The Tensor Product of Two Good Codes Is Not Necessarily Robustly Testable*

Oded Goldreich† Or Meir‡

July 2007

Abstract

Given 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.

Paul Valiant (APPROX-RANDOM 2005) gave an example of two linear codes with constant relative distance whose tensor product is not robust. However, one of those codes has a sub-constant rate. We show that this example can be modified so that both codes have constant rate and relative distance.

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 [4] and since then few constructions of LTCs were suggested (See [3] for a survey of those constructions).

Eli Ben-Sassson and Madhu Sudan [1] suggested using the tensor product operation for the construction of LTCs. Given two codes R, C, their tensor product $R \otimes C$ consists of all matrices

*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: oded.goldreich@weizmann.ac.il

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

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. Paul Valiant gave an example of two linear codes whose tensor product is not robust [6], and his example was extended in [2]. However, in the example of Valiant, one of the codes is of sub-constant rate. In this note, we show that the example of Valiant can be changed so that both codes have constant rate. Using Theorem 2 of [2], it follows that there exists a linear code of constant rate and relative distance, whose tensor product *with itself* is not robust.

We also give a new proof for the correctness of Valiant's example, that gives a new intuition for why this example works. Our proof is based on the reverse direction of the "Rectangle Method" presented by Meir [5].

2 Preliminaries

Let R, C denote binary linear codes with block lengths m, n and relative distances δ_R, δ_C. 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 $R \otimes C$. 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

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

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

In this note we show an example of codes C_1, C_2 with constant rate and constant relative distance such that $C_2 \otimes C_1$ is not α-robust for any constant α.

3 The codes

Let C_1,C_g be two random linear codes with parameters (with high probability) $\left[n, k = \frac{1}{5}n, d = \frac{1}{100}n\right]_2$ for n that is divisible by 100. Let G_1, G_g be their generating matrices. Let $H = G_1^T G_g$. We claim that H has rank k: On one hand, the columns of H are linear combinations of rows of G_1, so its rank can be at most k. On the other hand, both G_1 and G_g are matrices of rank k and have k rows, so each of them contains a full rank $k \times k$ submatrix, denote those submatrices K_1, K_g respectively. Now, note that $K_1^T K_g$ is a submatrix of $G_1^T G_g$, so the rank of H is at least k. It follows that the rank of H is exactly k, and the columns of H therefore span C_1.

Let H^{10} be the $n \times 10n$ matrix that consists of 10 consecutive copies of H and let I_n^{10} be the n-rank identity matrix with each column duplicated to appear 10 times consecutively. That is, I_n^{10} is a matrix of the form

$$n\left\{\begin{pmatrix}
\overbrace{\begin{matrix}1&1&\dots&1\end{matrix}}^{10} & \overbrace{\begin{matrix}0&0&\dots&0\end{matrix}}^{10} & & \overbrace{\begin{matrix}0&0&\dots&0\end{matrix}}^{10}\\
\begin{matrix}0&0&\dots&0\end{matrix} & \begin{matrix}1&1&\dots&1\end{matrix} & & \begin{matrix}0&0&\dots&0\end{matrix}\\
\begin{matrix}0&0&\dots&0\end{matrix} & \begin{matrix}0&0&\dots&0\end{matrix} & \dots & \begin{matrix}\vdots&\vdots&\vdots&\vdots\end{matrix}\\
\begin{matrix}\vdots&\vdots&\vdots&\vdots\end{matrix} & \begin{matrix}\vdots&\vdots&\vdots&\vdots\end{matrix} & & \begin{matrix}0&0&\dots&0\end{matrix}\\
\begin{matrix}0&0&0&0\end{matrix} & \begin{matrix}0&0&0&0\end{matrix} & & \begin{matrix}1&1&\dots&1\end{matrix}
\end{pmatrix}\right.$$

We define the code C_2 to be the space spanned by the rows of $G_2 = H^{10} + I_n^{10}$. We show that C_2 has a constant rate and constant relative distance and that $C_2 \otimes C_1$ is not robust.

4 Required properties

The dual code of C_1 is a random linear code with rate $\frac{4}{5}$, and since $\frac{4}{5} < 1 - H\left(\frac{1}{100}\right)$ it follows that with high probability this dual has distance $d = \frac{1}{100}n$.

Let S be the set of n-bit vectors that consist of $\frac{n}{10}$ "homogenous" blocks of 10 bits. By "homogenous" we mean that in each block all the bits are equal. Formally:

$$S = \left\{x \in \{0,1\}^n : \forall 0 \leq i < \frac{n}{10},\, 1 \leq j < 10,\, x_{10i+j} = x_{10i+j+1}\right\}$$

Note that the zero vector is in S.

We show that with high probability any nonzero codeword of C_g is $\frac{1}{100}$-far from S. For any $v \in \{0,1\}^k$, observe that vG_g is a uniformly distributed vector in $\{0,1\}^n$ over random choices of

G_g. We denote by $B_n(s,d)$ the Hamming Ball with center s and radius d in $\{0,1\}^n$ and note that

$$\begin{aligned}
\Pr_{G_g}\left[\Delta\left(vG_g, S\right) < d\right] &\leq \sum_{s\in S} \Pr\left[\Delta\left(vG_g, s\right) < d\right] \\
&= \sum_{s\in S} \frac{|B_n(s,d)|}{2^n} \\
&\approx \sum_{s\in S} 2^{\left[H\left(\frac{1}{100}\right)-1\right]n} \\
&< \sum_{s\in S} 2^{-0.9n} \\
&= 2^{\frac{1}{10}n}\cdot 2^{-0.9n} \\
&= 2^{-0.8n}
\end{aligned}$$

By the union bound we obtain that

$$\Pr_{G_g}\left[\Delta\left(C_g\backslash\{0\}, S\right) < d\right] < |C_g|\cdot 2^{-0.8n} = 2^{k-0.8n} = 2^{-0.6n}$$

And thus with high probability $C_g\backslash\{0\}$ is $\frac{1}{100}$-far from S.

5 The rate of C_2

We shall show that the rank of G_2 is at least k, and therefore the rate of C_2 is at least $\frac{1}{50}$ (since C_2 has block length $10n$). Recall that H has rank k (see Section 3), and therefore so does H^{10}. It follows that there are k independent rows of H^{10}. Let I denote the indices of those rows.

Take any $m \leq k$ rows $w_1,\ldots,w_m$ of G_2 whose indices are in I. For each i we write $w_i = u_i + v_i$ where u_i and v_i are rows of H^{10} and I_n^{10} respectively. Recall that $u_1,\ldots,u_m$ are independent, since they were chosen in I. We have that

$$\sum_{i=1}^{m} w_i = \left(\sum_{i=1}^{m} u_i\right) + \left(\sum_{i=1}^{m} v_i\right)$$

We make the following observations:

1. Each row of H is a codeword of C_g.

2. Each row u_i of H^{10} consists of 10 consecutive copies of a row of H, denote it u'_i. Thus, the left summand $(\sum_{i=1}^{m} u_i)$ consists of 10 consecutive copies of $u' = (\sum_{i=1}^{m} u'_i)$. Note that u' is a codeword of C_g, and that it is non-zero because the rows $u_1,\ldots,u_m$ are independent.

3. Every row of I_n^{10} consists of 10 blocks of length n, each of which is an element of S. Clearly, S is closed under addition, and therefore every linear combination of rows of I_n^{10} is a concatenation of 10 elements of S. In particular, the right summand $(\sum_{i=1}^{m} v_i)$ is concatenation of 10 elements of S.

4. It follows that the sum $(\sum_{i=1}^{m} w_i)$ consists of 10 blocks of length n, each of which is the sum of u' and an element of S. Since u' is a non-zero codeword of C_g, the sum of u' with an element of S can not be zero (see Section 4) and therefore $(\sum_{i=1}^{m} w_i)$ is non-zero.

This implies that the rows of G_2 whose indices are in I are independent, so G has rank at least k.

6 The distance of C_2

We shall show that the distance of C_2 is at least $10d$, so its relative distance is $\frac{1}{100}$. Let $c = vG_2$ be any nonzero codeword of C_2. If $vH = 0$, then since the columns of H span C_1, it must be that v is a codeword of the dual of C_1. Thus the weight of v must be at least d (see Section 4) and so $vG_2 = vI_n^{10}$ must have weight of at least $10d$.

Suppose that $vH \neq 0$, and let us denote $x = vH$. We proceed as in the analysis of the rate of C_2: Observe that

1. x is a codeword of G_g.

2. vH^{10} is a concatenation of 10 copies of x

3. vI_n^{10} is the concatenation of 10 elements of S.

It follows that $c = vH^{10} + vI_n^{10}$ consists of 10 blocks, each of them is the sum of x with an element of S. The string x is a non-zero codeword of C_g, so by Section 4 it differs on at least d coordinates from every element of S. It follows that the weight of c is at least $10d$.

7 The non-robustness of $C_2 \otimes C_1$

In this section we review the proof of Paul Valiant to the non-robustness of $C_2 \otimes C_1$. We now consider G_2 as a $n \times 10n$ matrix, which is not a codeword of $C_2 \otimes C_1$, and show that that it is far from $C_2 \otimes C_1$ while its rows and columns are close to C_2 and C_1. That is, G_2 is a counter-example to the robustness of $C_2 \otimes C_1$.

Every row of G_2 is a codeword of C_2, so $\delta_{\text{row}}(G_2) = 0$. Furthermore, every column of $H^{10} = G_2 - I_n^{10}$ is a codeword of C_1, so $\delta_{\text{col}}(G_2) = \frac{1}{n}$. We thus have that $\rho(G_2) \leq \frac{1}{2n}$.

Claim 7.1

$$\delta(G_2) \geq \frac{(n-k)\,d}{10n^2}$$

Proof Consider an arbitrary $M \in C_2 \otimes C_1$. Every row of $G_2 - M$ is a codeword of C_2. Furthermore, each column of $G_2 - I_n^{10} - M$ is a codeword of C_1, so the rank of $G_2 - I_n^{10} - M$ is at most k. This implies that the rank of $G_2 - M$ must be at least $n-k$: Otherwise, the rank of $-I_n^{10} = (G_2 - I_n^{10} - M) + (M - G_2)$ would have been less than n (since rank is sub-additive and the ranks of $G_2 - M$ and $M - G_2$ are equal).

Thus, there are at least $n-k$ non-zero rows in $G_2 - M$, each of which is a codeword of C_2. Each of those non-zero rows of $G_2 - M$ has weight of at least d. It follows that $\Delta(G_2, M) \geq (n-k)d$, so

$$\delta(G_2) = \min_{M \in C_2 \otimes C_1} \{\delta\,(G_2, M)\} \geq \frac{(n-k)\,d}{10n^2}$$

As required. ∎

This implies that $C_2 \otimes C_1$ is at most $\alpha(n)$-robust for

$$\alpha(n) = \frac{10n}{2(n-k)d} = \frac{5n}{\frac{4}{5}n \cdot \frac{1}{100}n} \leq \frac{2500}{n}$$

which is sub-constant.

8 Alternative proof for the non-robustness of $C_2 \otimes C_1$

We give an alternative proof that $C_2 \otimes C_1$ is not robust, (See Section 5 of [5]). For any $n \times 10n$ matrix M, let M_R denote the matrix obtained from decoding every row of M to nearest codeword of C_2, and let M_C be defined similarly for the columns and C_1. Suppose that $C_2 \otimes C_1$ is α-rboust. Then for $\alpha_0 = \frac{1}{6}\delta_{C_1}\delta_{C_2}\alpha$ and for every matrix M that satisfies $\rho(M) < \alpha_0$ we have that M_R and M_C agree on the coordinates in a rectangle $U \times V$, where $U \subseteq [n]$, $V \subseteq [10n]$, $|U| > \left(1 - \frac{1}{100}\right) \cdot n = 0.99n$, $|V| > \left(1 - \frac{1}{100}\right) \cdot n = 9.9n$. We call such rectangle large.

Claim 8.1. *There is no large rectangle $U \times V$ on which $(G_2)_R$ and $(G_2)_C$ agree.*

Proof Let U and V the sets such that $U \times V$ is a large rectangle. Observe that $(G_2)_R = G_2$ and $(G_2)_C = H^{10} = G_2 - I_n^{10}$, so $(G_2)_R - (G_2)_C = I_n^{10}$. We show that I_n^{10} has an entry with value 1 in $U \times V$.

We know that every column of I_n^{10} contains exactly one entry with value 1, so the total number of entries with value 1 contained in the columns of V is $|V|$. We also know that every row of I_n^{10}

contains exactly ten entries with value 1, so there are at least $\frac{1}{10}|V|$ rows that contain 1's *in their intersection with* V. Now, note that $\frac{1}{10}|V| > n - |U|$, and thus the rows containing entries with value 1 *in their intersection with* V can not all be in $[n] \setminus U$. It follows that I_n^{10} has 1 on at least one of the coordinates in $U \times V$, as required. ■

Using Claim 8.1, it is straightforward to show that $C_2 \otimes C_1$ is not robust. However, the quantative bound we get for the robustness of $C_2 \otimes C_1$ is little weaker from the one we get in Section 7. We write the details below, so the bounds can be compared.

Claim 8.2. *$C_2 \otimes C_1$ is at most $\alpha(n)$-robust for $\alpha(n) = \frac{30000}{n}$.*

Proof Suppose that $C_2 \otimes C_1$ is α-robust for $\alpha > \frac{30000}{n}$. It follows that for

$$\alpha_0 = \frac{1}{6}\delta_{C_1}\delta_{C_2}\alpha > \frac{1}{6} \cdot \frac{1}{100} \cdot \frac{1}{100} \cdot \frac{30000}{n} = \frac{1}{2n}$$

we have that for any matrix M that satisfies $\rho(M) < \alpha_0$ we have that M_R and M_C agree on a large rectangle. Recall that $\rho(G_2) = \frac{1}{2n} < \alpha_0$, so it follows that $(G_2)_R$ and $(G_2)_C$ agree on a large rectangle, contradicting Claim 8.1. ■

We comment that the bound derived in Claim 8.2 is not optimal. A stronger bound can be derived by analyzing more carefully the relative distance of C_1 and C_2.

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

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

[5] O. Meir, *On the Rectangle Method in proofs of Robustness of Tensor Products*, ECCC TR07-, 2007

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