Electronic Colloquium on Computational Complexity, Report No. 171 (2010)

A Note on high-rate Locally Testable Codes with sublinear query complexity

Michael Viderman
Computer Science Department
Technion — Israel Institute of Technology
Haifa 32000, Israel
viderman@cs.technion.ac.il

November 12, 2010

Abstract

Inspired by recent construction of high-rate locally correctable codes with sublinear query complexity due to Kopparty, Saraf and Yekhanin (2010) we address the similar question for locally testable codes (LTCs).

In this note we show a construction of high-rate LTCs with sublinear query complexity. More formally, we show that for every $\epsilon, \rho > 0$ there exists a family of LTCs over the binary field with query complexity n^{ϵ} and rate at least $1 - \rho$. To obtain this construction we use the result of Ben-Sasson and Viderman (2009).

1 Introduction

Ben-Sasson and Sudan [2] suggested to use tensor product codes as a means to construct locally testable codes (LTCs) combinatorially. They showed that taking the repeated tensor product of any code $C \subseteq \mathbf{F}^n$ with sufficiently large distance results in a locally testable code with sublinear query complexity and constant rate. Based on their result Meir [6] demonstrated a combinatorial construction of LTCs with constant query complexity and inverse poly-logarithmic rate.

However, these works did not result in LTCs of arbitrary high rate over a field of constant size because for such fields the requirement of large distance in [2] limits the rate to a constant strictly smaller than 1. This problem was solved by Ben-Sasson and Viderman [3] who showed that repeated tensoring can be applied even over the binary field with no distance requirements as in [2]. In this note we stress that the result of [3] implies a simple construction (repeated tensor product) of LTCs over the binary field with sublinear query complexity and arbitrary high rate. More formally, for every $\epsilon, \rho > 0$ there exists a family of LTCs over the binary field with query complexity n^{ϵ}, linear distance and rate $\geq 1 - \rho$.

This note is published in light of the interesting recent construction of locally correctable codes (LCCs) due to Kopparty et al. [5]. They show that for every $\epsilon, \rho > 0$ there exists a family of LCCs with query complexity n^{ϵ}, linear distance and rate $\geq 1 - \rho$. In this note we show that in the area of LTCs similar parameters can be obtained from [3].

ISSN 1433-8092

2 Preliminary Definitions

Throughout this paper, $\mathbf{F}$ is a finite field, $[n]$ denotes the set $\{1, \ldots, n\}$ and $\mathbf{F}^n$ denotes $\mathbf{F}^{[n]}$. All codes discussed in this paper will be a linear. Let $C \subseteq \mathbf{F}^n$ be a linear code over $\mathbf{F}$. We let $\dim(C)$ denote the dimension of C. The rate of the code C is denoted by $\mathrm{rate}(C)$ and defined by $\mathrm{rate}(C) = \dim(C)/n$. We define the *distance* between two words $x, y \in \mathbf{F}^n$ to be $\Delta(x, y) = |\{i \mid x_i \neq y_i\}|$ and the relative distance to be $\delta(x, y) = \frac{\Delta(x,y)}{n}$. The distance of a code is denoted $\Delta(C)$ and defined to be the minimal value of $\Delta(x, y)$ for two distinct codewords $x, y \in C$. Similarly, the relative distance of the code is denoted $\delta(C) = \frac{\Delta(C)}{n}$. For $x \in \mathbf{F}^n$ and $C \subseteq \mathbf{F}^n$, let $\delta(x, C) = \min_{y \in C} \{\delta(x, y)\}$ denote the relative distance of x from the code C.

Locally Testable Codes and their testers

We define LTCs in a standard way. We repeat here the definitions from [3].

Definition 2.1 (LTCs and strong LTCs)**.** A q-*test* is a set of coordinates $I \subseteq [n]$ s.t. $|I| \leq q$. A q-*tester* T is a distribution $\mathbf{D}$ over q-tests, i.e., over subsets $I \subseteq [n]$ s.t. $|I| \leq q$. The tester outputs accept if $w|_I \in C|_I$ and otherwise output reject.

A code $C \subseteq F^n$ is a (q, ϵ, δ)-LTC if it has a q-tester $\mathbf{D}$ such that for all $w \in \mathbf{F}^n$, if $\delta(w, C) \geq \delta$ we have $\Pr_{I \sim \mathbf{D}}[w|_I \notin C|_I] \geq \epsilon$.

A code $C \subseteq F^n$ is a (q, ϵ)-strong LTC if it has a q-tester $\mathbf{D}$ such that for all $w \in \mathbf{F}^n$, we have $\Pr_{I \sim \mathbf{D}}[w|_I \notin C|_I] \geq \epsilon \cdot \delta(w, C)$.

Clearly, a (q, ϵ)-strong LTC is a $(q, \epsilon\alpha, \alpha)$-LTC for any $\alpha > 0$.

Expander Codes

In this section we give the definitions of expander codes as they appear in [1]. We start from the definition of "neighbors" (2.2) and then proceed with the definition of "expansion" (2.3).

Definition 2.2 (Neighbors)**.** Let $G = (V, E)$ be a graph. For $S \subseteq V$, let

- $N(S)$ be the set of neighbors of S.
- $N^1(S)$ be the set of unique neighbors of S, i.e., vertices with exactly one neighbor in S.
- $N^{odd}(S)$ be the set of neighbors of S with an odd number of neighbors in S.

Notice that $N^1(S) \subseteq N^{odd}(S)$.

We note that $N(S)$ and $N^1(S)$ are standard notations, while $N^{odd}(S)$ is not standard and was defined in [1].

Definition 2.3 (Expansion)**.** Let $c, d \in N$ and let $\gamma, \alpha \in (0, 1)$.

Define a (c, d)-bounded (γ, α)-expander to be a bipartite graph (L, R, E) with vertex sets L, R such that all vertices in L have degree $\leq c$, and all vertices in R have degree $\leq d$;

- G is called a (c, d, γ, α)-*expander* if for all subsets $S \subseteq L$ s.t. $|S| \leq \alpha n$ we have $|N(S)| > \gamma \cdot c|S|$

- G is called a (c, d, γ, α)-*odd expander* if for all subsets $S \subseteq L$ s.t. $|S| \leq \alpha n$ we have $|N^{odd}(S)| > \gamma \cdot c|S|$

We say that a code C is a (c, d, γ, α)-*odd expander code* if it has a parity check graph (see [4, Section 2.3]) that is an odd (c, d)-bounded (γ, α)-expander.

Tensor Product Codes

The definitions appearing here are standard in the literature on tensor-based LTCs (e.g. [2, 6, 3]).

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

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

We let $C^{2^0} = C$ and $C^{2^t} = C^{2^{t-1}} \otimes C^{2^{t-1}}$ for $t > 0$. We have the following claim.

Claim 2.4. *Let $C \subseteq \mathbf{F}^n$ be a code and $t > 0$. Then* $\mathrm{rate}(C^{2^t}) = (\mathrm{rate}(C))^{2^t}$ *and* $\delta(C^{2^t}) = (\delta(C))^{2^t}$.

3 Main Result

Theorem 3.1 (Main Theorem)**.** *Let $0 < \epsilon, \rho < 1$. Then there exists $\epsilon' > 0$ (which depends only on ϵ, ρ) and a family of codes $\{C_N\}_N$, s.t.*

- *$C_N \subseteq \mathbf{F}_2^N$ is a (N^ϵ, ϵ')-strong LTC,*
- *$\delta(C_N) = \Omega(1)$ and $\mathrm{rate}(C_N) \geq 1 - \rho$.*

Now we state Proposition 3.2 and Theorem 3.3. The proof of Theorem 3.1, which appears below, will follow from Claim 2.4, Proposition 3.2 and Theorem 3.3.

Proposition 3.2 (Folklore)**.** *For every $\rho > 0$ there exist $c, d, \gamma, \alpha > 0$ and (c, d, γ, α)-odd-expander code $C \subseteq \mathbf{F}_2^n$ s.t.* $\mathrm{rate}(C) \geq 1 - \rho$.

Proof Sketch. Let $\rho > 0$ be a constant. We pick a (c, d)-regular expander code $C \subseteq \mathbf{F}_2^n$ at random s.t. an associated parity check graph (L, R, E) satisfies $|L| = n$, $|R| = \rho n$ and $d = \frac{c}{\rho}$ (which implies that $d \cdot |R| = c \cdot |L|$). Then $\mathrm{rate}(C) \geq 1 - \rho$.

Letting c be sufficiently large it follows that with high probability C is a (c, d, γ, α)-odd expander for some constants $\gamma, \alpha > 0$ which depends only on c and d. The proof of a similar statement appeared in [1, Claim 6.4] and hence we omit it. □

The following theorem is due to Ben-Sasson and Viderman [3, Corollary 13].

Theorem 3.3. *Let $t > 0$ be an integer. Let $C \subseteq \mathbf{F}^n$ be a (c, d, γ, α)-odd expander code. Then C^{2^t} is a (n, ϵ')-strong LTC, where $\epsilon' = \frac{\gamma^t \cdot \alpha^{2^{t+2}}}{(96d^2)^t \cdot 8^{t^2}}$.*

We are ready to prove Theorem 3.1.

Proof of Theorem 3.1. Let $t = \lceil \log(1/\epsilon) \rceil$. Let $\rho_0 > 0$ be s.t. $(\rho_0)^{2^t} \geq \rho$. Proposition 3.2 implies the existence of (c, d, ϵ, α)-odd-expander code $C \subseteq \mathbf{F}_2^n$ s.t. $\mathrm{rate}(C) \geq 1 - \rho_0$, where the constants c, d, ϵ, α depends only on ρ_0. Theorem 3.3 implies that C^{2^t} is a (n, ϵ')-strong LTC, where $\epsilon' = \frac{\gamma^t \cdot \alpha^{2^{t+2}}}{(96d^2)^t \cdot 8^{t^2}}$. Moreover, $\delta(C^{2^t}) = (\delta(C))^{2^t} = \alpha^{2^t} = \Omega(1)$ and $\mathrm{rate}(C^{2^t}) = (\mathrm{rate}(C))^{2^t} \geq (\rho_0)^{2^t} \geq \rho$. Note also that the blocklength of C^{2^t} is $N = n^{2^t}$. Hence $N^\epsilon \geq n$ and so C^{2^t} is a (N^ϵ, ϵ')-strong LTC. □

Acknowledgements

The author would like to thank Eli Ben-Sasson for valuable comments on an earlier draft. The author thanks Swastik Kopparty and Shubhangi Saraf for helpful discussions about locally testable and locally decodable codes.

References

[1] E. Ben-Sasson, P. Harsha, and S. Raskhodnikova, "Some 3CNF properties are hard to test," *SIAM Journal on Computing*, vol. 35, no. 1, pp. 1–21, 2005. [Online]. Available: http://epubs.siam.org/SICOMP/volume-35/art_44544.html

[2] E. Ben-Sasson and M. Sudan, "Robust locally testable codes and products of codes," *Random Struct. Algorithms*, vol. 28, no. 4, pp. 387–402, 2006. [Online]. Available: http://dx.doi.org/10.1002/rsa.20120

[3] E. Ben-Sasson and M. Viderman, "Composition of semi-LTCs by two-wise tensor products," in *APPROX-RANDOM*, ser. Lecture Notes in Computer Science, I. Dinur, K. Jansen, J. Naor, and J. D. P. Rolim, Eds., vol. 5687. Springer, 2009, pp. 378–391. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-03685-9

[4] I. Dinur, M. Sudan, and A. Wigderson, "Robust local testability of tensor products of LDPC codes," in *APPROX-RANDOM*, ser. Lecture Notes in Computer Science, vol. 4110. Springer, 2006, pp. 304–315. [Online]. Available: http://dx.doi.org/10.1007/11830924_29

[5] S. Kopparty, S. Saraf, and S. Yekhanin, "High-rate codes with sublinear-time decoding," in *ECCC - TR10-148*, 2010. [Online]. Available: http://eccc.hpi-web.de/report/2010/148/

[6] O. Meir, "Combinatorial construction of locally testable codes," *SIAM J. Comput*, vol. 39, no. 2, pp. 491–544, 2009. [Online]. Available: http://dx.doi.org/10.1137/080729967

ECCC ISSN 1433-8092

http://eccc.hpi-web.de