Information Processing Letters 116 (2016) 521–525

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Bounds on 2-query Locally Testable Codes with affine tests

Gillat Kol [a,*], Ran Raz [b]

[a] Institute for Advanced Study (IAS), United States
[b] Weizmann Institute of Science, Israel

ARTICLE INFO

Article history:
Received 25 January 2014
Received in revised form 18 February 2016
Accepted 13 March 2016
Available online 17 March 2016
Communicated by A. Muscholl

Keywords:
Locally Testable Codes
Unique Games Conjecture
Computational complexity
Theory of computation

ABSTRACT

We study *Locally Testable Codes* (*LTCs*) that can be tested by making two queries to the tested word using an affine test. That is, we consider LTCs over a finite field $\mathbb{F}$, with codeword testers that only use tests of the form $av_i + bv_j = c$, where v is the tested word and $a, b, c \in \mathbb{F}$.

We show that such LTCs, with high minimal distance, must be of constant size. Specifically, we show that every 2-query LTC with affine tests over $\mathbb{F}$, that has minimal distance at least $\frac{9}{10}$, completeness at least $1-\epsilon$, and soundness at most $1-3\epsilon$, is of size at most $|\mathbb{F}|$.

Our main motivation in studying LTCs with affine tests is the *Unique Games Conjecture* (*UGC*), and the close connection between LTCs and PCPs. We mention that all known PCP constructions use LTCs with corresponding properties as building blocks, and that many of the LTCs used in PCP constructions are affine. Furthermore, the UGC was shown to be equivalent to the UGC with affine tests [13], thus the UGC implies the existence of a low-error 2-query PCP with affine tests. We note, however, that our result has no implication on the correctness of the UGC.

1. Introduction

1.1. Locally Testable Codes

Locally Testable Codes (*LTCs*) are error correcting codes for which the proximity of a given word to a codeword can be probabilistically tested with good confidence. The test should be done by an efficient procedure (a "*tester*") that only reads a *constant* number of locations in the given word. We say that a tester has *completeness* $1-\epsilon$, if it accepts every codeword with probability at least $1-\epsilon$. The tester has *soundness* s, if it accepts any word that is "far" from every codeword with probability at most s.

We mention that one of the main motivations in studying LTCs is their central role in PCP constructions.

1.1.1. Unique Locally Testable Codes

In [16] we study the Unique Games Conjecture by examining LTCs with testers that only read two locations in the tested word, and only use *unique tests*. That is, given the value read from the first queried location, there is a unique value for the second location that makes the tester accept, and vice versa.

In other words, if T is a tester for an LTC $C \subseteq \Sigma^n$, we require that for every pair of coordinates $(i, j) \in [n]^2$ that may be queried by T there exists a permutation π_{ij} over Σ for which the following holds. If $v \in \Sigma^n$ is the tested word, then after querying v_i and v_j, T accepts if and only if $v_j = \pi_{ij}(v_i)$.

1.1.2. Affine Locally Testable Codes

In this work we consider the special case of LTCs with unique tests, where the tests are also *affine*. That is, we assume that the alphabet set is a finite field $\Sigma = \mathbb{F}$, and require every permutation π_{ij} to be of the form $\pi_{ij}(x) =$

* Corresponding author.
E-mail addresses: gillat.kol@gmail.com (G. Kol), ran.raz.mail@gmail.com (R. Raz).

http://dx.doi.org/10.1016/j.ipl.2016.03.008
0020-0190/

$ax+b$, where $a, b \in \mathbb{F}$. In other words, the tests carried out by the testers are of the form $av_i + bv_j = c$, where $v \in \mathbb{F}^n$ is the tested word, $i, j \in [n]$, and $a, b, c \in \mathbb{F}$.

We next give the formal definition of an affine LTC. We use the following notations. For a natural number $t \in \mathbb{N}$, denote $[t] = \{1, \ldots, t\}$. Let $\mathbb{F}$ be a finite field, and let $n \in \mathbb{N}$ be a natural number. The distance between two words $u, w \in \mathbb{F}^n$ is defined as $\Delta(u, w) = \frac{1}{n}|\{i \in [n] \mid u_i \neq w_i\}|$. A subset $C \subseteq \mathbb{F}^n$ is called a code. The relative distance of the code C is $\min_{u \neq w \in C}\{\Delta(u, w)\}$, and the distance of a word $v \in \mathbb{F}^n$ from the code C is $\Delta(v, C) = \min_{u \in C}\{\Delta(v, u)\}$. Let $\mathcal{A}_{\mathbb{F}}$ be the set of all affine functions over $\mathbb{F}$, $\mathcal{A}_{\mathbb{F}} = \{f : \mathbb{F} \to \mathbb{F} \mid f(x) = ax + b,\ a, b \in \mathbb{F},\ a \neq 0\}$.

Definition 1 *(Affine local tester, affine LTC).* Let $\mathbb{F}$ be a finite field, $n \in \mathbb{N}$ be a natural number, and $C \subseteq \mathbb{F}^n$ be a code. Let $\epsilon, s \in [0, 1)$ be real numbers. Assume that T is a probabilistic, non-adaptive, oracle machine with access to a string $v \in \mathbb{F}^n$. In addition, assume that T makes at most two queries to v, and outputs either `accept` or `reject`. Then, T is an (ϵ, s)-affine local tester for C if it satisfies the following conditions:

- **Affineness:** For every pair of coordinates $(i, j) \in [n]^2$ that may be queried by T in a single execution, there exists an affine function $f_{ij} \in \mathcal{A}_{\mathbb{F}}$ such that the following holds. After querying v_i and v_j, T outputs `accept` if and only if $v_j = f_{ij}(v_i)$.
  In addition, if T makes a single query to coordinate $i \in [n]$, then there exists $a \in \mathbb{F}$ such that the following holds. After querying v_i, T outputs `accept` if and only if $v_i = a$.
- **Completeness:** If $v \in C$, then $\Pr[T^v = \texttt{accept}] \geq 1 - \epsilon$.
- **Soundness:** If $\Delta(v, C) \geq \frac{1}{5}$, then $\Pr[T^v = \texttt{accept}] < s$. In other words, if $\Pr[T^v = \texttt{accept}] \geq s$, then there exists a codeword u such that $\Delta(v, u) < \frac{1}{5}$.

A code C is an (α, ϵ, s)-affine LTC if it has relative distance at least $1 - \alpha$, and has an (ϵ, s)-affine local tester.

1.2. Motivation

1.2.1. The PCP Theorem and the Unique Games Conjecture

The celebrated PCP Theorem, discovered in 1992 [3,9,2,1], states that any NP membership statement (e.g., $\varphi \in SAT$) has a proof that can be probabilistically checked with good confidence. The check can be performed by an efficient procedure (a "*verifier*") that only reads a *constant* number of locations in the proof.

The PCP Theorem was a major turning point in the research of hardness of approximation. However, for some fundamental problems, optimal inapproximability results are still not known. To cope with such problems, a strengthening of the PCP Theorem, called the *Unique Games Conjecture* (*UGC*), was introduced by Subhash Khot in 2002 [12]. The conjecture, or variants of it, was shown to imply many improved inapproximability results [12,15,17,7,8,13,14,18].

The UGC considers a special type of PCP verifiers: verifiers that read at most *two* locations in the proof, and only make *unique tests*. The conjecture predicts the existence of such a verifier, that errs (rejects a correct proof or accepts a false statement) with arbitrarily small probability. We mention that the UGC with affine tests is equivalent to the UGC [13].

1.2.2. The relations between PCPs and LTCs

As mentioned above, LTCs and PCPs are closely related. All known PCP constructions use LTCs as building blocks. For example, variants of Reed–Muller, Hadamard, and the Long Code are codes that have been extensively used in PCP constructions. Furthermore, to obtain PCPs with certain properties, one usually uses LTCs with corresponding properties.

In the opposite direction, some PCP constructions were shown to imply LTCs [10]. Moreover, the existence of a special type of PCP, called *PCP of Proximity* (*PCPP*), is known to imply LTCs [4]. For further discussion of the relations between PCPs and LTCs, see [10].

In light of the strong connection between PCPs and LTCs, in [16] we study LTCs analogues to the UGC. Specifically, we consider LTCs with testers that only use *unique tests*. Roughly speaking, we show that such LTCs with low error are of constant size.

In this work we consider the special case of LTCs with unique tests, where the tests are also *affine*. Roughly speaking, we show that such LTCs are of constant size, even if the error is a large constant. As mentioned above, the special case of UGC with affine tests was shown to be equivalent to the UGC [13]. In addition, many of the LTCs used in PCP constructions are affine, e.g., variants of Reed–Muller, Hadamard, and the Long Code.

1.3. Our result

The main result of this paper is the following Theorem 2. The theorem states that every affine LTC with minimal distance at least $\frac{9}{10}$, completeness at least $1 - \epsilon$, and soundness at most $1 - 3\epsilon$, is of size at most $|\mathbb{F}|$.

Theorem 2 *(Main). Let $\epsilon \in \left[0, \frac{1}{3}\right)$ be a real number, $\mathbb{F}$ be a finite field, and $n \in \mathbb{N}$ be a natural number. Then, every $\left(\frac{1}{10}, \epsilon, 1 - 3\epsilon\right)$-affine locally testable code $C \subseteq \mathbb{F}^n$ satisfies $|C| \leq |\mathbb{F}|$.*

Remark 1. The upper bound on the size of the code suggested by the theorem is tight: Let $\mathbb{F}$ be a finite field, and $n \in \mathbb{N}$ be a natural number. Consider the code $C = \{a^n\}_{a \in \mathbb{F}} \subseteq \mathbb{F}^n$, and the following affine local tester for C: Randomly select $(i, j) \in [n]^2$, and test $v_i = v_j$. The code has minimal distance 1, completeness 1, and constant soundness $s < 1$, and $|C| = |F|$.

1.4. Previous works

Unique Locally Testable Codes In [16] we consider LTCs with properties similar to the ones required from a PCP by the UGC. Specifically, we study LTCs with *arbitrarily small constant error* (soundness close to 0), that only make unique tests. We show that such LTCs must be of constant size