New Directions in Coding Theory: Capacity and Limitations

Ameya Velingker
avelingk@cs.cmu.edu

November 30, 2015

Computer Science Department
Carnegie Mellon University
Pittsburgh, PA 15213

Thesis Proposal

Thesis Committee Members:
Venkatesan Guruswami, Chair
Bernhard Haeupler
Gary Miller
Emmanuel Abbe, Princeton University

Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy
Abstract

Error-correcting codes were originally developed in the context of reliable delivery of data over a noisy communication channel and continue to be widely used in communication and storage systems. More recently, error-correcting codes have been shown to have several exciting connections to areas in theoretical computer science.

This thesis proposal explores several new directions in modern coding theory. To this end, we:

1. Show that polar codes over prime alphabets are the first explicit construction of efficient codes to provably achieve capacity for symmetric channels with a polynomial convergence. We introduce interesting new techniques involving entropy sumset inequalities, which are an entropic analogue of sumset inequalities studied in additive combinatorics.

2. Consider the problem of coding over two-party interactive channels. Specifically, we bridge the gap between channel capacities for interactive communication and one-way communication. We also consider a model of one-way communication with partial feedback.

3. Study the problem of list decodability for codes. We resolve an open question about the list decodability of random linear codes and show surprising connections to the field of compressed sensing.

4. Study locally-testable codes and affine invariance. Specifically, we investigate the limitations posed by the local testability property.
## Contents

1. **Introduction** 4
   - 1.1 Overview ................................................. 4

2. **Achieving Channel Capacity for Error-Correcting Codes** 5
   - 2.1 Further Work ............................................. 6

3. **Coding for Interactive Communication** 7
   - 3.1 Background ................................................ 7
   - 3.2 Feedback and Optimal Error Fractions for Binary Coding Schemes 8
   - 3.3 Capacity of Interactive Communication Channels for Low Error Rates ........................................ 9

4. **Structural Properties of Error-Correcting Codes** 12
   - 4.1 List Decodability ........................................... 12
   - 4.2 Local Testability ............................................ 14
1 Introduction

The subject of this thesis is coding theory, or the study of error-correcting codes. Historically, error-correcting codes were developed in the context of reliable communication, in which a sender is trying to transmit a message consisting of symbols to a receiver over a noisy channel. While much research continues to focus on the initial motivation for the field, in recent years, there have emerged a number of new exciting connections of error-correcting codes to other areas. We explore several new directions in coding theory in this proposal.

1.1 Overview

Polar codes. One important question in the realm of coding theory has been the explicit construction of capacity-achieving error correcting codes over various channels. A major breakthrough in this area was made in 2008 by Arıkan, who discovered a new class of capacity-achieving codes known as polar codes. Polar codes are efficiently encodable and decodable and have been shown to achieve capacity for symmetric channels.

Our contribution is to analyze the convergence properties of these codes to capacity. In the process, we introduce an interesting technique involving entropy sumset inequalities.

Coding in the interactive setting. Classical coding theory has primarily dealt with the setting of one-way communication, in which a single party wishes to transmit a message. However, with the advent of such notions such as communication complexity and information complexity, there has recently been much interest in coding for interactive two-party communication protocols. In hopes of better understanding the limits of coding schemes in such a setting, we consider questions regarding feedback as well as the capacity of interactive channels.

List decodability and local testability. We also investigate limitations of error-correcting codes with additional structure. Two important structural notions that have gained importance in recent years are list decodability and local testability. The former allows decoding beyond the unique decoding radius by allowing a decoder to output a small list of possible messages corresponding to a received word. The latter is a notion of locality that allows one to test a received word for membership in the code by querying a small number of positions in the word and has connections to property testing and probabilistically checkable proofs (PCPs).
in complexity theory. In the process of investigating these properties, we introduce some interesting techniques and connections to the area of compressed sensing.

2 Achieving Channel Capacity for Error-Correcting Codes

One of seminal works in the field of information theory and coding theory is Shannon’s noisy channel coding theorem:

**Theorem 2.1** (Shannon’s noisy channel coding theorem). For any discrete memoryless channel $W = (X, Y, \Pi)$, there exists a constant $C(W) \geq 0$ known as the capacity such that:

1. For any $R < C(W)$, for large enough $N$, there exists an error-correcting code over alphabet $X$ of block length $N$ and rate $\geq R$ along with a decoder such that the probability of an error in decoding is $2^{-\Omega(RC(W)(n))}$.

2. For any $R > C(W)$, it is impossible to find an error-correcting code for sufficiently large $N$ such that the probability of an error in decoding is $< \delta$ for all $\delta > 0$.

In fact, the result of Shannon implies that there exists a constant $a_W$ such that for any gap to capacity $\epsilon > 0$ and $N \geq a_W/\epsilon^2$, there exists a binary code $C \subset \{0, 1\}^N$ of rate at least $R \geq C(W) - \epsilon$ that enables reliable communication. Though a random code with the appropriate block length $N$ and rate $I(W) - \epsilon$ satisfies the desired property with high probability, Shannon’s theorem says nothing about how to construct such a code.

Over the past several decades, the existential result of Shannon has guided the quest of coding theorists to find explicit constructions of codes that achieve the parameters guaranteed by random codes while having encoding and decoding procedures that are efficient (say, with running time that is polynomial in $1/\epsilon$ for a gap to capacity of $\epsilon$). Numerous codes have been constructed, but most constructions either fail to provably achieve capacity for a large enough class of channels, or do not have efficient encoders/decoders. For instance, Forney’s construction of concatenated codes has long been known to achieve capacity, but the time complexity of the decoder is unfortunately not efficient in terms of the gap to capacity. Similarly, the widely used low-density parity-check (LDPC) codes are known to
achieve capacity only for the binary erasure channel, while turbo codes are not known to achieve capacity arbitrarily closely.

A recent breakthrough was made in 2008, when Arıkan discovered polar codes, which were shown to achieve capacity for all symmetric binary-input channels \cite{Ari08}. Furthermore, the codes were shown to have encoding and decoding complexity \( O(N \log N) \), where \( N \) is the block length of the code. However, a question remained about how big \( N \) needed to be in terms of the gap to capacity of \( \epsilon \). In order to get efficient encoding and decoding procedures in terms of \( \epsilon \), one needs \( N \) to be \( \text{poly}(1/\epsilon) \). A work of Guruswami and Xia \cite{GX15} showed that this is indeed the case for polar codes over the binary alphabet. We extend this work to \( q \)-ary polar codes over all prime alphabets \cite{GV15}:

**Theorem 2.2** (\cite{GV15}). Let \( W \) be a symmetric channel over a \( q \)-ary input, where \( q \) is prime. Let \( 0 < \epsilon < 1/2 \). Then, for some constant \( c(q) < \infty \) depending only on \( q \), the \( q \)-ary polar code (instantiated with the \( 2 \times 2 \) kernel of Arıkan in \cite{Ari08}) has rate \( R \geq I(W) - \epsilon \), where \( I(W) \) is the capacity of \( W \).

This resolves a longstanding open question by showing that polar codes over prime alphabet are the first-known construction of explicit efficient codes to provably achieve capacity for symmetric channels with a polynomial speed of convergence to capacity. Furthermore, the main proof technique we use is to establish an entropy sumset inequality:

**Theorem 2.3** (\cite{GV15}). Let \( (X_i, Y_i), i = 1, 2 \) be i.i.d. copies of a correlated random variable \( (X, Y) \) with \( X \) supported on \( \mathbb{F}_q \) for a prime \( q \). Then for some \( \alpha(q) > 0 \) depending only on \( q \),

\[
H(X_1 + X_2|Y_1, Y_2) - H(X|Y) \geq \alpha(q) \cdot H(X|Y)(1 - H(X|Y)).
\]

The entropic sumset inequality may be viewed as an entropic analogue of the usual sumset inequalities that are commonly studied in the field of additive combinatorics. The constant \( \alpha(q) \) that we achieve is \( \alpha(q) = 1/\text{poly}(q) \).

### 2.1 Further Work

As mentioned in the previous section, polar codes provide the first-known construction of explicit error-correcting codes that are efficiently encodable/decodable and provide polynomial speed of convergence to capacity over all symmetric prime arity channels. However, the dependence of the block length on \( N \) on the
gap to capacity $\epsilon$ depends poorly on the arity $q$. In particular, \[GV15\] shows that it suffices to take $N \geq (1/\epsilon)^{\text{poly}(q)}$. In fact, for $q = 2$ (the binary case), one can take $N \geq (1/\epsilon)^c$ where $c \approx 3.5$ \[HAU14\]. On the other, for a random code, it suffices to take $c = 2$. Thus, our objective is to close this gap:

**Objective 2.4.** Establish explicit capacity-achieving error-correcting codes whose speed of convergence to capacity matches the guarantees obtained by random codes.

One possible route is to obtain a tighter bound than the one in \[GV15\] by improving the entropy sumset inequality that is used in the proof technique. It may be possible to reduce the exponent from $c = \text{poly}(q)$ to $c = O(\text{polylog}(q))$ via such an approach by proving Theorem 2.3 with $\alpha(q) = 1/\text{poly}(q)$. This leads us to the following concrete question:

**Question 2.5.** Is it possible to obtain a tighter analysis of the speed of convergence to capacity of polar codes by improving entropy sumset inequalities?

Another interesting approach to tightening the gap between polar codes and random codes is to consider different kernels. The construction of polar codes is a recursive construction that involves an underlying polarizing kernel (an invertible matrix). The standard kernel that has been used by Arıkan \[Ari08\] as well as other works such as \[HAU14, GV15\] is the $2 \times 2$ matrix $K = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. However, it is possible that using larger kernels could provide better polynomial bounds:

**Question 2.6.** Can polar codes based on larger $\ell \times \ell$ polarizing kernels (for $\ell > 2$) achieve a tighter polynomial dependence of block length on inverse gap to capacity with scaling exponent $c \approx 2$?

As a motivating factor for studying this direction, it is known that in the limit $\ell \to \infty$, one can achieve a scaling exponent $c \approx 2$ because of the known behavior of random linear codes. Thus, it would be an interesting question to study the dependence of $\ell$ and $c$.

3 Coding for Interactive Communication

3.1 Background

While error-correcting codes have traditionally been concerned with making one-way communication reliable, one can ask whether there is a similar analogue in
the context of analyzing interactive communication protocols. This is a natural question in light of recent interest in problems relating to communication complexity and information complexity of computational tasks. In this setting, one wishes to encode an arbitrary two party communication protocol into a longer protocol that can handle errors in the communication.

This problem was first addressed by Schulman [Sch96], who showed that it is possible to find coding schemes that tolerate a non-zero fraction of errors, namely, $\epsilon = 1/240$. This work was later built upon by Braverman and Rao [BR14], who showed that any adversarial error fraction $\epsilon < 1/4$ can be tolerated, provided that one can use symbols from a larger alphabet in communication, and that this bound is optimal. Subsequent works [BE14, GH14, GHS14] have worked to determine the error rate region under which non-zero communication rates can be obtained for a variety of models, e.g., adversarial errors, random errors, list-decoding, while many more recent works [KR13, Hae14] have focused on determining the optimal communication rate or overhead for tolerating low error fractions.

3.2 Feedback and Optimal Error Fractions for Binary Coding Schemes

One problem that our work seeks to address is the problem of one-way communication in the presence of partial feedback. In order to motivate the problem, we first consider the following fundamental question asked in [BR14]:

**Question 3.1.** What is the maximum adversarial error fraction $\epsilon$ that can be tolerated by a binary coding scheme that encodes an arbitrary two-way protocol?

While [BR14] showed that any adversarial error fraction $\epsilon < 1/4$ can be tolerated by encoding a given protocol into a longer protocol, approaching $1/4$ arbitrarily closely requires use of symbols from an alphabet that grows. If one restricts to coding schemes in which the output is a binary protocol, then the coding scheme of [BR14] only allows one to tolerate error rates up to $1/8$, and indeed, this is the best known bound so far.

On the other hand, it is known that a binary coding scheme cannot tolerate an error fraction of $1/6$ or more. This bound follows from an impossibility result for the problem of communication with noiseless feedback [Ber64, EGH15]. In this setup, the Alice and Bob communicate over a noisy channel, but the sender has access to an uncorrupted feedback channel. Essentially, one can show an upper limit of $1/3$ for the fraction of errors that one can tolerate in an interactive
coding scheme over channels with feedback, and this translates to the $1/6$ bound for Question 3.1. It should be noted that the problem of communication with noiseless feedback is also related to the classic game of “Twenty Questions with a Liar” [SW92].

With an eye on Question 3.1 and given the role that feedback channels play in bounds for Question 3.1 we study a related problem of communication in the presence of partial noiseless feedback. In this setting, Alice wishes to communicate a message to Bob but does not receive feedback bits for every single bit that she sends. Rather, Alice can only receive feedback bits for up to a $\delta$ fraction of the bits she sends. The question is to determine the optimal error fraction $\epsilon$ one can tolerate as a function of $\delta$. The case $\delta = 0$ corresponds to the usual case of one-way communication without feedback (in which the limit is $\epsilon = 1/4$, by use of an error-correcting code), while the case $\delta = 1$ corresponds to the full feedback case (in which $\epsilon = 1/3$ is known to be the answer [Ber64, EGH15]). Our work shows lower bounds on the optimal error fraction as we interpolate between $\delta = 0$ and $\delta = 1$ [HKV15]:

**Theorem 3.2.**

The tightness of the above result is not known. There are some further avenues for extending this work that could be a stepping stone to resolving Question 3.1.

**Question 3.3.** What error fractions can be tolerated for one-way communication with partial noisy feedback?

The feedback problem that we have considered in Theorem 3.2 of [HKV15] is essentially a first step for the corresponding problem in which feedback is noisy, i.e., can be corrupted by an adversary. Showing impossibility results for the noisy analogue of the problem provides an approach to proving better bounds than $1/6$ for Question 3.1. Thus far, very little if anything is known about limits of one-way communication in the presence of partial noisy feedback.

### 3.3 Capacity of Interactive Communication Channels for Low Error Rates

While the problems mentioned in the previous section deal with determining optimal error fractions that can be tolerated by interactive coding schemes, another interesting question is to determine what communication rates can be achieved for
various error rates. Here, we concentrate on small error rates $\epsilon > 0$ that are close to 0.

In the setting of non-interactive one-way communication, the classical result of Shannon shows that the capacity of a binary symmetric channel with error rate $\epsilon$ is $1 - H(\epsilon)$. Furthermore, for the case of adversarial errors, in which an adversary is allowed to introduce any error pattern of up to an error fraction of $\epsilon$, the capacity is known to be $1 - \Theta(H(\epsilon))$ (as suggested by the Gilbert-Varshamov and Hamming bounds). However, this leaves the question of capacity in an interactive setting.

One of the first works to consider the question of communication rate in an interactive setting is the work of Kol and Raz [KR13]. Their work showed that under a certain model, in which the output protocol of a coding scheme is restricted to be non-adaptive, one can achieve matching lower and upper bounds of $1 - \Theta(\sqrt{H(\epsilon)})$ for the capacity of an interactive communication channel that corrupts each transmitted bit with probability $\epsilon$ (in other words, the binary symmetric channel with error parameter $\epsilon$). Therefore, there is a gap between the capacities in the non-interactive and interactive settings.

A subsequent work of Haeupler [Hae14] showed that allowing adaptivity in the output protocol (i.e., a non-fixed speaking order) can allow communication rates that surpass the bound of [KR13]. Specifically, Haeupler showed that for random errors or oblivious adversarial errors (where an adversary must commit to an error pattern at the start of the protocol), there is a randomized coding scheme that allows one to achieve an error rate of $1 - O(\sqrt{\epsilon})$. Furthermore, in the case of full adversarial errors, he showed that a capacity of $1 - O(\sqrt{\epsilon \log \log(1/\epsilon)})$ is achievable. These respective error rates are conjectured to be optimal, though this has not yet been proved. This leads to the following natural question:

**Question 3.4.** Is it possible to show the optimality of the best-known communication rates of $1 - \sqrt{\epsilon}$ and $1 - \sqrt{\epsilon \log \log(1/\epsilon)}$ for random errors and adversarial errors with low error fraction $\epsilon > 0$?

One potential approach to resolving the question would be to use lower-bound techniques from [KR13].

While the result of [Hae14] is somewhat disappointing in that the (conjectured to be optimal) communication rates are worse than the $1 - \Theta(H(\epsilon))$ rate achievable for non-interactive communication, it does leave open some interesting questions. In particular, the hardest protocols to encode under the underlying coding schemes of Haeupler seem to be “maximally alternating” protocols, those in which Alice and Bob alternate speaking after every bit. However, most protocols that are likely to show up in real-world applications do not have a speaking order that alternates
so rapidly. This leaves open the possibility for some assumptions on the input protocol that would allow coding schemes with better rates:

**Question 3.5.** Is there a reasonable set of assumptions under which a two party protocol can be encoded into a longer protocol that is resilient to an $\epsilon$ error fraction of fully adversarial errors with a communication rate of $1 - O(\epsilon \log(1/\epsilon))$?

Another shortcoming of [Hae14] is that while the coding schemes are rather simple and elegant, they have virtually nothing in common with error-correcting codes and techniques for non-interactive communication that have been developed over the past several decades. This is true for other interactive coding schemes from past works as well, where seemingly disparate methods have been used across several works. More specifically, the early works in the field [Sch96, BR14] used the combinatorial object of tree codes to construct coding schemes, while latter works [GHS14, GH14, Hae14] that obtain efficient schemes have used no such objects and are much simpler. Explicit efficient constructions of tree codes have thus far eluded researchers; on the other hand, tree codes are a nice clean combinatorial object that appears to be a natural analogue to the sphere packing interpretation of normal error-correcting codes. Thus, we consider the following goal.

**Objective 3.6.** Find a unifying mathematical theory for coding of (two-way) interactive protocols that relates to coding theory for one-way communication.

In our work, we address both Question 3.5 and Objective 3.6. In particular, with regards to Question 3.5 we establish the notion of a protocol’s average message length $\ell$, or the average number of rounds for which a party communicates before receiving a reply from the other party, as a natural measure of the amount of interaction in a protocol. As an example, for an $n$-round protocol, the case $\ell = 1$ corresponds to a “maximally alternating” protocol, while the case $\ell = n$ corresponds to a non-interactive protocol (one-way message). Our work shows that for protocols that have an average message length above some constant (in $\epsilon$) threshold, one can obtain a coding scheme that achieves a communication rate of $1 - O(H(\epsilon))$, which, up to constant factors in front of the second term, matches the optimal communication rate in the one-way setting [HV15]!

**Theorem 3.7** ([HV15]). Suppose $\Pi$ is an interactive protocol between Alice and Bob. Then, for sufficiently small $\epsilon > 0$, there exists another protocol $\Pi_{\text{oblivious}}$ that successfully simulates $\Pi$, with high probability, in the presence of oblivious adversarial errors with error fraction $\epsilon$, provided that the average message length of $\Pi$ is
\( \ell = \Omega(\text{poly}(1/\epsilon)). \) Furthermore, the communication rate is \( 1 - \Theta(\epsilon \log(1/\epsilon)) = 1 - \Theta(H(\epsilon)). \)

One should note that the underlying assumption on the average message length is fairly modest, as it is constant in \( \epsilon. \) Thus, for most “reasonable” protocols, it is possible to achieve the optimal \( 1 - \Theta(H(\epsilon)) \) capacity that is achievable for one-way protocol under oblivious adversarial or random noise. Moreover, our interactive coding scheme uses rateless error-correcting codes in the construction. These are error-correcting codes that have incremental distance properties and allow for error correction of messages in settings where the error rate is not known in advance. The use of such techniques somewhat addresses Objective 3.6. Other techniques that we use include information hiding as well as use of a regularization procedure called blocking.

One point of interest is that the coding scheme we provide seems to be a rateless coding scheme. One direction that is currently in progress is to figure out what rateless guarantees the encoded protocol \( \Pi_{\text{oblivious}}^{\text{enc}} \) of Theorem 3.7 provides.

Another interesting follow-up to our work would be to investigate Question 3.5 in the presence of full adversarial noise, where our current techniques seem to fall short.

4 Structural Properties of Error-Correcting Codes

In this section, we consider problems that investigate limitations of error-correcting codes with certain additional locality structures (e.g., list decodability, local testability). We describe these works below.

4.1 List Decodability

One desirable property of an error-correcting code is list decodability. List decoding is an alternative to unique decoding and operates on the principle that the decoding algorithm of an error-correcting code can output a list of possibilities instead of a single message. The advantage of list decodability is that it allows decoding up to a radius that goes beyond the unique decoding radius. As is generally the case with arguments in coding theory, a random error-correcting code with appropriate parameters has reasonable list-decoding properties. In particular, an easy argument (similar to Shannon’s proof of capacity of the binary symmetric channel) shows that a random \( q \)-ary code of rate \( R = \Omega_q(\epsilon^2) \) is \( (1 - 1/q - \epsilon, \text{poly}(1/\epsilon)) \)-list decodable (meaning that one can decode the code up to a radius of \( 1 - 1/q - \epsilon \)
with a $L = \text{poly}(1/\epsilon)$ list size). Over the past few decades, several explicit constructions of list-decodable codes have been obtained, culminating with folded Reed-Solomon codes, which achieve the list decoding radius guaranteed by random codes [Sud97, GS99, PV05, GR06]. However, one question that remained open for a while was whether random linear codes (where one samples $Rn$ random vectors in $F_q^n$ and let the code $C$ be their $F_q$-span) perform similarly well.

Our work [CGV13] essentially answers this question and shows the following:

**Theorem 4.1 ([CGV13]).** Let $q$ be a prime power, and let $\epsilon > 0$ be a constant parameter. Then for some constant $a_q > 0$ only depending on $q$ and all large enough integers $n$, a random linear code $C \subseteq F_q^n$ of rate $R = a_q \epsilon^2 / \log^3(1/\epsilon)$ is $(1 - 1/q - \epsilon, O(1/\epsilon^2))$-list decodable with probability at least 0.99. (One can take $a_q = \Omega(1/\log^4 q)$.)

It should be noted that the parameters above match a known lower bound of $L = \Omega_q(1/\epsilon^2)$ and upper bound of $R = O_q(\epsilon^2)$ up to polylogarithmic factors. Previously, only existence but not abundance of such codes was known for $q = 2$ [GHSZ02].

What is interesting is that our proof technique relates list decoding guarantees to the Restricted Isometry Property (RIP) for random submatrices of the $N \times N$ Hadamard-Walsh transform matrix (or discrete Fourier transform matrix), a notion that is important in the field of compressed sensing. In particular, our work improves the upper bound on the number of rows needed for a subsampled Fourier matrix to satisfy the RIP property of order $k$ to $O(k \log^3 k \log N)$ (from the $O(k \log^6 N)$ bound of Candès and Tao [CT06] as well as the subsequent improved $O(k \log^2 k \log(k \log N) \log N)$ bound of Rudelson and Vershynin [RV08]). This improvement for the RIP problem is critical for the list-decoding problem, as it allows one to show an average-distance guarantee for random linear codes, which is then used in conjunction with a relaxed version of the well-known Johnson bound. However, the RIP question is also interesting in its own right. It should be noted that a further improvement to our RIP upper bound has been subsequently made by Haviv and Regev [HR15], who show an upper bound of $O(k \log^2 k \log N)$. Furthermore, Wootters [Woo13] has subsequently improved our list decodability result by removing the polylogarithmic factors in $1/\epsilon$ in the rate, though the techniques used in the work do not have any implications for the aforementioned RIP problem.
4.2 Local Testability

Another property of interest in the context of error-correcting codes is local testability. Locally testable codes (LTCs) are codes that are equipped with a tester, a randomized algorithm that queries the received word at a few positions and decides whether the word is a valid codeword. The tester is required to accept valid codewords with probability 1 and reject words that are far (in Hamming distance) from the code with nontrivial probability. LTCs have been the subject of much interest due to their connections to probabilistically checkable proofs (PCPs) and property testing.

Most literature has centered on the study of LTCs with a constant or sublinear number of queries. However, my work centers on high-rate LTCs, in which the underlying tester is allowed to make a linear number of queries. One motivation for studying the linear regime is a beautiful connection between such LTCs and the construction of small set expander graphs [BGH+12].

The specific question we consider is as follows. The \( n \)-variate binary Reed-Muller (RM) code of constant distance \( d \) has a dimension that is approximately \( N - (\log N)^{\log d - 1} \), where \( N = 2^n \). Moreover, the RM code is locally testable with \( 2N/d \) queries. On the other hand, a BCH code of constant distance \( d \) has a dimension that is roughly \( N - \frac{d}{2} \log N \), and this is optimal (up to lower order terms) by the Hamming bound for codes. However, unlike the RM code, the BCH code is not testable with \( O(N/d) \) queries. This raises the following question.

**Question 4.2.** How significant of a limitation does the local testability requirement (with \( O(N/d) \) queries) pose on the dimension of a binary code of distance \( d \) and block length \( N \)?

In other words, the question seeks to answer whether the highest possible dimension of an LTC with distance \( d \) is closer to that of BCH or RM. The construction of a code that has better dimension than the RM code would imply small set expanders whose Laplacians have a large number of small eigenvalues, and this has connections to the theory of approximation algorithms [BGH+12].

We show that under certain assumptions, the testability requirement is a severe limitation, and a slightly higher dimensional variant of RM codes known as lifted codes (see [GKS13]) is essentially optimal. The formal theorem is as follows.

**Theorem 4.3 ([GSVW15]).** Let \( C \supseteq \text{RM}(n - \log d, n) \) be a linear affine-invariant code of block length \( N = 2^n \) that has distance \( d \) and is testable with \( \frac{2N}{d} \) queries. Then, \( \dim(C^\perp) \geq \left( \frac{n}{\log^2 d} \right)^{\log d - 1} \).
Our result applies to codes for which the assumption of affine invariance holds. Affine invariance is a symmetry property that is satisfied by many interesting classes of codes (e.g., BCH codes, RM codes, lifted codes). A natural question would be to determine whether we can prove a similar result under fewer assumptions. Also, it would be interesting to determine whether there are non-affine-invariant codes that are locally testable with the appropriate number of queries while having a dimension that is closer to that of BCH codes.

References


[GSVW15] Venkatesan Guruswami, Madhu Sudan, Ameya Velingker, and Carol Wang. Limitations on testable affine-invariant codes in the high-rate


[PV05] Farzad Parvaresh and Alexander Vardy. Correcting errors beyond the guruswami-sudan radius in polynomial time. In *46th Annual IEEE*


