Localized Error Correction in Projective Space

Ning Cai

Xidian University

20 Aug, 2012

INC, CUHK
1 Previous Works and Background

2 The Model

3 The Main Results

4 The Outline of the Direct Proof

5 Proof of the Converse

6 The Conclusion
In the standard coding theory, the assumption is that neither sender nor receiver has side information about the state of the channel. For the erasure error correction, it is assumed that the receiver knows at which coordinates errors may occur but the sender has no side information of the channel. The localized error correction, introduced by Bassalygo-Gelfand-Pinsker, is in the third case that the sender initially knows the possible error positions before choosing codeword but the receiver knows nothing about it. Their motivation for introducing the model is writing on unreliable medium. They considered the fact that the writer (sender) may know the unreliable cells in the medium initially. This prior knowledge can help us to improve the error correction.
Previous Works and Background

Binary Localized Error Correction Code, Bassalygo-Gelfand-Pinsker, 1989

- The message is encoded into a codeword of length $n$ and sent via a noisy channel.
- The states of the channel are described by configurations $J$, $t$-subsets of $[n] := \{1, 2 \ldots, n\}$.
- Bits in the current configuration of the channel possibly are flipped by the noise during the transmission.
- No error occurs at the components of out of the configuration.
- The encoder initially knows the configuration and so he can choose codeword according to not only the message but also the configuration.
- The decoder knows nothing about the configuration.
Previous Works and Background

- The rates of binary localized error correction codes are upper bounded by Hamming Bound.
- Hamming Bound is asymptotically achievable by binary localized error correction codes and therefore actually it is the capacity of binary localized error correction codes.
- Side information of configuration is helpful because in general Hamming bound is not achievable by error correction codes without the side information.
Previous Works and Background

- The problem itself is a beautiful combinatorial problem.
- Generalizations to non-binary and other scenarios,
  (Bassalygo-Gelfand-Pinsker 1991,
  Ahlswede-Bassalygo-Pinsker, 1993,1994..., 
  Ahlswede-Deppe-Lebedev 2005,...)
Code in projective space, (code for operator channel, or non-coherent network error correction code etc)
Kötter-Kschischang, 2008

- Codewords are $x$-dim subspaces of an $n$-dim space $N$ (the ground space) i.e., members of Grassmannian $G(n, k)$.
- A $z_1$-dim subspace of a codeword may be deleted from codewords and a $z_2$-dim subspace may be added to codewords, by the noise during the transmission.
- A code in projective space is a $z$-error correction code if it is able to correct $z_1$ deleting errors and $z_2$ injecting errors simultaneously, for all $z_1 + z_2 \leq z$. 
Previous Works and Background

The subspace stance of codewords $X$ and $X'$ is defined as

$$d(X, X') := \dim(X + X') - \dim(X \cap X').$$

- It was proven that a code corrects $z$ errors iff its minimum subspace distance is larger than $2z$.
- Several bounds analogue to the bounds for error correction codes in Hamming space, (e.g. Gilbert-Varshamov bound, Hamming bound, Singleton bound, Johnson bound, ...) were derived.
- The code is a hot topic for research and it is likely much more complicate than error correction codes in Hamming space.
Two well known posets

**boolean lattice** with ground set \([n] = \{1, 2, \ldots, n\}\) and **subspace lattice** with of an \(n\)-dim ground space \(N\)

<table>
<thead>
<tr>
<th>Boolean Lattice</th>
<th>Subspace Lattice</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a^n \in {0, 1}^n \leftrightarrow S(a^n) := {i : a_i = 1})</td>
<td>(V \subset N)</td>
</tr>
<tr>
<td>(w_H(a^n) \leftrightarrow</td>
<td>A</td>
</tr>
<tr>
<td>(a^n \land b^n \leftrightarrow A \cap B)</td>
<td>(U \cap V)</td>
</tr>
<tr>
<td>(a^n \lor b^n \leftrightarrow A \cup B)</td>
<td>(U + V)</td>
</tr>
<tr>
<td>(d_H(a^n, b^n) \leftrightarrow</td>
<td>A \cup B</td>
</tr>
</tbody>
</table>

because \(d_H(a^n, b^n) = |S(a^n) \cup S(b^n)| - |S(a^n) \cap S(b^n)|\) and \(d(U, V) = \text{dim}(U + V) - \text{dim}(V \cap U)\).

Error correction code in the binary Hamming space \(\sim\) error correction codes in projective space

binary localized error correction code \(\sim\) ?
The Model

In the following we want to extend the localized error correction code to operator channel \textit{analogously}.

- As the configurations for the binary $t$-localized error correction codes are $t$-subsets of the ground set $\{1, 2, \ldots, n\}$, we take $z$-dim subspaces of $N$ as our configurations.

- Suppose a channel in binary Hamming space is governed by a configuration $J$ and a codeword $x^n$ is sent through the channel. Then by definition of the binary localized error, a subset in $S(x^n) \cap J$ is possibly removed from $S(x^n)$ and a subset in $J \cup S(x^n)$ is possibly added to $S(x^n)$. Subsequently we assume that a subspace in $X \cap Z$ may be erased from $X$ and a subspace in $X + Z$ may be injected to the codeword $X$ if the input and the configuration of the channel are $X$ and $Z$ respectively.
The Model

• Again we assume the encoder knows the configuration but the decoder does not know it.

• Note that for the localized error correction in binary Hamming space, the set of the possible output sequences is

\[
\text{Out}(x^n, J) := \{y^n : S(y^n) \subset S(x^n) \cup J, \\
(S(y^n) \cap S(x^n)) \cup (J \cap S(x^n)) = S(x^n)\},
\]

when a codeword \(x^n\) is sent through a channel governed by a configuration \(J\);

whereas for localized error correction in projective space, the set of the possible output subspaces is

\[
\mathcal{Y}(X, Z) := \{Y : Y \subset X + Z, (Y \cap X) + (Z \cap X) = X\},
\]

when the codeword \(X\) is sent through a channel governed by the configuration \(Z\).
Although the two output sets are analogue to each other formally,

\[ |Out(x^n, J)| = 2^{|J|} \]

depends only on \( J \) and is independent of \( w_H(x^n) \) and relative positions of the codeword and the configuration,
The Model

\[ |\mathcal{Y}(X, Z)| = \sum_{y=x}^{x} \sum_{z=y}^{z-\lambda+w} q^{(x+y-\lambda-w)(x-w)} \begin{bmatrix} \lambda \\ w + \lambda - x \end{bmatrix} \begin{bmatrix} z - \lambda \\ y - w \end{bmatrix}, \]

depends on the dimensions of \( X, Z \) and \( X \cap Z \), where

\[ \begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{\prod_{j=0}^{k-1} (q^n - q^j)}{\prod_{j=0}^{k-1} (q^k - q^j)}, \]

is the Gaussian coefficient, the number of \( k \)-dimensional linear subspaces in an \( n \)-dimensional linear space over \( GF(q) \), \( \dim X = x, \dim Z = z \), and \( \dim X \cap Z = \lambda \).
For example,

\[ |\mathcal{V}(X, Z)| = \sum_{v=0}^{z} q^{(x-z)(z-v)} \begin{bmatrix} z \\ v \end{bmatrix}. \]

if \( Z \subset X \) whereas

\[ |\mathcal{V}(X, Z)| = \sum_{u=0}^{z} \begin{bmatrix} z \\ u \end{bmatrix} \]

if \( X \cap Z = \{0\} \).

This makes difference between our code and localized error correction code in Hamming space and makes our problem more difficult.
The Model

• A $z$-localized error correction code in projective space is called an $(n, m)$ $z$-localized error correction code in projective space, (or $(n, m)$ $z$-LECCPS in short), if the dimension of the ground space is $n$ and the cardinality of message set is equal to $m$.

• Denote by $\mathcal{V}(n)$, the set of linear subspaces in $N$, and by $\mathcal{G}(n, k)$, the set of $k$-dim linear subspaces in $N$ (i.e., so-called Grassmannian). Then for an $(n, m)$ $z$-LECCPS, the configurations take values in $\mathcal{G}(n, z)$.

• An $(n, m)$ $z$-LECCPS is specified by its encoding function $\phi : M \times \mathcal{G}(n, z) \to \mathcal{V}(n)$ and decoding function $\psi : \mathcal{V}(n) \to M$ with $\psi(Y) = i$ for all $Y \in \mathcal{V}(\phi(i, Z), Z), i \in M$ and $Z \in \mathcal{G}(n, z)$. 
The Model

- An \((n, m)\) \(z\)-LECCPS is called an \((n, m)\) \(x\)-constant dimensional \(z\)-localized error correction code in projective space (or \((n, m)\) \([x, z]\)-CDLECCPS in short) if all codewords have the dimension of \(x\) (i.e., \(\phi\) takes values in \(G(n, x)\)).

- We are interested in the asymptotic behaves of the codes. We fix \(\xi := \frac{x}{n}\) and \(\tau = \frac{z}{n}\) and let \(n \to \infty\). The rate of an \((n, m)\)-code in projective space is defined as \(\frac{1}{n^2} \log_q m\), where \(q\) is the order of the coding field, because

\[
|G(n, x)| = \begin{bmatrix} n \\ x \end{bmatrix} = q^{n^2[\xi(1-\xi)+o(1)]}
\]

if \(\xi = \frac{x}{n}\).
The Model

• Thus for $\xi, \tau \in (0, 1)$, $R \geq 0$, we say $R$ is $(\xi, \tau)$-CDLECCPS achievable if for any $\epsilon > 0$ and sufficiently large $n$, there is an $(n, m) (n\xi, n\tau)$-CDLECCPS with $\frac{1}{n^2} \log_q m > R - \epsilon$. The maximum $(\xi, \tau)$-CDLECCPS achievable rate is defined as $(\xi, \tau)$-CDLECCPS capacity and denoted by $C'(\xi, \tau)$.

• For non-constant dimensional codes, the $\tau$-LECCPS capacity is defined in the same way and denoted by $C^*(\tau)$.

• Obviously

$$\max_{\xi} C'(\xi, \tau) \leq C^*(\tau)$$

because an $(n, m) (n\xi, n\tau)$-CDLECCPS is an $(n, m)$ $n\tau$-LECCPS.
The Main Results

Direct Coding Theorem for CDLECCPS

\[ C'(\xi, \tau) \geq \xi [1 - (\xi + \tau)], \]

provided that \( \tau < \xi \leq \frac{1}{2} \).
Converse Coding Theorem

\[
m \leq \sum_{d = \max(x, z)}^{x + z} \begin{bmatrix} n \\ d \end{bmatrix} \begin{bmatrix} d \\ z \end{bmatrix},
\]

if there exists an \((n, m) (x, z)\)-CDLECCPS, and

\[
m \leq \sum_{d = x}^{n} \begin{bmatrix} n \\ d \end{bmatrix} \begin{bmatrix} d \\ z \end{bmatrix},
\]

if there exists an \((n, m) x\)-LECCPS.
The Main Results

By the estimation of Gaussian coefficients we conclude that the logarithms of the two upper bounds in the converse theorem are asymptotically equal to

\[ n^2 \left[ \max_{\Delta \leq \xi + \tau} (1 - \delta)(\delta - \tau) + o(1) \right] \]

and

\[ n^2 \left[ \max_{\Delta \leq 1} (1 - \delta)(\delta - \tau) + o(1) \right] \]

respectively. For fixed \( \tau \), the function \((1 - \delta)(\delta - \tau)\) achieves its maximum value \( \frac{(1-\tau)^2}{4} \) at point \( \delta_0 = \frac{1+\tau}{2} \). When \( \xi + \tau \leq \delta_0 \), or equivalently \( \xi \leq \frac{1-\tau}{2} \), \( \delta_0 \) falls out of the interval \([\max(\xi, \tau), \xi + \tau]\). Therefore in this case the maximum value of the function in the interval is achieved at the boundary point \( \xi + \tau \) and takes the value \( \xi[1 - (\xi + \tau)] \). Thus we have that
The Main Results

Corollary

\[ C'(\xi, \tau) \leq \begin{cases} \xi(1 - (\xi + \tau)) & \text{if } \xi \leq \frac{1-\tau}{2} \\ \frac{(1-\tau)^2}{4} & \text{else,} \end{cases} \]

and

\[ C^*(\tau) \leq \frac{(1 - \tau)^2}{4}. \]

By combining this with direct part of coding theorem for CDLECCPS, we have that

\[ C(\xi, \tau) = \xi[1 - (\xi + \tau)], \]

provided that \( \tau < \xi \leq \frac{1-\tau}{2} \).
Next we turn to the lower bound $\xi[1 - (\xi + \tau)]$ of $C(\xi, \tau)$, in the case that $\tau < \xi \leq \frac{1}{2}$. For a fixed $\tau$, the function $\xi[1 - (\xi + \tau)]$ takes its maximum value $\frac{(1-\tau)^2}{4}$ at point $\xi_0 = \frac{1-\tau}{2}$. Let $\tau < \frac{1}{3}$, and then $\tau < \xi_0 \leq \frac{1}{2}$. Thus we may apply the direct coding theorem of CDLECCPS for $\xi = \xi_0$ to achieve the upper bound of $C^*(\tau)$ by a $(\xi_0, \tau)$-CDLECCPS. Therefore

$$C^*(\tau) = \frac{(1 - \tau)^2}{4}$$

if $\tau < \frac{1}{3}$. By summery above, we have

**Coding Theorem**

$$C(\xi, \tau) = \xi[1 - (\xi + \tau)], \text{ if } \tau < \xi \leq \frac{1 - \tau}{2},$$

and

$$C^*(\tau) = \frac{(1 - \tau)^2}{4} \text{ if } \tau < \frac{1}{3}.$$
The Main Results

When $\tau > \frac{1}{3}$, $\xi_0 < \tau$ and therefore we may not apply the direct coding theorem to approach the upper bound of $C^*(\tau)$ by a $(n\xi_0, n\tau)$-CDLECCPS. As a matter of fact, we can choose a $\xi$ arbitrarily close to $\tau$ then the lower bound $\xi[1 - (\xi + \tau)]$ for the $(\xi, \tau)$-CDLECCP is arbitrarily close to $\tau(1 - 2\tau)$. Namely, $\tau(1 - 2\tau)$ is achievable. By combining this with the upper bound, we have

**Proposition** For $\tau \geq \frac{1}{3}$,

$$\tau(1 - 2\tau) \leq C^*(\tau) \leq \frac{(1 - \tau)^2}{4}.$$  

The gap between of the two bounds in the proposition is

$$\frac{(1 - \tau)^2}{4} - \tau(1 - 2\tau) = \frac{(3\tau - 1)^2}{4}.$$
The Main Results

As the gap is due to the condition that $\tau < \xi$ in lower bound of $C(\xi, \tau)$, probably to determine $C(\xi, \tau)$ and $C^*(\tau)$ completely, we have to remove the condition from the direct theorem. We set up the condition because without the condition, all codewords would be unavoidably contained by some configurations. We employ the minimum subspace distance decoder, a natural decoder, as our decoding function in the proof and in this case one may not decode correctly by minimum distance decoder.

To determine $C^*(\tau)$ and $C(\xi, \tau)$ completely probably we need:
- to use an alternative decoder and/or
- to find a better upper bound.
But currently we leave it open.
The Main Results

Denote the lower bound in Direct Theorem by $\xi [1 - (\xi + \tau)] := \mu$. We compare it with two well known upper bounds of capacity of $n\xi$-constant dimensional $n\tau$-error correction codes in projective space (without localized side information).

Asymptotic Singleton Bound for “non-localized” codes (Koetter-Kschischang, 2008)

$$\eta_S := (\xi - \tau)(1 - \xi)$$

and

Asymptotic Hamming Bound for “non-localized” codes (Koetter-Kschischang, 2008)

$$\eta_H := \xi - \xi^2 - \frac{\tau}{2} + \frac{\tau^2}{4}.$$
The Main Results

Then

$$\eta_S - \mu = -\tau(1 - 2\xi).$$

Thus $$\eta_S < \mu$$ if $$\xi < 1/2$$. This is no surprising because we expect the localized side information improves ability of error correction. (As same as localized error correction in Hamming space, the side information is helpful.)

$$\eta_H - \mu = \tau(\xi - \frac{1}{2} + \frac{\tau}{4}).$$

Thus $$\eta_H < \mu$$ if $$\xi < \frac{1}{2} - \frac{\tau}{4}$$. The capacity of binary localized error codes is equal to the Hamming Bound and capacity of non-binary localized error correction code is upper bounded by Hamming bound. Unexpected and surprising, it is different from the classical case!
The Outline of the Direct Proof

The Main Idea in the Proof by BGP

- For each message \( i \in M \) create \( n \) codewords \( x^n(i, 1), x^n(i, 2), \ldots, x^n(i, n) \), of length \( n \). Thus the codebook contains \( n|M| \) codewords.

- Use the minimum Hamming distance decoder (MHD-decoder) to decode.

- To show a codeword \( x^n(i, j) \) is uniquely decoded to \( i \) by MHD-decoder when it is sent via a channel governed by the configuration \( J \), if for no \( i' \neq i, j' \), the Hamming sphere centered at \( v^n_J + x^n(i', j') \) with radius \( t \) contains \( x^n(i, j) \), where \( v^n_J \) is the binary sequence whose \( k \)th component is 1 iff \( k \in J \). In this case they said the codeword is “good” for \( i \) and \( J \).
The Main Idea in the Proof by BGP

• To prove existence of a codebook such that for each pair of $(i, J)$, the sender can always find a good codeword $x^n(i, j)$, by greedy algorithm. Thus he sends the good codeword if he want to send $i$ and the channel is governed by $J$.

• Notice in this case the “bad sets” are Hamming spheres of radius $t$, and their sizes are fixed if $t$ is fixed (i.e., independent of the relative positions of the codewords and the configurations).
The Outline of the Direct Proof

- Choosing size of message:

\[ \xi[1 - (\xi + \tau)] - \epsilon < \frac{1}{n^2} \log_q |M| < \xi[1 - (\xi + \tau)] - \frac{1}{2} \epsilon, \]

where \( q \) is the order of the field.

- **Random Codebook**: For each message \( i \), \( n \) codewords \( X(i, j), j = 1, 2, \ldots n \) are randomly and independently generated.

- **Minimum Subspace Distance Decoder** (MSD-decoder).
The Outline of the Direct Proof

• To prove that a codeword $X(i, j)$ is uniquely decoded by MSD-decoder to message $i$ for a given configuration $Z$ if for no $i' \neq i, j' \in \{1, 2, \ldots, n\}$, the set of linear subspace

$$\Xi(Z, X(i', j')) := \{X : \dim X = x, \dim(X + Z) \cap X(i', j') \geq \dim(X + Z) - z\}.$$ 

contains it. We say “$X(i, j)$ is good for the message $i$ and configuration $Z$,” in this case.

• One can use the codebook to define a localized error correction code if there exists a codebook such that for all $i, Z$, one may find a good codeword, because the $i$ can be encoded to the good codeword when the configuration $Z$ governs the channel.

• We say a codebook is good if for all $i \in M$ and $Z \in G(n, n\tau)$, one can find a good codeword $X(i, j)$ of message $i$. 

The Outline of the Direct Proof

- Thus our problem is reduced to show that with a positive probability one may successfully generate a good codebook.
- To this end we first fix $i \in M, Z \in \mathcal{G}(n, n\tau)$ and a $j \in \{1, 2, \ldots, n\}$, and estimate the probability of that the random codeword $X(i, j)$ to be good for $i$ and $Z$.
- To bound the probability, we must estimate the probability for the randomly generated codeword $X(i, j)$ falls into a “bad set” $\Xi(Z, X(i', j'))$ of linear subspaces for a $i' \neq i$. Consequently we have to estimate the cardinality of $\Xi(X', Z)$, for $X' \in \mathcal{G}(n, n\xi)$ and $Z \in \mathcal{G}(n, n\tau)$.
- Due to the irregularity of the subspace lattice, the estimation is quite complicate. It turn out that the cardinalities depends on the relative position of $X'$ and $Z$, or more precisely $\dim X' \cap Z$. 
The Outline of the Direct Proof

• Next for the fixed $Z \in \mathcal{G}(n, n\tau)$ we partition $\mathcal{G}(n, n\xi)$, into $n\tau + 1$ classes, according to $\dim X' \cap Z$, and estimate the number of randomly generated codewords $X(i', j')$ falling into each class with a “high probability” ($1 - \exp\{-2^{n\delta}\}$, for $\delta > 0$). This was done by combinatorially counting and Chernoff bound.

• Based the estimations, we proved, that the probability of, that the randomly chosen codeword $X(i, j)$ is no good for a fixed pair $i, j, Z$, is upper bounded by $q^{-n^2\alpha}$ for a “small” but positive $\alpha$ under the assumption to $|M|$.

• Recalling for each message $i$, we randomly and independently generated $n$ codewords, then by the independence of the random codewords, probability for none of $X(i, 1), X(i, 2) \ldots, X(i, n)$ to be good for fixed $i, Z$ is $(q^{-n^2\alpha})^n = q^{-n^3\alpha}$.
The Outline of the Direct Proof

- By the union bound the unsuccessful probability is upper bounded by $|M||\mathcal{G}(n, n\tau)|q^{-n^3\alpha} < q^{-\frac{n^3}{2}\alpha}$ because both $|M|$ and $|\mathcal{G}(n, n\tau)|$ are upper bounded by $q^{n^2A}$ for a sufficiently large (but fixed) $A$.

- That is, with a high probability a random codebook is successful. Done.
Proof of the Converse Coding Theorem for CDLECCPS (the proof for LECCPS is done by slightly adjustment)

Suppose we are given a \((n, m) (x, z)\)-CDLECCPS \((\phi, \psi)\). Then we have to show

\[
m \leq \sum_{d=\max(x,z)}^{x+z} \left[ \begin{array}{cc}
    n \\
    d \\
    \end{array} \right] \left[ \begin{array}{c}
    d \\
    z \\
    \end{array} \right] \left[ \begin{array}{c} 
    n \\
    z \\
    \end{array} \right],
\]
Proof of the Converse

At first, we fix a message $i$. Denote by

$$A(i, d) := \{ Y = \phi(i, Z) + Z : \dim Y = d, Z \in G(n, z) \},$$

and $B(i, Y) := \{ Z : \phi(i, Z) + Z = Y \}$. Then,

$$|B(i, Y)| \leq \begin{bmatrix} d \\ z \end{bmatrix}$$

if $Y \in A(i, d)$ because $Z$ is a $z$-dim subspace of $d$-dim subspace $Y$.

By counting the number of configurations in different ways we have

$$\begin{bmatrix} n \\ z \end{bmatrix} = |G(n, z)| = \sum_{d=\max(x,z)}^{x+z} \sum_{Y \in A(i, d)} |B(i, Y)|$$

$$\leq \sum_{d=\max(x,z)}^{x+z} |A(i, d)| \begin{bmatrix} d \\ z \end{bmatrix}.$$
Proof of the Converse

Because for a $z$-localized error code, all $i \neq i'$ and $Z, Z' \in G(n, z)$, $\phi(i, Z) + Z \neq \phi(i', Z') + Z'$ i.e., $A(i, d) \cap A(i', d) = \emptyset$, and thus

$$\sum_{i \in M} |A(i, d)| \leq \left[ \begin{array}{c} n \\ d \end{array} \right].$$

By above two formulas

$$|M| \left[ \begin{array}{c} n \\ z \end{array} \right] \leq \sum_{d=\max(x, z)}^{x+z} \sum_{i \in M} |A(i, d)| \left[ \begin{array}{c} d \\ z \end{array} \right] \leq \sum_{d=\max(x, z)}^{x+z} \left[ \begin{array}{c} n \\ d \end{array} \right] \left[ \begin{array}{c} d \\ z \end{array} \right].$$

Thus converse follows, by dividing both sides of the inequality by $\left[ \begin{array}{c} n \\ z \end{array} \right]$. 
In this work, we extend localized error correction codes by BGP from Hamming space to projective space. That is, we introduce CDLECCPS and LECCPS.

For $(n, m) (x, z)$-CDLECCP we have a lower bound and a upper bound, which are asymptotically tight when $z < x \leq \frac{n-z}{2}$.

For $(n, m) z$-LECCPS we determine the capacity for $z < \frac{n}{3}$. In the rest case we only have an upper and a lower bounds.

It similar to localized error correction in Hamming space that the localized side information is helpful.

It is different from localized error correction in Hamming space, Hamming bound is no upper bound for localized error correction in projective space.

To completely solve the problem, we suggest to use alternative decoder and/or improve the upper bound.
Thank You!
Previous Works and Background

The Model

The Main Results

The Outline of the Direct Proof

Proof of the Converse

The Conclusion