section 3 we formally define weakly smooth codes and state our main results. In Section 4 we prove that weakly smooth codes form robustly testable tensor codes. Section 5 shows the smooth codes of [6] are also weakly smooth. The last two sections prove that unique-neighbor expander codes and locally correctable codes are weakly smooth.

2 Preliminary Definitions

Throughout this paper, F is a finite field and $C, R \subseteq F^n$ are linear codes over F, i. e., linear subspaces of F^n. For $x \in F^n$ let $\mathrm{supp}(x) = \{i \mid x_i \neq 0\}$ and $\mathrm{wt}(x) = |\mathrm{supp}(x)|$. We define the *distance* between two words $x, y \in F^n$ to be $\mathrm{d}(x,y) = \mathrm{wt}(x-y)$ and the relative distance to be $\delta(x,y) = \mathrm{d}(x,y)/n$. The distance of a code is denoted $\mathrm{d}(C)$ and defined to be the minimal value of $\mathrm{d}(x,y)$ for two distinct codewords $x, y \in C$. Similarly, the relative distance of the code is denoted $\delta(C) = \mathrm{d}(C)/n$. For $x \in F^n$ and $C \subseteq F^n$, let $\delta_C(x) = \min_{y \in C}\{\delta(x,y)\}$ denote the relative distance of x from code C. We note that $\mathrm{d}(C) = \min_{c \in C \setminus \{0\}}\{\mathrm{wt}(c)\}$. We let $\dim(C)$ denote the dimension of C. The vector inner product between u_1 and u_2 is denoted by $\langle u_1, u_2 \rangle$. For a code C let

$$C^{\perp} = \{u \in F^n \mid \forall c \in C\colon\ \langle u, c \rangle = 0\}$$

be its dual code and let

$$C^{\perp}_t = \left\{u \in C^{\perp} \mid \mathrm{wt}(u) = t\right\}.$$

In a similar way we define

$$C^{\perp}_{<t} = \left\{u \in C^{\perp} \mid \mathrm{wt}(u) < t\right\} \quad \text{and} \quad C^{\perp}_{\leq t} = \left\{u \in C^{\perp} \mid \mathrm{wt}(u) \leq t\right\}.$$

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 $w|_S = (w_{j_1}, w_{j_2}, \ldots, w_{j_m})$ be the *restriction* of w to the subset S. We let $C|_S = \{c|_S \mid c \in C\}$ denote the projection of the code C to the coordinates corresponding to S.

[1]Clearly, there exist non-unique-neighbor expander codes with good distance. However, the distance of these codes cannot be argued merely using the combinatorial structure of the underlying parity check matrix.

2.1 Tensor Product of Codes

The definitions appearing here are standard in the literature on tensor-based LTCs.

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

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

Note that the tensor product $F^m \otimes F^n$ is the tensor product of codes F^m and F^n. Let $M \in F^m \otimes F^n$ and let $\delta(M) = \delta_{R \otimes C}(M)$. Let $\delta^{row}(M) = \delta_{R \otimes F^n}(M)$ denote the distance from the space of matrices whose rows are codewords of R. This is the expected distance of a random row in x from R. Similarly let $\delta^{col}(M) = \delta_{F^m \otimes C}(M)$.

2.2 Robust Locally Testable Codes

Definition 2.1 (Robustness)**.** Let M be a candidate codeword for $R \otimes C$. The *robustness* of M is defined as $\rho(M) = (\delta^{row}(M) + \delta^{col}(M))/2$, i. e., it is the average distance of "views" of the codeword. The code $R \otimes C$ is *robustly testable* if there exists a constant $\alpha > 0$ such that $\rho(M)/\delta(M) \geq \alpha$ for every $M \notin R \otimes C$.

The robustness of a Tester T is defined as

$$\rho^T = \min_{M \notin R \otimes C} \frac{\rho(M)}{\delta_{R \otimes C}(M)}.$$

For further information and the motivation for the notion of robustness see [2, Section 2].

2.3 Low Density Parity Check (LDPC) Codes

Binary as well as q-ary LDPC codes were introduced by Gallager more than four decades ago [7, 8]. They have been studied extensively in information theory (cf. [4]). Binary LDPC codes motivated Margulis' explicit construction of graphs of large girth [12], the precursor of his construction of Ramanujan graphs. The celebrated expander codes of Sipser and Spielman [14] are binary LDPC codes. In the context of local testability, q-ary LDPC codes were studied in [6].

Definition 2.2 (Check graphs)**.** A *check graph* $([n], [m], E, e)$ consists of a bipartite graph $([n], [m], E)$ ($E \subseteq [n] \times [m]$ is the set of edges) and a function $e : E \to F \setminus \{0\}$. This check graph defines the code $C \subseteq F^n$ via the rule that for all $x \in F^n$

$$x \in C \iff (\forall j \in [m]) \left(\sum_{i \in N(j)} x_i \cdot e(i, j) = 0 \right),$$

where $N(j)$ denotes the set of neighbors of j in the graph.

Clearly, any linear code $C \subseteq F$ has a corresponding check graph. The code C is called a "low-density parity-check code" over F if C admits a "low-density" check graph. Note that if $C^\perp = \text{span}(C^\perp_{\leq d})$ then without loss of generality every right hand node $j \in [m]$ has degree at most d, guaranteeing "low density" if d is "small."

Definition 2.3 (Expander graphs)**.** Let $c,d \in \mathbb{N}$ and let $\gamma,\delta \in (0,1)$. Define a (c,d)-regular (γ,δ)-expander to be a bipartite graph (L,R,E) with vertex sets L,R such that all vertices in L have degree c, and all vertices in R have degree d; and the additional property that every set $L' \subset L$ of vertices such that $|L'| \leq \delta|L|$ has at least $(1-\gamma)c|L'|$ neighbors.

We say that a code C is an (c,d,γ,δ)-*expander code* if it has a check graph that is a (c,d)-regular (γ,δ)-expander.

It is well known that if $\gamma < 1/2$ then the graph has *unique-neighbor* expansion. Recall that unique-neighbor expansion means that for every subset $L' \subseteq L$ such that $0 < |L'| \leq \delta|L|$ there exists a vertex $v \in R$ which is a neighbor of exactly one vertex in L'. Thus, from here on we refer to (γ,δ)-expanders, where $\gamma < 1/2$, as *unique-neighbor* expanders. The following well-known observation (the proof of which is included for the sake of completeness) shows that unique-neighbor expansion of G is sufficient to guarantee that the code whose check graph is G has large distance.

Proposition 2.4. *If C is a (c,d,γ,δ)-expander code over F and $\gamma < \frac{1}{2}$ then $\delta(C) > \delta$.*

Proof. We prove that every non-zero word in C must have weight more than δn. Indeed, let (L,R,E,e) be a check graph of C that is a (c,d)-regular (γ,δ)-expander. The proposition follows by examining the unique neighbor structure of the graph. Let $x \in C$ be such that $0 < \text{wt}(x) \leq \delta n$ and let $L' = \text{supp}(x) \subseteq L$. But then L' has at least $(1-\gamma)c|L'| > \frac{c}{2}|L'|$ neighbors in R. At least one of these sees only one element of L', so the check by this element (corresponding dual word) will give $x_i \cdot e(i,j)$ when $x_i \neq 0, e(i,j) \neq 0$ and thus $x_i \cdot e(i,j) \neq 0$, violating the corresponding constraint and contradicting $x \in C$. $\square$

3 Main Results

Our first main result says that codes obtained by the tensor product of a code with constant relative distance and a unique-neighbor expander code are robustly testable.

Theorem 3.1 (Unique-Neighbor Expander codes)**.** *Let $R \subseteq F^m$ be a code of distance at least $\delta_R > 0$. Let $C \subseteq F^n$ be a (c,d,γ,δ)-expander code for some $c,d \in \mathbb{N}, \delta > 0$, and $0 < \gamma < 1/2$. Then,*

$$\rho^T \geq \frac{\delta \cdot \delta_R}{5.2d^*}$$

where $d \leq d^* < d^k$, $k = (\log_{(0.5+\gamma)} 0.05) + 1$.

The above theorem extends the result of [6] where a similar result was proved for expanders with the stronger requirement $\gamma < 1/6$. Notice the difference between $\gamma < 1/6$ and unique-neighbor expansion $(\gamma < 1/2)$ is qualitative, not merely quantitative. This is because expansion $\gamma < 1/4$ is required to guarantee efficient decoding algorithms, as shown by Sipser and Spielman in [15], whereas $\gamma < 1/2$ is sufficient for claiming the code has large distance, but does not necessarily guarantee efficient decoding.

Our next result extends [6] in a different direction by showing that locally correctable codes can also be used to construct robustly testable tensor codes. Informally, locally correctable codes allow to recover each entry of a codeword with high probability by reading only a few entries of the codeword even if a large fraction of it is adversarially corrupted (see Definition 7.1).

Theorem 3.2 (Locally correctable codes)**.** *Let $R \subseteq F^m$ be a code of distance at least $\delta_R > 0$. Let $C \subseteq F^n$ be a (ε, δ, q)-locally correctable code with $\varepsilon > 0$. Then,*

$$\rho^T \geq \frac{0.5\delta \cdot \delta_R}{2(q+1)}.$$

To prove both theorems we first define *weakly smooth* codes and prove that the tensor of a weakly smooth code and another code with constant relative distance is robustly testable. Then we show that *smooth* codes are also weakly smooth. Finally we show in Claims 6.6 and 7.2 that all unique-neighbor expander codes (with $\gamma < 1/2$) and all locally correctable codes are weakly smooth. This will prove Theorems 3.1 and 3.2.

Remark 3.3. The proofs of Claims 6.6 and 7.2 are similar and rely on the following property shared by both families of codes. For any small subset $I \subset [n]$, most elements $i \in I$ have a low-weight dual constraint u_i such that $\mathrm{supp}(u_i) \cap I = \{i\}$, i. e., a large fraction of I has unique neighbors.

3.1 Weakly Smooth codes

We are coming now to the central definition of the paper, that of a weakly smooth code. This definition allows us to generalize the work of [6] using essentially the same proof as there. In particular, in Section 5 we show that every code that is *smooth* according to [6] is also weakly smooth as per Definition 3.4. Furthermore, using our definition we get robustly testable tensor products from a broader family of base codes.

Both the *smooth* codes of [6] and our weakly smooth codes require the code to retain large distance even after a portion of its coordinates and constraints have been removed. The are, however, two subtle differences between the two notions.

1. In the *smooth* codes setting an adversary is allowed to remove an *arbitrary* small fraction of constraints. In the *weakly smooth* setting the adversary is further limited to removing a small fraction of constraints that must touch a small fraction of indices. This extra limitation on the sets of constraints that can be removed makes it much easier to prove that a given code is weakly smooth. This difference also accounts for our ability to show that both unique-neighbor expander codes and locally correctable codes are weakly smooth (neither of the two families of codes is known to be smooth).

2. In the *smooth* codes setting we work with a predefined set of low-weight constraints coming from a regular bipartite graph. Our Definition 3.4 does not assume any graph, nor does it require any regularity of degrees. This slackness and nonregularity will be crucial in arguing that unique-neighbor expanders are weakly smooth.

Definition 3.4 (Weakly smooth codes)**.** Let $0 \leq \alpha_1 \leq \alpha_1' < 1,\ 0 < \alpha_2 < 1,\ d^*$ be constants. The code C is $(\alpha_1, \alpha_1', \alpha_2, d^*)$-*weakly smooth* if for all subsets $I \subseteq [n]$ of size $|I| < \alpha_1 n$, letting

$$\mathrm{Constr}_{(I)} = \left\{u \in C^{\perp}_{\leq d^*} \mid \mathrm{supp}(u) \cap I = \emptyset\right\}$$

and $C' = (\mathrm{Constr}_{(I)})^{\perp}$, there exists $I' \subset [n]$, $I \subseteq I'$, $|I'| < \alpha_1' n$ such that $\mathrm{d}(C'|_{[n]\setminus I'}) \geq \alpha_2 n$.

The following is the main technical lemma we use to show that weakly smooth codes can be used to construct robustly testable tensor products. Its proof, which follows [6], appears in the next section.

Lemma 3.5 (Main Lemma)**.** *Let $R \subseteq F^m$ and $C \subseteq F^n$ be codes of relative distance δ_R and δ_C, respectively. Assume C is $(\alpha_1, \alpha_1', \alpha_2, d^*)$-weakly smooth, where $\alpha_1' < \delta_C/2$, and let $M \in F^m \otimes F^n$. If*

$$\rho(M) < \min\left\{\frac{\alpha_1 \delta_R}{2d^*}, \frac{\delta_R \alpha_2}{2}\right\}$$

then $\delta(M) \leq 8\rho(M)$.

4 Weakly smooth codes—Proof of Lemma 3.5

We follow the proof of the Main Lemma in [6], but attend to the required modifications needed to carry out the proof with the weaker requirement of smoothness. The main place where we use the weakly smooth property is Proposition 4.2.

Proof of Lemma 3.5. For row $i \in [n]$, let $r_i \in R$ denote a codeword of R closest to the i-th row of M. For column $j \in [m]$, let $c^{(j)} \in C$ denote a 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*. Note that $\delta(M, M_R) = \delta^{row}(M)$ and $\delta(M, M_C) = \delta^{col}(M)$ and with some abuse of notation let $\mathrm{wt}(E)$ be the relative weight of E, so

$$\begin{aligned} \mathrm{wt}(E) &= \delta(M_R, M_C) \leq \delta(M, M_R) + \delta(M, M_C) \\ &= \delta^{row}(M) + \delta^{col}(M) = 2\rho(M)\,. \end{aligned} \tag{4.1}$$

Our proof strategy is to show that the error matrix E is actually very structured. We do this in two steps. First we show that its columns satisfy most low-weight constraints of the column code. Then we show that E contains a large submatrix which is all zeroes. Finally using this structure of E we show that M is close to some codeword in $R \otimes C$. The following is from [6, Proposition 4]; we give the proof for the sake of completeness.

Proposition 4.1. *Let $u \in C^{\perp}_d$ be a constraint of C with* $\mathrm{supp}(u) = \{i_1, \ldots, i_d\}$. *Let e_i denote the i-th row of E. Suppose* $\mathrm{wt}(e_{i_j}) < \delta_R/d$ *for every $j \in [d]$. Then $u^T \cdot E = 0$.*

Proof. Note that for all $c \in C$ we have $\langle c, u \rangle = 0$. Let c_i denote the i-th row of the matrix M_C. (Recall that the rows of M_C are not necessarily codewords of any nice code—it is only the columns of M_C that are codewords of C). For every column j, we have $\langle (M_C)_j, u \rangle = 0$ (since the columns of M_C are codewords of C).

Thus we conclude that $u^T \cdot M_C = 0$ as a vector. Clearly, $u^T \cdot M_R \in R$ since each one of the rows of M_R is a codeword of R. But this implies

$$u^T \cdot E = u^T \cdot (M_R - M_C) = u^T \cdot M_R - u^T \cdot M_C = u^T \cdot M_R - 0 \in R\,.$$

Now we use the fact that the e_{i_j}s have small weight for $i_j \in [d]$. This implies that

$$\mathrm{wt}(u^T \cdot E) < \mathrm{wt}(u) \cdot (\delta_R / d) = \delta_R\,.$$

But R is a code of minimum distance δ_R so the only word of weight less than δ_R in it is the zero codeword, yielding $u^T \cdot E = 0$. □

Proposition 4.2. *There exist subsets $U \subseteq [m]$ and $V \subseteq [n]$ with $|U|/m < \delta_R$ and $|V|/n < \delta_C/2$ such that letting $\bar{V} = [n] \setminus V$ and $\bar{U} = [m] \setminus U$ we have for all $i \in \bar{V}, j \in \bar{U}$ that $E(i, j) = 0$.*

Proof. Let $V_1 \subseteq [n]$ be the set of indices corresponding to rows of the error matrix E with weight at least δ_R / d^*, i. e.,

$$V_1 = \{i \in [n] \mid \mathrm{wt}(e_i) \geq \delta_R / d^*\}\,.$$

Clearly, $|V_1| < \alpha_1 n$, since

$$\frac{|V_1|}{n} \cdot \frac{\delta_R}{d^*} \leq \mathrm{wt}(E) \leq 2\rho(M)$$

and thus

$$\frac{|V_1|}{n} \leq \frac{2\rho(M)}{\delta_R / d^*} < \alpha_1$$

where the last inequality follows from the assumption $\rho(M) < \frac{\alpha_1 \delta_R}{2d^*}$. Let

$$\mathrm{Constr}_{(V_1)} = \left\{u \in C^{\perp}_{\leq d^*} \mid \mathrm{supp}(u) \cap V_1 = \emptyset\right\}$$

and let $C' = (\mathrm{Constr}_{(V_1)})^{\perp}$. Proposition 4.1 implies that $\forall u \in \mathrm{Constr}_{(V_1)}$ we have $u^T \cdot E = 0$, i. e., every column of E, denoted by E_j, satisfies constraint u and therefore $E_j \in C'$.

Recall that C is a $(\alpha_1, \alpha_1', \alpha_2, d^*)$-weakly smooth, where $\alpha_1' < \delta_C/2$. Associate the set V_1 with I from Definition 3.4. Following this definition, there exists a set I' (let $V = I'$), $|V| = |I'| < \alpha_1' n$, such that

$$\mathrm{d}(C'_{[n]\setminus I'}) = \mathrm{d}(C_{[n]\setminus V}) \geq \alpha_2 n\,.$$

We notice that for every column of E, denoted by E_j, we have $(E_j)|_{[n]\setminus I'} \in C_{[n]\setminus V}$. Thus E_j is either zero outside V or has at least $\alpha_2 n$ non-zero elements outside V.

Let U be the set of indices corresponding to the "heavy columns" of E that have $\alpha_2 n$ or more non-zero elements in the rows outside V. We conclude that every column of E that is not zero outside V is located in U. We argue that for each $(i, j) \in \bar{V} \times \bar{U}$ we have $E(i, j) = 0$. This is true since after we remove the rows corresponding to V, all nonzero columns have weight at least $\alpha_2 n$. It follows that all nonzero columns are located in U. Hence all columns of $\bar{V} \times \bar{U}$ are zero columns.

Clearly, $|U|/m < \delta_R$, since

$$\frac{|U|}{m} \cdot \alpha_2 \leq \mathrm{wt}(E) \leq 2\rho(M)$$

and thus

$$\frac{|U|}{m} \leq \frac{2\rho(M)}{\alpha_2} < \delta_R\,,$$

where the last inequality follows from the assumption $\rho(M) < \delta_R \alpha_2/2$. □

Proposition 6 of [6] 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 $R \otimes C$. For the sake of completeness we reproduce the proof from [6].

Proposition 4.3 ([6]). *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 $j \in U$ or $i \in V$. Then $\delta(M) \leq 8\rho(M)$.*

Proof. Let $\bar{V} = [n] \setminus V$ and $\bar{U} = [m] \setminus U$. 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 [2, Proposition 3]). Recall also that $\delta(M, M_R) = \delta^{row} \leq 2\rho(M)$. So it suffices to show $\delta(M_R, N) \leq 6\rho(M)$. We do so in two steps. First we show that $\delta(M_R, N) \leq 2\rho(M_R)$. We then show that $\rho(M_R) \leq 3\rho(M)$ 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 (assume r_1, r_2) are codewords of R which may disagree only on entries from the columns of U, i. e., $\mathrm{supp}(r_1 - r_2) \subseteq U$, but $|U| < \delta_R m$ and thus $\mathrm{d}(r_1, r_2) < \delta_R m$ that means $r_1 = r_2$. Next we claim that for every column $j \in [m]$ the closest codeword of C to $M_R(\cdot, j)$, the j-th column of M_R, is $N(\cdot, j)$, the j-th column of N. This is true since $M_R(i,j) \neq N(i,j)$ implies $i \in V$, where $|V| < \delta_C n/2$ and so the number of such i is less than $\delta_C n/2$. Thus for every j, we have $N(\cdot, j)$ is the (unique) decoding of the j-th column of M_R.

Averaging over j, we get that $\delta^{col}(M_R) = \delta(M_R, N)$. In turn this yields

$$\rho(M_R) \geq \delta(M_R)/2 = \delta(M_R, N)/2\,.$$

This yields the first of the two desired inequalities.

Now to bound $\rho(M_R)$, note that for any pair of matrices M_1 and M_2 we have

$$\rho(M_1) \leq \rho(M_2) + \delta(M_1, M_2)\,. \tag{4.2}$$

Indeed it is the case that $\delta^{row}(M_1) \leq \delta^{row}(M_2) + \delta(M_1, M_2)$ and $\delta^{col}(M_1) \leq \delta^{col}(M_2) + \delta(M_1, M_2)$. When the above two arguments are combined it yields (4.2). Applying this inequality to $M_1 = M_R$ and $M_2 = M$ we get

$$\rho(M_R) \leq \rho(M) + \delta(M_R, M) \leq 3\rho(M)\,.$$

This yields the second inequality and thus the Proposition. □

The Main Lemma (Lemma 3.5) follows immediately from the last two propositions. □

5 Smooth codes are also weakly smooth

We now show that our Definition 3.4 is indeed a generalization of *smooth* codes of Dinur et al. [6]. In what follows $\mathbb{F}_2$ denotes the two-element field and $C(R_0)$ is a code defined by constraints in $R \setminus R_0$. We recall the definition of smooth code.

Definition 5.1 (Smooth Codes)**.** A code $C \subseteq \mathbb{F}_2^n$ is $(d, \alpha, \beta, \delta)$-*smooth* if it has a parity check graph $B = (L, R, E)$ where all the right vertices have degree d, the left vertices have degree $c = d|R|/|L|$, and for every set $R_0 \subseteq R$ such that $|R_0| \leq \alpha|R|$, there exist a set $L_0 \subseteq L$, $|L_0| \leq \beta|L|$ such that the code $C(R_0)|_{[n]\setminus L_0}$ has distance at least δ.

Claim 5.2. *If $C \subseteq \mathbb{F}_2^n$ is a $(d, \alpha, \beta, \delta)$-smooth code then it is $(\alpha_1, \alpha_1', \alpha_2, d^*)$-weakly smooth with $\alpha_1 = \alpha/d$, $\alpha_1' = \beta$, $\alpha_2 = \delta$, $d^* = d$.*

Proof. Let R be a set of constraints of degree d and let $I \subseteq [n]$, $|I| < \alpha_1 n = \alpha n/d$ be the index set from Definition 3.4. Remove all d-constraints that touch at least one index in I. Let R_0 be a set of removed constraints from R. We have left degree $c = d|R|/n$, so, we removed at most $c \cdot \alpha_1 n = d|R|\alpha_1 = \alpha|R|$ constraints. Let

$$\mathrm{Constr}_{(I)} = \left\{u \in C_d^{\perp} \mid \mathrm{supp}(u) \cap I = \emptyset\right\}$$

be the set of constraints in $R \setminus R_0$ (low-weight dual words). We notice that $C(R_0) = (\mathrm{Constr}_{(I)})^{\perp}$. Let $I' \subseteq [n]$, $|I'| < \beta n = \alpha_1' n$ be the index set from the definition of smooth codes (Definition 5.1) that needs to be removed in order to maintain good distance, i. e.,

$$\mathrm{d}(C(R_0)|_{[n]\setminus I'}) \geq \delta n = \alpha_2 n\,.$$

Clearly $I \subseteq I'$ as otherwise $\mathrm{d}(C(R_0)|_{[n]\setminus I'}) = 1$. Thus from the definition of smoothness, letting

$$C' = (\mathrm{Constr}_{(I)})^{\perp}$$

we have $\mathrm{d}(C'|_{[n]\setminus I'}) \geq \alpha_2 n$, which proves that C is $(\alpha_1, \alpha_1', \alpha_2, d^*)$-weakly smooth. □

6 Unique-Neighbor Expander Codes are weakly smooth

As explained in Section 3.1, Dinur et al. [6] showed that expander codes with $\gamma < 1/6$ are smooth and thus result in robustly testable tensor products. In this section we show that it is possible to obtain robustly testable tensor codes from expander codes under the weaker assumption $\gamma < 1/2$. We first define the *gap property* (Definition 6.1) and prove that it implies weak smoothness. Then we show that unique-neighbor expander codes have the gap property.

Definition 6.1 (Gap property)**.** Code C has the (α, δ, d)-gap property if for all subsets $J \subseteq [n], |J| < \alpha n$, letting

$$\mathrm{Constr}_{(J)} = \left\{u \in C_{\leq d}^{\perp} \mid \mathrm{supp}(u) \cap J = \emptyset\right\} \quad \text{and} \quad C' = (\mathrm{Constr}_{(J)})^{\perp}\,,$$

we have that for all vectors $c \in C'|_{[n]\setminus J}$ either $\mathrm{wt}(c) < 0.1\delta n$ or $\mathrm{wt}(c) > 0.8\delta n$.

The next claim generalizes an idea from the proof of [6, Lemma 3].

Claim 6.2. *If C has the (α,δ,d)-gap property then it is $(\alpha,\alpha+0.3\delta,0.5\delta,d)$-weakly smooth.*

Proof. Clearly, C has no codewords of weight between $0.1\delta n$ and $0.8\delta n$. To see this take $J=\emptyset$ and then the gap property implies that for all words $w\in F^n$ if $0.1\delta n \le \mathrm{wt}(w)\le 0.8\delta n$ then $\langle w,u\rangle \neq 0$ for some $u\in C^{\perp}_{\le d}$.

For $A\subseteq C$ let $J_A=\bigcup_{c\in A}\mathrm{supp}(c)$. Let

$$S=\{c\in C \mid 0<\mathrm{wt}(c)<0.1\delta n\}$$

be the set of all non-zero low-weight codewords. We show that $|J_S|<0.3\delta n$.

Assume the contrary, i. e., $|J_S|\ge \delta\cdot 0.3n$. Then there exists $S'\subseteq S$ such that $0.2\delta n<|J_{S'}|<0.3\delta n$. To see this, remove low-weight words one by one from S, each time decreasing S at most by $0.1\delta n$.

Consider a random linear combination of codewords from S'. The expected weight of this linear combination is more than $0.1\delta n$ but cannot exceed $0.3\delta n$, thus there exists such a linear combination of low-weight codewords that produces a codeword with weight more than $0.1\delta n$ but less than $0.3\delta n$. Contradiction.

Thus for the rest of the proof we assume $|J_S|<0.3\delta n$. We are ready to show that the code C is $(\alpha,\alpha+0.3\delta n,0.5\delta n,d)$-weakly smooth.

Let $I\subset[n]$, $|I|<\alpha n$ be an arbitrarily chosen set. Let

$$\mathrm{Constr}_{(I)}=\left\{u\in C^{\perp}_{\le d} \mid \mathrm{supp}(u)\cap I=\emptyset\right\} \quad \text{and} \quad C'=\left(\mathrm{Constr}_{(I)}\right)^{\perp}.$$

From the definition of the gap property and from the above it follows that for all $c\in C'|_{[n]\setminus I}$ either $\mathrm{wt}(c)<0.1\delta n$ and thus $\mathrm{supp}(c)\subseteq J_S$ or $\mathrm{wt}(c)>0.8\delta n$.

Let $I'=J_S\cup I$. We have $|I'|\le |J_S|+|I|<\alpha n+0.3\delta n$. We claim that

$$\mathrm{d}(C'|_{[n]\setminus(I\cup J_S)})=\mathrm{d}(C'|_{[n]\setminus(I')})\ge 0.5\delta n\,.$$

To see this assume $c'\in C'|_{[n]\setminus I}$, $c''=c'|_{[n]\setminus(I\cup J_S)}$, $c''\in C'|_{[n]\setminus(I\cup J_S)}$ such that $0<\mathrm{wt}(c'')<0.5\delta n$. But then,

$$0<\mathrm{wt}(c'')\le \mathrm{wt}(c')\le |J_S|+\mathrm{wt}(c'')<0.8\delta n$$

and thus c' is a low-weight word. Therefore $\mathrm{supp}(c')\subseteq J_S$. Hence $c''=c'|_{[n]\setminus(I\cup J_S)}=0$, contradicting $\mathrm{wt}(c'')>0$. □

Proposition 6.3. *Let C be a linear code over F. If $u_1\in C^{\perp}_{<f}$ and $u_2\in C^{\perp}_{<g}$ and $i\in\mathrm{supp}(u_1)\cap\mathrm{supp}(u_2)$ then there exists $u_3\in C^{\perp}_{<f+g}$ such that $\mathrm{supp}(u_3)\subseteq(\mathrm{supp}(u_1)\cup\mathrm{supp}(u_2))\setminus\{i\}$.*

Proof. Let $a\in F$ be the i-th entry of u_1 and $b\in F$ be the i-th entry of u_2. Then $u_3=a^{-1}u_1+b^{-1}u_2\in C^{\perp}_{<f+g}$ has the desired properties. □

The next claim shows that expander codes with $\gamma<1/2$ have specific low-weight constraint structure. We use this claim later to argue that expander codes with $\gamma<1/2$ have the gap property (Definition 6.1) and thus are weakly smooth.

Claim 6.4. *Let C be a (c,d,γ,δ)-expander code over F with constant $\gamma < 1/2$. Let $I \subseteq [n]$ such that $0 < |I| < \delta n$. Then at least a 0.95-fraction of indices $i \in I$ satisfy $u_i \in C^{\perp}_{<d^*}$ where $d^* < d^k$, $k = (\log_{0.5+\gamma}(0.05)) + 1$ such that* $\mathrm{supp}(u_i) \cap I = \{i\}$.

Proof. Fix $I \subseteq [n]$ with $|I| < \delta n$. Let (L,R,E,e) be a check graph of C that is a (c,d)-regular (γ,δ)-expander; here $L = [n]$ and $R = C^{\perp}_{\leq q}$. The Claim follows by examining the unique neighbor structure of the graph. For $j = 1,\dots,k$ we construct, inductively, sets I_j satisfying

- $I_1 = I, I_{j+1} \subset I_j$
- $|I_{j+1}| \leq (\frac{1}{2}+\gamma)|I_j|$
- for all $i \in I_j \setminus I_{j+1}$ there exists $u_i \in C^{\perp}_{\leq d^j}$ with $\mathrm{supp}(u_i) \cap I = \{i\}$.

We then conclude $(\frac{1}{2}+\gamma)^k < 0.05$. Therefore $I_k \subset I$, $|I_k| < 0.05 \cdot |I|$ and for all $i \in I \setminus I_k$ there exists $u_i \in C^{\perp}_{<d^k}$ with $\mathrm{supp}(u_i) \cap I = \{i\}$. This will complete the proof of the Claim.

For the base case let $I_1 = I$. Since C is an expander and $|I_1| \leq \delta n$, I_1 has at least

$$(1-\gamma)c|I_1| = \left(\frac{c}{2} + (0.5-\gamma)c\right)|I_1|$$

neighbors in R. Each index $i \in I_1$ has c neighbors in R. So the number of constraints in R that involve at least 2 indices from I_1 is bounded from above by $(c/2)|I_1|$. Hence there are at least $((1/2-\gamma)c)|I_1|$ unique neighbors in R. Since a single index cannot have more than c unique neighbors in R, the number of indices in I_1 having a unique neighbor is at least $(1/2-\gamma)|I_1|$. This means that at least a $(1/2-\gamma)$-fraction of all indices in I_1 have a unique neighbor with support $d = d^1$. Let $I_2 \subset I_1$ be the subset of all indices $i \in I_1$ that have no unique neighbor of weight at most d^1. We constructed sets I_1, I_2 such that

- $I_1 = I, I_2 \subset I_1$
- $|I_2| \leq (\frac{1}{2}+\gamma)|I_1|$
- for all $i \in I_1 \setminus I_2$ there exists $u_i \in C^{\perp}_{\leq d^1}$ with $\mathrm{supp}(u_i) \cap I = \{i\}$.

This completes the base case.

Assume correctness up to $j-1$ and let us prove it for j. Consider I_j, $|I_j| \leq |I_1| \leq \delta n$. We say that $u \in C^{\perp}_d$ is an *I_j-restricted unique neighbor* of the index $i \in I_j$ if $\mathrm{supp}(u) \cap I_j = \{i\}$. By the unique neighbor expansion, at least a $(1/2-\gamma)$-fraction of indices $i \in I_j$ have I_j-restricted unique neighbors. Let $I_{j+1} \subset I_j$ be the set of indices $i \in I_j$ that have no I_j-restricted unique neighbor. It follows that $|I_{j+1}| \leq (1/2+\gamma)|I_j|$.

Fix $i \in I_j \setminus I_{j+1}$ arbitrarily. There exists $u_i \in C^{\perp}_d$ such that $\mathrm{supp}(u_i) \cap I_j = \{i\}$. Every index $\ell \in \mathrm{supp}(u_i)$, $\ell \neq i$ is located either in $[n] \setminus I_1$ or in $I_1 \setminus I_j$. We handle all $\ell \in I_1 \setminus I_j$ using linear combination according to Proposition 6.3 to obtain a constraint $u'_i \in C^{\perp}_{\leq d^j}$ such that $\mathrm{supp}(u'_i) \cap I = \{i\}$. This is possible since every $\ell \in I_1 \setminus I_j$ is located in some I_f for $1 \leq f < j$ and therefore, by the inductive hypothesis, satisfies $u_\ell \in C^{\perp}_{\leq d^{j-1}}$ such that $\mathrm{supp}(u_\ell) \cap I = \{\ell\}$. Since $\mathrm{wt}(u_i) \leq d$ we obtain $u'_i \in C^{\perp}_{\leq d^{j-1} \cdot d} = C^{\perp}_{\leq d^j}$ such that $\mathrm{supp}(u'_i) \cap I = \{i\}$. So we have shown

- $I_{j+1} \subset I_j$
- $|I_{j+1}| \le (\frac{1}{2}+\gamma)|I_j|$
- for all $i \in I_j \setminus I_{j+1}$ there exists $u_i \in C^{\perp}_{\le d^j}$ with $\mathrm{supp}(u_i) \cap I = \{i\}$.

This completes the induction and the proof of Claim 6.4. □

Corollary 6.5. *If C is a (c,d,γ,δ)-expander code with $\gamma < \frac{1}{2}$ then C has the $(0.5\delta, 0.5\delta, d^*)$-gap property where $d^* < d^k$, $k = (\log_{(0.5+\gamma)} 0.05) + 1$.*

Proof. Let $J \subset [n]$, $|J| < 0.5\delta$ be arbitrarily chosen. Let

$$\mathrm{Constr}_{(J)} = \left\{u \in C^{\perp}_{<d^k} \mid \mathrm{supp}(u) \cap J = \emptyset\right\} \quad \text{and} \quad C' = (\mathrm{Constr}_{(J)})^{\perp}.$$

Assume by contradiction that there exists $w \in C'_{[n]\setminus J}$ such that

$$0 < 0.1 \cdot (0.5\delta)n \le \mathrm{wt}(w) \le 0.8 \cdot (0.5\delta)n.$$

It follows that there is no $u \in \mathrm{Constr}_{(J)}$ such that $|\mathrm{supp}(u) \cap \mathrm{supp}(w)| = 1$.

Let

$$I = J \cup \mathrm{supp}(w) \quad \text{and} \quad |I| \le |J| + \mathrm{wt}(w) < 0.5\delta n + 0.4\delta n < \delta n.$$

We notice that $\mathrm{supp}(w) \cap J = \emptyset$ and $|\mathrm{supp}(w)| > 0.05 \cdot |I|$. So, by Claim 6.4, there exists $u \in C^{\perp}_{<d^k}$ such that $|\mathrm{supp}(u) \cap \mathrm{supp}(w)| = 1$ and $|\mathrm{supp}(u) \cap I| = |\mathrm{supp}(u) \cap \mathrm{supp}(w)| = 1$. Hence $u \in \mathrm{Constr}_{(J)}$ and $|\mathrm{supp}(u) \cap \mathrm{supp}(w)| = 1$. Contradiction. □

Claim 6.6. *If C is a (c,d,γ,δ)-expander code with $\gamma < \frac{1}{2}$ then C is $(0.5\delta, 0.65\delta, 0.25\delta, d^*)$-weakly smooth where $d^* < d^k$, $k = (\log_{(0.5+\gamma)} 0.05) + 1$.*

Proof. Follows immediately from Corollary 6.5 and Claim 6.2. Corollary 6.5 implies that C has the $(0.5\delta, 0.5\delta, d^*)$-gap property where $d^* < d^k$, $k = (\log_{(0.5+\gamma)} 0.05) + 1$. Claim 6.2 implies that C is $(0.5\delta, 0.5\delta + 0.15\delta, 0.25\delta, d^*)$-weakly smooth. □

Proof of Theorem 3.1. It is sufficient to prove that

$$\rho^T \ge \min\left\{\frac{\delta \cdot \delta_R}{5.2d^*}, \frac{\delta \cdot \delta_R}{10.4}, \frac{1}{8}\right\}$$

because $\delta_R, \delta \le 1$ and $d^* \ge d > 1$ and thus

$$\frac{1}{8} \ge \frac{\delta \cdot \delta_R}{10.4} \ge \frac{\delta \cdot \delta_R}{5.2d^*}.$$

Let $R \subseteq F^m$ and $C \subseteq F^n$ be codes of distance δ_R and δ_C, resp. By Proposition 2.4, $\delta_C > \delta$. Clearly, C is a (c,d,γ,δ')-expander code, where $\delta' = 0.5\delta/0.65$. Let $M \in F^m \otimes F^n$. Claim 6.6 implies that C is

$(0.5\delta', 0.65\delta', 0.25\delta', d^*)$-weakly smooth where $0.65\delta' = 0.5\delta$, $d \leq d^* < d^k$, $k = (\log_{(0.5+\gamma)} 0.05) + 1$. The Main Lemma (Lemma 3.5) implies that if

$$\rho(M) < \min\left\{\frac{(0.5\delta')\cdot\delta_R}{2d^*}, \frac{\delta_R\cdot(0.25\delta')}{2}\right\}$$

then $\delta(M) \leq 8\rho(M)$.

We conclude that $\rho^T \geq \min\left\{\frac{\delta\cdot\delta_R}{5.2d^*}, \frac{\delta\cdot\delta_R}{10.4}, \frac{1}{8}\right\}$. □

7 Locally correctable codes are weakly smooth

Definition 7.1 (Locally Correctable Code)**.** A code $C \subseteq F^n$ is called a (q,ε,δ)-*locally correctable* code if there exists a randomized decoder (D) that reads at most q entries and the following holds.

- For all $c \in C$, $i \in [n]$ we have $\Pr[D^c[i] = c_i] = 1$.
- For all $c \in C$, $i \in [n]$ and for all $\hat{c} \in F^n$ such that $\mathrm{d}(c,\hat{c}) \leq \delta n$ we have $\Pr[D^{\hat{c}}[i] = c_i] \geq \dfrac{1}{|F|} + \varepsilon$, i. e., with probability at least $\frac{1}{|F|} + \varepsilon$, entry c_i will be recovered correctly.

Without loss of generality we assume that given $\hat{c} \in F^n$, the "correction" of entry i (recovering the original c_i) is done by choosing an arbitrary $u \in C^{\perp}_{\leq q+1}$ such that $i \in \mathrm{supp}(u)$. Formally, assume the i-th entry of u is u_i. Let

$$u^{\mathrm{proj}} = u|_{[n]\setminus\{i\}} \quad \text{and} \quad \hat{c}^{\mathrm{proj}} = \hat{c}|_{[n]\setminus\{i\}}\,.$$

Then c_i is recovered by setting

$$D^{\hat{c}}[i] = \frac{\langle u^{proj}, \hat{c}^{proj}\rangle}{u_i}\,.$$

Notice that $u_i \neq 0$. It can be readily verified that if the "correction" of entry i is not done in the way described then there exists $c \in C$ such that $\Pr[D^c[i] = c_i] < 1$.

The next claim holds for variable $\varepsilon > 0$ (e. g., $\varepsilon = o(1)$) whereas locally correctable codes are usually defined with a fixed ε.

Claim 7.2. *If C is an (ε,δ,q)-locally correctable code with $\varepsilon > 0$ then it is $(0.5\delta, 0.5\delta, 0.5\delta, q+1)$-weakly smooth and its relative distance is greater than δ.*

Proof. We first show that for all sets $I \subseteq [n]$, $|I| \leq \delta n$, and for all $i \in I$, we have $u_i \in C^{\perp}_{\leq q+1}$ with $\mathrm{supp}(u_i) \cap I = \{i\}$. Assume the contrary and fix $I \subseteq [n]$, $|I| \leq \delta n$ and $i \in I$. So, for all $u_i \in C^{\perp}_{\leq q+1}$ with $i \in \mathrm{supp}(u_i) \cap I$, we have $|\mathrm{supp}(u_i) \cap I| \geq 2$. Consider an adversary that takes $c \in C$ and sets c_j to a random element from F for each $j \in I$, producing the vector $\hat{c}$. Clearly, the original value of c_i will be recovered with probability at most $\frac{1}{|F|}$ since for every $u^{(i)} \in C^{\perp}_{\leq q+1}$ such that $i \in \mathrm{supp}(u^{(i)})$ the inner product

$$\langle (u^{(i)})|_{[n]\setminus\{i\}}, c|_{[n]\setminus\{i\}}\rangle$$

will produce a uniformly distributed random value in F.

We next show that $\mathrm{d}(C) > \delta n$. To see this assume $c \in C$ such that $0 < \mathrm{wt}(c) \leq \delta n$. Let $I = \mathrm{supp}(c)$, $|I| \leq \delta n$ and $i \in I$. There exists $u \in C^{\perp}_{\leq q+1}$ with $\mathrm{supp}(u) \cap \mathrm{supp}(c) = \{i\}$ and thus $\langle u, w\rangle \neq 0$ implies $c \notin C$.

We finally show the weak smoothness of C. Let $I \subset [n]$, $|I| < 0.5\delta n$ be the set chosen by the adversary and let $I' = I$. Let

$$\mathrm{Constr}_{(I)} = \left\{u \in C^{\perp}_{\leq q+1} \mid \mathrm{supp}(u) \cap I = \emptyset\right\} \quad \text{and} \quad C' = (\mathrm{Constr}_{(I)})^{\perp}.$$

We claim that $\mathrm{d}(C'|_{[n]\setminus I}) \geq 0.5\delta n$. This is true, since otherwise there exists $c' \in C'$, $c'_{[n]\setminus I} \in C'|_{[n]\setminus I}$ such that $0 < \mathrm{wt}(c'_{[n]\setminus I}) < 0.5\delta n$. But then $0 < \mathrm{wt}(c') < 0.5\delta n + |I| \leq \delta n$ and so there exists $u \in \mathrm{Constr}_{(I)}$ such that $|\mathrm{supp}(u) \cap \mathrm{supp}(c')| = 1$ which implies $\langle u, c'\rangle \neq 0$ and $c' \notin C'$. Contradiction, proving that C is $(0.5\delta, 0.5\delta, 0.5\delta, q+1)$-weakly smooth. □

Proof of Theorem 3.2. It is sufficient to show that

$$\rho^T \geq \min\left\{\frac{0.5\delta \cdot \delta_R}{2(q+1)}, \frac{1}{8}\right\}$$

because $q \geq 1$, $\delta \leq 1$ and $\delta_R \leq 1$. Let $R \subseteq F^m$ and $C \subseteq F^n$ be linear codes such that $\delta(R) \geq \delta_R$. Let $M \in F^m \otimes F^n$. Claim 7.2 implies that C is $(0.5\delta, 0.5\delta, 0.5\delta, q+1)$-weakly smooth and $\delta(C) > \delta$. The Main Lemma (Lemma 3.5) implies that if

$$\rho(M) < \min\left\{\frac{(0.5\delta)\cdot\delta_R}{2(q+1)}, \frac{\delta_R \cdot (0.5\delta)}{2}\right\} = \frac{(0.5\delta)\cdot\delta_R}{2(q+1)}$$

then $\delta(M) \leq 8\rho(M)$. □

Acknowledgements.

We thank Madhu Sudan for helpful discussions and the anonymous referees for their valuable comments.

References

[1] LÁSZLÓ BABAI, LANCE FORTNOW, LEONID A. LEVIN, AND MARIO SZEGEDY: Checking computations in polylogarithmic time. In *Proc. 23rd STOC*, pp. 21–31. ACM Press, 1991. [STOC:10.1145/103418.103428]. 240

[2] ELI BEN-SASSON AND MADHU SUDAN: Robust locally testable codes and products of codes. In KLAUS JANSEN, SANJEEV KHANNA, JOSÉ D. P. ROLIM, AND DANA RON, editors, *Proc. 8th Intern. Workshop on Randomization and Comput. (RANDOM'04)*, volume 3122 of *LNCS*, pp. 286–297. Springer, 2004. [doi:10.1007/b99805, ECCC:TR04-046]. 240, 242, 247

[3] ELI BEN-SASSON AND MICHAEL VIDERMAN: Tensor products of weakly smooth codes are robust. In ASHISH GOEL, KLAUS JANSEN, JOSÉ D. P. ROLIM, AND RONITT RUBINFELD, editors, *Proc. 12th Intern. Workshop on Randomization and Comput. (RANDOM'08)*, volume 5171 of *LNCS*, pp. 290–302. Springer, 2008. [doi:10.1007/978-3-540-85363-3_24]. 239

[4] AMIR BENNATAN AND DAVID BURSHTEIN: On the application of LDPC codes to arbitrary discrete-memoryless channels. *IEEE Trans. Inform. Theory*, 50(3):417–438, 2004. [IEEE:10.1109/TIT.2004.824917]. 242

[5] DON COPPERSMITH AND ATRI RUDRA: On the robust testability of product of codes. Technical Report 104, Elect. Colloq. Comput. Complex. (ECCC), 2005. [ECCC:TR05-104]. 240

[6] IRIT DINUR, MADHU SUDAN, AND AVI WIGDERSON: Robust local testability of tensor products of LDPC codes. In JOSEP DÍAZ, KLAUS JANSEN, JOSÉ D. P. ROLIM, AND URI ZWICK, editors, *Proc. 10th Intern. Workshop on Randomization and Comput. (RANDOM'06)*, volume 4110 of *LNCS*, pp. 304–315. Springer, 2006. [doi:10.1007/11830924_29, ECCC:TR06-118]. 240, 241, 242, 243, 244, 245, 247, 248, 249

[7] R. G. GALLAGER: *Low-density Parity Check Codes*. MIT Press, 1963. 242

[8] R. G. GALLAGER: *Information Theory and Reliable Communication*. Wiley, New York, 1968. 242

[9] ODED GOLDREICH: Short locally testable codes and proofs (survey). Technical Report 014, Elect. Colloq. Comput. Complex. (ECCC), 2005. [ECCC:TR05-014]. 240

[10] ODED GOLDREICH AND OR MEIR: The tensor product of two good codes is not necessarily robustly testable. Technical Report 062, Elect. Colloq. Comput. Complex. (ECCC), 2007. [ECCC:TR07-062]. 240

[11] ODED GOLDREICH AND MADHU SUDAN: Locally testable codes and PCPs of almost-linear length. In *Proc. 43rd FOCS*, pp. 13–22. IEEE Comp. Soc. Press, 2002. [FOCS:10.1109/SFCS.2002.1181878, ECCC:TR02-050]. 240

[12] GRIGORIĬ A. MARGULIS: Explicit constructions of graphs without short cycles and low density codes. *Combinatorica*, 2(1):71–78, 1982. [doi:10.1007/BF02579283]. 242

[13] OR MEIR: Combinatorial construction of locally testable codes. In RICHARD E. LADNER AND CYNTHIA DWORK, editors, *Proc. 40th STOC*, pp. 285–294. ACM Press, 2008. [STOC:1374376.1374419]. 241

[14] MICHAEL SIPSER AND DANIEL A. SPIELMAN: Expander codes. *IEEE Trans. Inform. Theory*, 42(6):1710–1722, 1996. Preliminary version appeared in FOCS 1994. [IEEE:10.1109/18.556667]. 242

[15] DANIEL A. SPIELMAN: Linear-time encodable and decodable error-correcting codes. *IEEE Trans. Inform. Theory*, 42(6):1723–1731, 1996. Preliminary version appeared in STOC 1995. [IEEE:10.1109/18.556668]. 241, 244

[16] PAUL VALIANT: The tensor product of two codes is not necessarily robustly testable. In CHANDRA CHEKURI, KLAUS JANSEN, JOSÉ D. P. ROLIM, AND LUCA TREVISAN, editors, *Proc. 9th Intern. Workshop on Randomization and Comput. (RANDOM'05)*, volume 3624 of *LNCS*, pp. 472–481. Springer, 2005. [doi:10.1007/11538462_40]. 240

AUTHORS

Eli Ben-Sasson
Computer Science Department
Technion – Israel Institute of Technology, Israel
eli@cs.technion.ac.il
http://www.cs.technion.ac.il/~eli

Michael Viderman
Computer Science Department
Technion – Israel Institute of Technology, Israel
viderman@cs.technion.ac.il
http://www.cs.technion.ac.il/people/viderman

ABOUT THE AUTHORS

ELI BEN-SASSON has too little time for his hobbies: skiing, hiking and general outdoor activities. When not writing about himself (as he is doing right now), he enjoys spending time with his two daughters and son: Hallel, Nitzan, and Yair.

MICHAEL VIDERMAN is a Ph. D. student, and enjoys spending time in the gym and in the swimming pool with his friends.