Robust local testability of tensor products of LDPC codes*

Irit Dinur[1], Madhu Sudan[2], and Avi Wigderson[3]

[1] Hebrew University, Jerusalem, Israel. dinuri@cs.huji.ac.il
[2] Massachusetts Institute of Technology, Cambridge, MA. madhu@mit.edu
[3] Institute for Advanced Study, Princeton, NJ. avi@ias.edu

Abstract. Given two binary linear codes R and C, their tensor product $R \otimes C$ consists of all matrices with rows in R and columns in C. We analyze the "robustness" of the following test for this code (suggested by Ben-Sasson and Sudan [6]): Pick a random row (or column) and check if the received word is in R (or C). Robustness of the test implies that if a matrix M is far from $R \otimes C$, then a significant fraction of the rows (or columns) of M are far from codewords of R (or C).
We show that this test *is* robust, provided one of the codes is what we refer to as *smooth*. We show that expander codes and locally-testable codes are smooth. This complements recent examples of P. Valiant [13] and Coppersmith and Rudra [9] of codes whose tensor product is not robustly testable.

1 Introduction

A binary linear code is a linear subspace $C \subseteq \{0,1\}^n$. A code is *locally testable* if given a word $x \in \{0,1\}^n$ one can verify whether $x \in C$ by reading only few (randomly chosen) bits from x. More precisely such a code has a *tester*, which is a randomized algorithm with oracle access to the received 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) from the code with "noticeable" probability.

Locally testable codes (LTCs) are related to probabilistically checkable proofs (PCPs). LTCs were first explicitly studied by Goldreich and Sudan [12], who describe them as the "combinatorial core of PCPs". They constructed LTCs relying on some of the PCP machinery [11, 2, 1]. Since locally testable codes are simpler than PCPs, it seems natural to seek alternative constructions for them, possibly departing from the PCP framework.

One of the most interesting challenges in constructing LTCs, is to come up with an LTC that has constant relative distance and highest possible (maybe linear?) rate. Several steps in this direction were made in recent years, see [12, 8, 3, 4, 6, 7, 10].

All known efficient constructions of LTCs rely on some form of "composition" of two (or more) codes. In this paper we focus on composition by tensor product, which is an elementary way to compose two codes. Given two binary codes $R \subseteq \{0,1\}^m$ and $C \subseteq \{0,1\}^n$, their tensor product is the code $R \otimes C$ consisting of all binary $n \times m$ matrices whose rows belong to R and whose columns belong to C.

* Most of the research was done while the authors were visiting Microsoft Research Theory group. Additionally, Irit Dinur's work was supported in part by ISF grant 984/04, Madhu Sudan's work was supported in part by NSF Award CCR-0514915, and Avi Wigderson's work was supported in part by NSF Award CCR-0324906.