Electronic Colloquium on Computational Complexity, Revision 3 of Report No. 61 (2007)

On the Rectangle Method in proofs of Robustness of Tensor Products[*]

Or Meir[†]

June 13, 2011

Abstract

Given two error correcting codes R, C, their tensor product $R \otimes C$ is the error correcting code that consists of all matrices whose rows are codewords of R and whose columns are codewords of C. The code $R \otimes C$ is said to be robust if, for every matrix M that is far from $R \otimes C$, it holds that the rows and columns of M are far from R and C respectively. Ben-Sasson and Sudan (ECCC TR04-046) asked under which conditions the product $R \otimes C$ is robust. So far, a few important families of tensor products were shown to be robust, and a counter-example of a product that is not robust was also given. However, a precise characterization of codes whose tensor product is robust is yet unknown.

In this work, we highlight a common theme in the previous works on the subject, which we call "The Rectangle Method". In short, we observe that all proofs of robustness in the previous works are done by constructing a certain "rectangle", while in the counterexample no such rectangle can be constructed. We then show that a rectangle can be constructed if and only if the tensor product is robust, and therefore the proof strategy of constructing a rectangle is complete.

1 Introduction

An error correcting code is said to be *locally testable* if there is a test that can check whether a given string is a codeword of the code, or rather far from the code, by reading only a constant number of symbols of the string. Locally Testable Codes (LTCs) were first systematically studied by Goldreich and Sudan [GS06] and since then several constructions of LTCs were suggested

[*] This research was partially supported by the Israel Science Foundation (grant No. 460/05).

[†] Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100 Israel. Email: or.meir@weizmann.ac.il

ISSN 1433-8092

(See [Gol05] for an extensive survey of some constructions, as well as [Din07, BSS08, Mei09] for a few later constructions).

Ben-Sassson and Sudan [BSS06] suggested using the tensor product operation for the construction of LTCs. Given two linear error correcting codes R, C, their tensor product $R \otimes C$ is the code that 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. [BSS06] suggested using the following test for testing the tensor product $R \otimes C$.

The Row/Column Test Choose a random row (or column) and accept iff it is a codeword of R (C, respectively).

In order to study the conditions under which $R \otimes C$ is locally testable, Ben-Sasson and Sudan introduced the notion of "robust" tensor product (which is a special case of the notion of robustness of [BSGH$^+$06, DR06]). The tensor product $R \otimes C$ is said to be robust if, for every matrix M that is far from $R \otimes C$, it holds that the rows and coluns of M are far from R and C respectively. It is not hard to see that if both R and C are locally testable, and $R \otimes C$ is robust, then $R \otimes C$ is locally testable.

This gives rise to the question in which cases the tensor product is robust. [BSS06] showed that the tensor product of three codes or more ($C_1 \otimes C_2 \otimes C_3 \otimes \ldots$) is robust under a more general notion of robustness, and their work was imroved in [Vid11]. As for the tensor product of two codes, it was proven that for three important families of codes that their tensor product is robust: The Reed-Solomon codes (this is the bivariate low degree test of [PS94]), "smooth" and "weakly smooth" LDPC codes [DSW06, BSV09b], and "semi-LTCs" [BSV09a][1]. In addition, [Val05] showed an example of codes whose tensor product is not robust, and his example was extended in [CR05] and in [GM07].

In this work, we highlight a common theme in all of those papers. We observe that all proofs of robustness share a common proof strategy, which we call "The Rectangle Method" and consists of constructing a "large rectangle". This gives rise to the question of whether this strategy is complete - that is, can it always be used to prove robustness. We answer this question positively, by showing that a "large rectangle" can be constructed for every robust tensor product.

We provide the required preliminaries in Section 2. We describe the rectangle method and our result in detail in Section 3, and prove our result in Section 4. We review the proof of [DSW06] that the existence of a "large rectangle" implies robustness in Section 5.

[1] The work of [BSV09a] uses a little different notion of robustness, but it is relevant for our work as well.

2 Preliminaries

For any two binary strings x, y of the same length, we denote by $\delta(x, y)$ the *relative* Hamming distance between x and y. We say that x and y are τ-close if $\delta(x, y) \leq \tau$, and otherwise we say that they are τ-far.

2.1 Error Correcting Codes

We review the basics of error correcting codes [MS88]. A linear code C is linear subspace of $\{0,1\}^n$, where n is called the block length of C. The vectors of C are called codewords. The code C has relative distance δ_C if for any two distinct codewords $c^1 \neq c^2 \in C$ it holds that $\delta(c^1, c^2) \geq \delta_C$.

2.2 Tensor Product Codes

Let R, C denote linear codes with block lengths m, n and relative distances δ_R, δ_C respectively. The tensor product $R \otimes C \subseteq \{0,1\}^{n \cdot m}$ is the linear code that consists of all the binary $n \times m$ matrices whose rows are codewords of R and whose columns are codewords of C. It is well known that the relative distance of $R \otimes C$ is $\delta_R \cdot \delta_C$.

For any binary $n \times m$ matrix M, we denote by $\delta_{R\otimes C}(M)$ the relative distance of M to $R \otimes C$, and by $\overline{M}$ the codeword of $R \otimes C$ that is closest to M. We denote by M_R the matrix that is obtained by replacing each row of M with the nearest codeword of R, and define M_C similarly. We also denote by $\delta_{\text{row}}(M)$ the average relative distance of a row of M to R, and define δ_{col} similarly. Note that $\delta_{\text{row}} = \delta(M, M_R)$ and that $\delta_{\text{col}} = \delta(M, M_C)$. Finally, we denote by $\rho(M)$ the average of $\delta_{\text{row}}(M)$ and $\delta_{\text{col}}(M)$, that is,

$$\rho(M) \stackrel{\text{def}}{=} \frac{\delta_{\text{row}}(M) + \delta_{\text{col}}(M)}{2}$$

We can now state the definition of robustness.

Definition 2.1. We say that $R \otimes C$ is α-robust if for every M it holds that $\rho(M) \geq \alpha \cdot \delta_{R\otimes C}(M)$.

We turn to state a few easy and useful facts. The following trivial fact upper bounds $\delta_{\text{row}}(M)$ and $\delta_{\text{col}}(M)$ in terms of $\rho(M)$.

Fact 2.2. *It holds that*

$$\begin{aligned} \delta_{row}(M) &\leq 2 \cdot \rho(M) \\ \delta_{col}(M) &\leq 2 \cdot \rho(M) \end{aligned}$$

The following fact is a triangle inequality for robustness.

Fact 2.3. *Let M_1 and M_2 be $n \times m$ binary matrices. Then,*

$$\rho(M_1) \leq \rho(M_2) + \delta(M_1, M_2)$$

Proof. It suffices to prove that

$$\begin{aligned} \delta_{\text{row}}(M_1) &\leq \delta_{\text{row}}(M_2) + \delta(M_1, M_2) \\ \delta_{\text{col}}(M_1) &\leq \delta_{\text{col}}(M_2) + \delta(M_1, M_2) \end{aligned}$$

The first inequality can be obtained by applying the triangle inequality of Hamming distance to each row of M_1 and M_2 separately, and the second inequality can be obtained similarly for columns. ■

The following fact is an easy corollary of the two facts above.

Fact 2.4. *For every matrix M we have*

$$\rho(M_R) \leq 3\rho(M)$$

$$\rho(M_C) \leq 3\rho(M)$$

Proof. We prove only for M_R:

$$\rho(M_R) \quad \leq \quad \rho(M) + \delta(M, M_R) = \rho(M) + \delta_{\text{row}}(M) \leq \rho(M) + 2\rho(M) = 3\rho(M)$$

The required inequality follows. ■

3 The Rectangle Method

Proofs for robustness of $R \otimes C$ usually go along the following line: They first prove that there exists $\alpha_0 \in (0,1)$ such that for every matrix M that satisfies $\rho(M) < \alpha_0$, the matrices M_R and M_C agree on a large rectangle. That is, for every matrix M such that $\rho(M) < \alpha_0$ there exists sets $U \subseteq [m]$, $V \subseteq [n]$ of sizes $|U| > (1 - \frac{1}{2}\delta_R) \cdot m$, $|V| > (1 - \frac{1}{2}\delta_C) \cdot n$, such that M_R and M_C agree on every coordinate in $U \times V$. The argument then uses a known property of tensor products, asserting that if M_R and M_C agree on a such a large rectangle, then $\rho(M) \geq \frac{1}{8}\delta(M)$ (For completeness, a proof of this fact is given in Section 5). The conclusion is that $R \otimes C$ is α-robust for $\alpha = \min\{\alpha_0, \frac{1}{8}\}$.

In this work, we prove that this strategy is "complete"; that is, it can always prove the robustness of $R \otimes C$, provided that $R \otimes C$ is indeed robust. We prove this by showing that if the code is robust and for a matrix M it holds that $\rho(M)$ is small, then there exists a large rectangle on which M_R and M_C agree.

More formally, consider the following two conditions on a tensor product of codes:

1. There exists α_0 such that for every matrix M that satisfies $\rho(M) < \alpha_0$ there exist sets $U \subseteq [n]$, $V \subseteq [m]$ of sizes $|U| > (1 - \frac{1}{2}\delta_C)n$, $|V| > (1 - \frac{1}{2}\delta_R)m$ such that M_R and M_C agree on every coordinate in $U \times V$.
2. There exists α such that $R \otimes C$ is α-robust.

The following theorem, which says that Condition 1 implies Condition 2, is already known.

Theorem 3.1. *If Condition 1 holds with a given value of α_0, then Condition 2 holds with*

$$\alpha \overset{\text{def}}{=} \min\{\alpha_0, \frac{1}{8}\}.$$

The possible novelty of this work is the following theorem, which says that Condition 2 implies Condition 1, and therefore those conditions are equivalent.

Theorem 3.2. *If Condition 2 holds with a given value of α, then Condition 1 holds with*

$$\alpha_0 \overset{\text{def}}{=} \frac{1}{6} \cdot \delta_R \cdot \delta_C \cdot \alpha.$$

We prove Theorem 3.2 in Section 4. For the sake of completeness, we also include the proof of Theorem 3.1 in Section 5

4 Proving that a large rectangle can always be found

In this section, we prove Theorem 3.2. That is, we prove that if $R \otimes C$ is robust, then for every matrix M whose rows and columns are sufficiently close to R and C respectively, there exists a large rectangle on which M_R and M_C agree. The proof proceeds in two steps: We first show that given M as above, it holds that $\overline{M} = \overline{M_R} = \overline{M_C}$ (see Claim 4.1). We then show that this implies the existence of a large rectangle, thus proving Theorem 3.2: The idea that underlies the proof of Theorem 3.2 is that the equality $\overline{M} = \overline{M_R} = \overline{M_C}$ implies that M_R and M_C must be very close to $\overline{M}$. Thus M_R and $\overline{M}$ must agree on many rows, and M_C and $\overline{M}$ must agree on many columns. We can therefore choose the rectangle to be the intersection of the rows on which M_R and $\overline{M}$ agree with the columns on which M_C and $\overline{M}$ agree.

Claim 4.1. *Suppose that $R \otimes C$ is α-robust, and let $\alpha_0 \overset{\text{def}}{=} \frac{1}{6} \cdot \delta_R \cdot \delta_C \cdot \alpha$. Then, for every matrix M that satisfies $\rho(M) < \alpha_0$, it holds that $\overline{M} = \overline{M_R} = \overline{M_C}$.*

Proof. We only prove that if $\rho(M) < \alpha_0$ then $\overline{M} = \overline{M_R}$, and the proof that $\overline{M} = \overline{M_C}$ is similar. We have the following:

$$\begin{aligned}
\delta(\overline{M}, \overline{M_R}) &\leq \delta(\overline{M}, M) + \delta(M, M_R) + \delta(M_R, \overline{M_R}) \\
\text{(By definition of } \delta_{\text{row}}) &= \delta_{R\otimes C}(M) + \delta_{\text{row}}(M) + \delta_{R\otimes C}(M_R) \\
\text{(Since } R \otimes C \text{is } \alpha\text{-robust)} &\leq \frac{1}{\alpha} \cdot \rho(M) + \delta_{\text{row}}(M) + \frac{1}{\alpha} \cdot \rho(M_R) \\
\text{(By Fact 2.2)} &\leq \frac{1}{\alpha} \cdot \rho(M) + 2 \cdot \rho(M) + \frac{1}{\alpha} \cdot \rho(M_R) \\
\text{(By Fact 2.4)} &\leq \frac{1}{\alpha} \cdot \rho(M) + 2 \cdot \rho(M) + \frac{3}{\alpha} \cdot \rho(M) \\
&= \left(2 + \frac{4}{\alpha}\right) \cdot \rho(M) \\
&< \left(2 + \frac{4}{\alpha}\right) \cdot \alpha_0
\end{aligned}$$

Now, observe that$\left(2 + \frac{4}{\alpha}\right) \cdot \alpha_0 \leq \delta_R \cdot \delta_C$. Thus, $\overline{M}$ and $\overline{M_R}$ are codewords of $R \otimes C$ whose relative distance is less than the relative distance of $R \otimes C$, which is $\delta_R \cdot \delta_C$. It therefore holds that $\overline{M} = \overline{M_R}$. ■

We turn to prove Theorem 3.2, restated below.

Theorem (3.2, restated)**.** *Suppose that $R \otimes C$ is α-robust, and let $\alpha_0 \overset{\text{def}}{=} \frac{1}{6} \cdot \delta_R \cdot \delta_C \cdot \alpha$. Then, for every matrix M that satisfies $\rho(M) < \alpha_0$, there exist sets $U \subseteq [n]$, $V \subseteq [m]$ of sizes $|U| > (1 - \frac{1}{2}\delta_C)n$, $|V| > (1 - \frac{1}{2}\delta_R)m$, such that M_R and M_C agree on every coordinate in $U \times V$, and .*

Proof of Theorem 3.2 Let M be such that $\rho(M) < \alpha_0$, so by Claim 4.1 it holds that $\overline{M} = \overline{M_R} = \overline{M_C}$. We first observe that this implies that $\overline{M}$ and $\overline{M_R}$ are close, since

$$\begin{aligned}
\delta(M_R, \overline{M}) &= \delta(M_R, \overline{M_R}) \\
&= \delta_{R\otimes C}(M_R) \\
\text{(Since } R \otimes C \text{is } \alpha\text{-robust)} &\leq \frac{1}{\alpha} \cdot \rho(M_R) \\
\text{(By Fact 2.4)} &\leq \frac{3}{\alpha} \cdot \rho(M) \\
&< \frac{1}{2} \cdot \delta_R \cdot \delta_C
\end{aligned}$$

Furthermore, every row of M_R and every row of $\overline{M}$ are codewords of R, and therefore every row of M_R is either equal to the corresponding row of $\overline{M}$ or they differ on at least δ_R-fraction of the coordinates. It follows that M_R and $\overline{M}$ must agree on more than $\left(1-\frac{1}{2}\delta_C\right)$-fraction of the rows, or otherwise they would disagree on $\frac{1}{2}\cdot\delta_R\cdot\delta_C$ of the coordinates. Similarly, it can be shown M_C and $\overline{M}$ must agree on more than $\left(1-\frac{1}{2}\delta_R\right)$-fraction of the columns. Now take U to be the set of rows on which M_R agrees with $\overline{M}$, and take V to be the set of columns on which M_C agrees with $\overline{M}$. We have that M_R and M_C both agree with $\overline{M}$ on $U\times V$, and therefore they agree with each other on $U\times V$. ■

5 Proving that a large rectangle implies robustness

For completeness, we review the proof (originally given in [DSW06]) of Theorem 3.1, which says that the existence of a large rectangle implies robustness. In order to prove the theorem, it suffices to prove the following result.

Proposition 5.1. *Let M be matrix and suppose there exist $U\subseteq[n]$,$V\subseteq[m]$ of sizes $|U|>(1-\frac{1}{2}\delta_C)n$, $|V|>(1-\frac{1}{2}\delta_R)m$, such that M_R and M_C agree on the coordinates in $U\times V$. Then, $\delta_{R\otimes C}(M)<8\cdot\rho(M)$.*

The rest of this section is devoted to proving Proposition 5.1. Let M be as in the proposition.

Claim 5.2. *There exists a codeword $N\in R\otimes C$ that agrees with M_R and M_C on $U\times V$.*

Proof. Let R' and C' denote the codes obtained from projecting the codewords of R,C to the coordinates in V and U respectively, and let $\Pi_R:R\to R'$ and $\Pi_C:C\to C'$ be the corresponding projections. Observe that Π_R is a bijection: Π_R is surjective by the definition of R'. As for showing that Π_R is injective, note that if two codewords of R are projected to the same codeword of R', then they must agree on more than $\left(1-\frac{1}{2}\delta_R\right)$ of the coordinates and therefore must be equal. Similarly, it can be shown that Π_C is a bijection.

Let M' denote the matrix obtained by projecting M_R or M_C to $U\times V$ (Since the two matrices agree on $U\times V$, the matrix M' is well defined). Observe that M' is a codeword of $R'\otimes C'$. Next, let M'' be the matrix obtained by applying Π_R^{-1} to each row of M', and observe that M'' is a codeword of $R\otimes C'$ that agrees with M' on $U\otimes V$. Finally, let N be the matrix obtained by applying Π_C^{-1} to each column of M'', and observe that N is a codeword of $R\otimes C$ that agrees with M' on $U\otimes V$. Therefore, N is the required codeword of $R\otimes C$. ■

Claim 5.3 ([DSW06])**.** $\delta(M_R,N)=\delta_{col}(M_R)$.

Proof. We show that for each $i\in[m]$, the codeword of C that is closest to the i-th column of M_R is the i-th column of N, and this will imply the required equality. For each row, M_R and N either agree on it or differ on at least δ_R-fraction of its coordinates. Since we know N and M_R agree on $U\times V$, they must agree on all the rows in U. This implies that in every column, M_R and N agree on more than $\left(1 - \frac{1}{2}\delta_C\right)$-fraction of the coordinates, and therefore the decoding of each column of M_R to the nearest codeword of C must result in the corresponding column of N. That is, we have that $(M_R)_C = N$. It follows that $\delta(M_R, N) = \delta_{\text{col}}(M_R)$, as required. ■

Proof of Proposition 5.1. It holds that

$$\begin{array}{rcl}
\delta(M,N) & \leq & \delta(M,M_R) + \delta(M_R,N) \\
\text{(By Definition of } \delta_{\text{row}}) & = & \delta_{\text{row}}(M) + \delta(M_R,N) \\
\text{(By Claim 5.3)} & = & \delta_{\text{row}}(M) + \delta_{\text{col}}(M_R) \\
\text{(By Fact 2.2)} & \leq & 2\rho(M) + 2\rho(M_R) \\
\text{(By Fact 2.4)} & \leq & 2\rho(M) + 6\rho(M) \\
 & = & 8\rho(M)
\end{array}$$

The proposition follows. ■

Acknowledgement. The author wishes to thank Oded Goldreich for his helpful comments on this work. The author also wishes to thank Changyuan Yu for pointing out an error in a previous version of this paper.

References

[BSGH$^+$06] Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. Robust PCPs of proximity, shorter PCPs and applications to coding. *SIAM Journal of Computing*, 36(4):120–134, 2006.

[BSS06] Eli Ben-Sasson and Madhu Sudan. Robust locally testable codes and products of codes. *Random Struct. Algorithms*, 28(4):387–402, 2006. Preliminary version in APPROX-RANDOM 2004.

[BSS08] Eli Ben-Sasson and Madhu Sudan. Short PCPs with polylog query complexity. *SIAM J. Comput.*, 38(2):551–607, 2008. Preliminary version in STOC 2005.

[BSV09a] Eli Ben-Sasson and Michael Viderman. Composition of semi-ltcs by two-wise tensor products. In *APPROX-RANDOM*, pages 378–391, 2009.

[BSV09b] Eli Ben-Sasson and Michael Viderman. Tensor products of weakly smooth codes are robust. *Theory of Computing*, 5(1):239–255, 2009.

[CR05] Don Coppersmith and Atri Rudra. On the robust testability of tensor products of codes. *Electronic Colloquium on Computational Complexity (ECCC)*, (104), 2005.

[Din07] Irit Dinur. The PCP Theorem by gap amplification. *Journal of ACM*, 54(3):241–250, 2007. Preliminary version in STOC 2006.

[DR06] Irit Dinur and Omer Reingold. Assignment testers: Towards combinatorial proof of the PCP theorem. *SIAM Journal of Computing*, 36(4):155–164, 2006.

[DSW06] Irit Dinur, Madhu Sudan, and Avi Wigderson. Robust local testability of tensor products of ldpc codes. In *APPROX-RANDOM*, pages 304–315, 2006.

[GM07] Oded Goldreich and Or Meir. The tensor product of two good codes is not necessarily locally testable. *Electronic Colloquium on Computational Complexity (ECCC)*, (062), 2007.

[Gol05] Oded Goldreich. Short locally testable codes and proofs (survey). *Electronic Colloquium on Computational Complexity (ECCC)*, (014), 2005.

[GS06] Oded Goldreich and Madhu Sudan. Locally testable codes and PCPs of almost linear length. *Journal of ACM*, 53(4):558–655, 2006. Preliminary version in FOCS 2002, pages 13-22.

[Mei09] Or Meir. Combinatorial construction of locally testable codes. *SIAM J. Comput.*, 39(2):491–544, 2009. Preliminary version appeared in STOC 2008, full version can be retrieved as ECCC TR07-115.

[MS88] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*. Elsevier/North-Holland, Amsterdam, 1988.

[PS94] Alexander Polishchuk and Daniel A. Spielman. Nearly-linear size holographic proofs. In *STOC*, pages 194–203, 1994.

[Val05] Paul Valiant. The tensor product of two codes is not necessarily robustly testable. In *APPROX-RANDOM*, pages 472–481, 2005.

[Vid11] Michael Viderman. Linear time decoding of regular expander codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:58, 2011.