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

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

Or Meir†

July 2007

Abstract

Given linear two 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. The 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 columns of M are far from R and C respectively. Ben-Sasson and Sudan (ECCC TR04-046) have asked under which conditions the product $R \otimes C$ is robust. During the last few years, 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 remains unknown.

In this note we highlight a common theme in the above papers, which we call "The Rectangle Method". In short, we observe that all proofs of robustness in the above papers are done by constructing a "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 explicitly studied by Goldreich and Sudan [5] and since then few constructions of LTCs were suggested (See [4] for an extensive survey of those constructions).

*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

Ben-Sassson and Sudan [1] suggested using the tensor product operation for the construction of LTCs. 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. Ben-Sasson and Sudan 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. 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. Ben-Sasson and Sudan managed to show 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. As for the tensor product of two codes, it was proven that for two important cases that the tensor product is robust: The case of Reed-Solomon codes (this is the bivariate low degree test of Polishchuk and Spielman [6]), and the case of "smooth" LDPC codes [3]. In addition, Paul Valiant gave an example of codes whose tensor product is not robust [7], and his example was extended in [2].

In this note 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 make the notation required to continue the discussion in Section 2. We describe the rectangle method and our results in detail in Section 3, and prove our results in Sections 4 and 5. We review the proof that the existence of a "large rectangle" implies robustness in Section 6.

2 Preliminaries

Let R, C denote binary linear codes with block lengths m, n and relative distances δ_R, δ_C. For any two binary strings x, y ($|x| = |y|$), we denote by $\delta(x, y)$ the *relative* Hamming distance between x and y. 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.

For any binary $n \times m$ matrix M we denote by $\delta(M)$ the *relative* distance of M to $R \otimes C$, and by $\overline{M}$ the codeword of $R \otimes C$ nearest to M. We also denote by $\delta_{\text{row}}(M)$ the average relative

distance of a row of M to R, and define δ_{col} similarly. Finally, we denote by $\rho(M)$ the average of $\delta_{\text{row}}(M), \delta_{\text{col}}(M)$, that is

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

The trivial observation that $\delta_{\text{row}}(M) \leq 2\rho(M)$ and $\delta_{\text{col}}(M) \leq 2\rho(M)$ will be useful later.

We say that $R \otimes C$ is α-robust if for every M it holds that $\rho(M) \geq \alpha \cdot \delta(M)$. We also 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.

3 The Rectangle Method

Proofs for robustness of $R \otimes C$ usually go along the following line: They first prove that there exists a constant α_0 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 $U \subseteq [m]$, $V \subseteq [n]$, $|U| > (1 - \delta_R)m$, $|V| > (1 - \delta_C)n$, 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 6). The conclusion is that $R \otimes C$ is α-robust for $\alpha = \min\{\alpha_0, \frac{1}{8}\}$.

In this note 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 a matrix M has very small $\rho(M)$, then there exists a large rectangle on which M_R and M_C agree.

To summarize, consider the following two conditions on a tensor product of codes:

1. There exists a constant α_0 such that for every matrix M that satisfies $\rho(M) < \alpha_0$ there exist sets $U \subseteq [n]$, $V \subseteq [m]$ such that M_R and M_C agree on every coordinate in $U \times V$, where $|U| > (1 - \delta_C)n$, $|V| > (1 - \delta_R)m$.

2. There exists a constant α such that $R \otimes C$ is α-robust.

It is a known fact that the Condition 1 implies Condition 2, and the proofs of robustness usually work by proving that the tensor product satisfies Condition 1, and then conclude that Condition 2 holds. The possible novelty of this note is that we prove that Condition 2 implies Condition 1, so they are equivalent.

We prove that Condition 2 implies Condition 1 in Section 5. For the sake of completeness, we also review the proof that Condition 1 implies Condition 2 in Section 6

The equivalence between the conditions holds also when α_0 and α are sub-constants. The exact quantative relation is that Condition 1 with α_0 implies Condition 2 with $\alpha = \min\left\{\alpha_0, \frac{1}{8}\right\}$, and that Condition 2 with α implies Condition 1 with $\alpha_0 = \frac{1}{6}\delta_R\delta_C\alpha$.

4 Triangle inequality for robustness

We will begin with reviewing the following useful inequality: For every two matrices M_1, M_2 we have that

$$\rho(M_1) \leq \rho(M_2) + \delta(M_1, M_2) \tag{1}$$

Inequality 1 results from averaging the two following inequalites:

$$\delta_{\text{row}}(M_1) \leq \delta_{\text{row}}(M_2) + \delta(M_1, M_2) \tag{2}$$

$$\delta_{\text{col}}(M_1) \leq \delta_{\text{col}}(M_2) + \delta(M_1, M_2) \tag{3}$$

We will only prove Inequality 2, and the proof of Inequality 3 is similar. Inequality 2 follows by applying the usual triangle inequality of distances for each row separately, details follow.

For every $1 \leq i \leq n$ we denote by M_1^i and M_2^i the i-th row of M_1 and M_2 respectively. With a slight abuse of notation, we denote by $\delta_R(M^i)$ the relative distance of the i-th row of M to R, and by $\delta(M_1^i, M_2^i)$ the relative distance between the i-th rows of M_1 and M_2. We now have that

$$\begin{aligned}
\delta_{\text{row}}(M_1) &= \frac{1}{n}\sum_{i=1}^{n} \delta_R(M_1^i) \\
&\leq \frac{1}{n}\sum_{i=1}^{n} \left[\delta_R(M_2^i) + \delta(M_1^i, M_2^i)\right] \\
&= \frac{1}{n}\sum_{i=1}^{n} \delta_R(M_2^i) + \frac{1}{n}\sum_{i=1}^{n} \delta(M_1^i, M_2^i) \\
&= \delta_{\text{row}}(M_2) + \delta(M_1, M_2)
\end{aligned}$$

This completes the proof of Inequality 1.

We mention that Inequality 1 yields the following useful conclusion:

Fact 4.1. *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:

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

Where the first equality is due to the definition of M_R. ■

5 Proving that a large rectangle can always be found

We prove that if $R \otimes C$ is robust then for every matrix M whose rows and columns are close enough to R and C, there exists a large rectangle on which M_R and M_C agree. The proof proceeds in two steps: We first show that $\overline{M} = \overline{M_R} = \overline{M_C}$ (see Claim 5.1). We then show that this implies the existence of a large rectange (see Claim 5.2): The idea is that $\overline{M} = \overline{M_R} = \overline{M_C}$ 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 5.1. *If $R \otimes C$ is α-robust, there exists a constant α_1 such that for every matrix M with $\rho(M) < \alpha_1$, we have that $\overline{M} = \overline{M_R} = \overline{M_C}$. Furthermore, we can choose $\alpha_1 = \frac{1}{6}\delta_R\delta_C\alpha$.*

Proof Suppose that $R \otimes C$ is α-robust for some constant $\alpha > 0$. We first show that there exists a constant $\alpha_1 > 0$ such that $\rho(M) < \alpha_1$ implies that $\overline{M} = \overline{M_R}$. It can be shown similarly for $\overline{M} = \overline{M_C}$, and by choosing α_1 to be small enough we will obtain $\overline{M} = \overline{M_R} = \overline{M_C}$ whenever $\rho(M) < \alpha_1$. So, assume that $\rho(M) < \alpha_1$ for some constant α_1 that will be chosen later. We have the following:

$$\begin{aligned}
\delta(\overline{M}, \overline{M_R}) &\leq \delta(\overline{M}, M) + \delta(M, M_R) + \delta(M_R, \overline{M_R}) \\
&= \delta(M) + \delta_{\text{row}}(M) + \delta(M_R) \\
&\leq \frac{1}{\alpha}\rho(M) + 2\rho(M) + \frac{1}{\alpha}\rho(M_R) \\
&\leq \frac{1}{\alpha}\rho(M) + 2\rho(M) + \frac{3}{\alpha}\rho(M) \\
&= \left(2 + \frac{4}{\alpha}\right) \cdot \rho(M) \\
&< \left(2 + \frac{4}{\alpha}\right) \cdot \alpha_1
\end{aligned}$$

Where the first equality uses $\delta(M, M_R) = \delta_{\text{row}}(M)$ (by definition of M_R), the second inequality uses $\delta_{\text{row}}(M) \leq 2\rho(M)$ and $\rho(M) \geq \alpha\delta(M)$, $\rho(M_R) \geq \alpha\delta(M_R)$ (By the α-robustness of $R \otimes C$) and the third inequality uses $\rho(M_R) \leq 3\rho(M)$ (Fact 4.1). Now, if we choose α_1 such that $\left(2 + \frac{4}{\alpha}\right)\alpha_1 \leq \delta_{R\otimes C} = \delta_R\delta_C$, we shall obtain that $\overline{M} = \overline{M}_R$ for any matrix M such that $\rho(M) < \alpha_1$. Note that choosing $\alpha_1 = \frac{1}{6}\delta_R\delta_C\alpha$ satisfies $\left(2 + \frac{4}{\alpha}\right)\alpha_1 \leq \delta_{R\otimes C}$. ■

Claim 5.2. *If $R \otimes C$ is α-robust, then for every matrix M that satisfies $\overline{M} = \overline{M_R} = \overline{M_C}$ and $\rho(M) < \frac{1}{3}\alpha\delta_R\delta_C$, there exist sets $U \subseteq [n]$, $V \subseteq [m]$ such that M_R and M_C agree on every coordinate in $U \times V$, and $|U| > (1 - \delta_C)n$, $|V| > (1 - \delta_R)m$.*

Proof Let M be such that $\overline{M} = \overline{M_R} = \overline{M_C}$ and $\rho(M) < \frac{1}{3}\delta_R\delta_C\alpha$. We know that

$$\delta(M_R, \overline{M}) = \delta(M_R, \overline{M_R}) = \delta(M_R) \leq \frac{1}{\alpha}\rho(M_R) \leq \frac{3}{\alpha}\rho(M) < \delta_R\delta_C$$

where the first inequality uses $\rho(M_R) \geq \alpha \cdot \delta(M_R)$ and the second inequality uses $\rho(M_R) \leq 3\rho(M)$ (by Fact 4.1).

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 $(1-\delta_C)$-fraction of the rows, or otherwise they would disagree on $\delta_R\delta_C$ of the coordinates. Similarly it can be shown M_C and $\overline{M}$ must agree on more than $(1-\delta_R)$-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 $U \times V$. ■

By combining the two last claims and choosing

$$\alpha_0 = \frac{1}{6}\delta_R\delta_C\alpha \leq \min\left\{\alpha_1, \frac{1}{3}\alpha\delta_R\delta_C\right\}$$

we get that $\rho(M) < \alpha_0$ implies the existence of a large rectangle for M, as required.

6 Proving that a large rectangle implies robustness

For the sake of completeness, we review the proof (given in [3]) that the existence of a large rectangle implies robustness. Let M be matrix and suppose there exist $U \subseteq [n]$,$V \subseteq [m]$ such that M_R and M_C agree on the coordinates in $U \times V$ and such that $|U| > (1-\delta_C)n$,$|V| > (1-\delta_R)m$. We shall show this implies that $\delta(M) < 8\rho(M)$.

Claim 6.1 ([1]). *There exists a legal codeword N 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. 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 the projection from R to R' is actually a bijection: The projection is surjective by the definition of R'. As for the projection being injective, note that if two codewords of R are projected to the same codeword of R', then they must agree on more than $(1-\delta_R)$ of the coordinates and therefore must be equal. Similarly the projection from C to C' is a bijection.

This implies that the projection from $R \otimes C$ to $R' \otimes C'$ (obtained by projecting codewords of $R \otimes C$ to $U \times V$) is one-to-one. Since $R \otimes C$ and $R' \otimes C'$ are linear spaces of the same dimension

$(\dim R \cdot \dim C)$, it follows that this projection is a bijection between $R \otimes C$ to $R' \otimes C'$. Now, note that M' is a legal codeword of $R' \otimes C'$, so it follows that there exists a codeword N of $R \otimes C$ whose projection to $U \times V$ equals M'. ■

Claim 6.2 ([3]). $\delta(M_R, N) = \delta_{col}(M_R)$.

Proof We shall show that if we decode each of the columns of M_R to the nearest codeword of C, we will get N. 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 $(1 - \delta_C)$-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. ■

The inequality $\delta(M) < 8\rho(M)$ now follows by

$$\delta(M, N) \leq \delta(M, M_R) + \delta(M_R, N) \leq \delta_{\text{row}}(M) + 2\rho(M_R) \leq 2\rho(M) + 6\rho(M) = 8\rho(M)$$

where the second inequality uses $\delta(M, M_R) = \delta_{\text{row}}(M)$ (by definition of δ_{row}) and $\delta(M_R, N) = \delta_{\text{col}}(M_R) \leq 2\rho(M_R)$ (by Claim 6.2) . The third inequality follos from $\delta_{\text{row}}(M) \leq 2\rho(M)$ and from $\rho(M_R) \leq 3\rho(M)$ (By fact 4.1).

Acknowledgement. *The author wishes to thank Oded Goldreich for his helpful comments on this note.*

References

[1] E. Ben Sasson and M. Sudan, *Robust locally testable codes and products of codes*, APPROX-RANDOM 2004, pp. 286-297 (See ECCC TR04-046, 2004).

[2] D. Coppersmith and A. Rudra, *On the robust testability of tensor products of codes*, ECCC TR05-104, 2005.

[3] I. Dinur, M. Sudan and A. Wigderson, *Robust local testability of tensor products of LDPC codes*, APPROX-RANDOM 2006, pp. 304-315.

[4] O. Goldreich, *Short Locally Testable Codes and Proofs (Survey)*, ECCC TR05-014, 2005.

[5] O. Goldreich and M. Sudan, *Locally testable codes and PCPs of almost linear length*, FOCS 2002, pp. 13-22 (See ECCC TR02-050, 2002).

[6] A. Polishchuk and D.A. Spielman, *Nearly-linear size holographic proofs*, STOC 1994, pp. 194-203.

[7] P. Valiant, *The Tensor Product of Two Codes Is Not Necessarily Robustly Testable*, APPROX-RANDOM 2005, pp. 472-481.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/