Minimum Distance Bounds for Expander Codes

Vitaly Skachek
Claude Shannon Institute
University College Dublin

Open Problems Session
Information Theory and Applications Workshop
UCSD
January 28, 2008
Basic Definitions
**Base Definitions**

**Definition**

*Code $C$* is a set of words of length $n$ over an alphabet $\Sigma$. 
Definition

*Code* $C$ is a set of words of length $n$ over an alphabet $\Sigma$.

Definition

The *Hamming distance* between $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ in $\Sigma^n$, $d(\mathbf{x}, \mathbf{y})$, is the number of pairs of symbols $(x_i, y_i)$, $1 \leq i \leq n$, such that $x_i \neq y_i$. 
Basic Definitions

**Definition**

*Code $C$* is a set of words of length $n$ over an alphabet $\Sigma$.

**Definition**

- The *Hamming distance* between $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ in $\Sigma^n$, $d(\mathbf{x}, \mathbf{y})$, is the number of pairs of symbols $(x_i, y_i)$, $1 \leq i \leq n$, such that $x_i \neq y_i$.
- The *minimum distance* of a code $C$ is

$$d = \min_{\mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}} d(\mathbf{x}, \mathbf{y}).$$
Definition

*Code* $C$ is a set of words of length $n$ over an alphabet $\Sigma$.

Definition

- The *Hamming distance* between $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\Sigma^n$, $d(x, y)$, is the number of pairs of symbols $(x_i, y_i)$, $1 \leq i \leq n$, such that $x_i \neq y_i$.
- The *minimum distance* of a code $C$ is
  \[ d = \min_{x, y \in C, x \neq y} d(x, y). \]
- The *relative minimum distance* of $C$ is defined as $\delta = d/n$. 

Vitaly Skachek  
Minimum Distance Bounds
A code $\mathcal{C}$ over field $\mathbb{F} = \text{GF}(q)$ is said to be a linear $[n, k, d]$ code if there exists a matrix $\mathcal{H}$ with $n$ columns and rank $n - k$ such that

$$\mathcal{H}x^t = \bar{0} \iff x \in \mathcal{C}.$$

The matrix $\mathcal{H}$ is a parity-check matrix.

The value $k$ is the dimension of the code $\mathcal{C}$.

The ratio $r = k/n$ is the rate of the code $\mathcal{C}$. 
Definition

- A code $\mathcal{C}$ over field $\mathbb{F} = \text{GF}(q)$ is said to be a linear $[n, k, d]$ code if there exists a matrix $\mathcal{H}$ with $n$ columns and rank $n - k$ such that
  $$\mathcal{H}x^t = \bar{0} \iff x \in \mathcal{C}.$$ 

- The matrix $\mathcal{H}$ is a parity-check matrix.
- The value $k$ is the dimension of the code $\mathcal{C}$.
- The ratio $r = k/n$ is the rate of the code $\mathcal{C}$.

Definition

- Let $\mathcal{C}$ be a code of minimum distance $d$ over $\Sigma$. 

Vitaly Skachek  Minimum Distance Bounds
A code $C$ over field $F = \text{GF}(q)$ is said to be a linear $[n, k, d]$ code if there exists a matrix $H$ with $n$ columns and rank $n - k$ such that

$$Hx^t = \bar{0} \iff x \in C.$$ 

The matrix $H$ is a parity-check matrix.

The value $k$ is the dimension of the code $C$.

The ratio $r = k/n$ is the rate of the code $C$.

Let $C$ be a code of minimum distance $d$ over $\Sigma$.

The unique decoding problem:
Linear Code

**Definition**

- A code \( C \) over field \( \mathbb{F} = \text{GF}(q) \) is said to be a *linear* \([n, k, d]\) code if there exists a matrix \( \mathcal{H} \) with \( n \) columns and rank \( n - k \) such that

\[
\mathcal{H} x^t = \bar{0} \iff x \in C.
\]

- The matrix \( \mathcal{H} \) is a *parity-check matrix*.
- The value \( k \) is the *dimension* of the code \( C \).
- The ratio \( r = k/n \) is the *rate* of the code \( C \).

**Definition**

- Let \( C \) be a code of minimum distance \( d \) over \( \Sigma \).
- The *unique decoding problem*:
  - **Input**: \( y \in \Sigma^n \).
Definition

A code $C$ over field $\mathbb{F} = \text{GF}(q)$ is said to be a *linear* $[n, k, d]$ *code* if there exists a matrix $H$ with $n$ columns and rank $n - k$ such that

$$Hx^t = \bar{0} \Leftrightarrow x \in C.$$ 

The matrix $H$ is a *parity-check matrix*.

The value $k$ is the *dimension* of the code $C$.

The ratio $r = k/n$ is the *rate* of the code $C$.

Definition

Let $C$ be a code of minimum distance $d$ over $\Sigma$.

The *unique decoding problem*:

**Input:** $y \in \Sigma^n$.

**Find:** $c \in C$, such that $d(c, y) < d/2$. 

Vitaly Skachek Minimum Distance Bounds
Let $H_q : [0, 1] \to [0, 1]$ be the $q$-ary entropy function:

$$H_q(x) = x \log_q (q - 1) - x \log_q x - (1 - x) \log_q (1 - x).$$
Let $H_q : [0, 1] \rightarrow [0, 1]$ be the $q$-ary entropy function:

$$H_q(x) = x \log_q (q - 1) - x \log_q x - (1 - x) \log_q (1 - x).$$

**Theorem**

Let $F = GF(q)$, and let $\delta \in (0, 1 - 1/q]$ and $R \in (0, 1)$, such that

$$R \leq 1 - H_q(\delta).$$

Then, for large enough values of $n$, there exists a linear $[n, Rn, \geq \delta n]$ code over $F$. 

Vitaly Skachek

Minimum Distance Bounds
Let $H_q : [0, 1] \rightarrow [0, 1]$ be the $q$-ary entropy function:

$$H_q(x) = x \log_q(q - 1) - x \log_q x - (1 - x) \log_q(1 - x).$$

**Theorem**

Let $\mathbb{F} = \text{GF}(q)$, and let $\delta \in (0, 1 - 1/q]$ and $R \in (0, 1)$, such that

$$R \leq 1 - H_q(\delta).$$

Then, for large enough values of $n$, there exists a linear $[n, Rn, \geq \delta n]$ code over $\mathbb{F}$.

- The above expression is called the *Gilbert-Varshamov bound*. 
Let $H_q : [0, 1] \rightarrow [0, 1]$ be the $q$-ary entropy function:

$$H_q(x) = x \log_q(q - 1) - x \log_q x - (1 - x) \log_q(1 - x).$$

**Theorem**

Let $F = GF(q)$, and let $\delta \in (0, 1 - 1/q]$ and $\mathcal{R} \in (0, 1)$, such that

$$\mathcal{R} \leq 1 - H_q(\delta).$$

Then, for large enough values of $n$, there exists a linear $[n, \mathcal{R}n, \geq \delta n]$ code over $F$.

- The above expression is called the *Gilbert-Varshamov bound*.
- Denote $\delta_{GV}(\mathcal{R}) = H_2^{-1}(1 - \mathcal{R})$. 
Ingredients:

- A linear $[\Delta, k=r\Delta, \theta\Delta]$ code $C$ over $\mathbb{F} = \text{GF}(q)$ (inner code).

[Forney ’66]
Concatenated Codes

[Forney '66] Ingredients:

- A linear $[\Delta, k=r\Delta, \theta\Delta]$ code $C$ over $\mathbb{F} = \text{GF}(q)$ (inner code).
- A linear $[N, R\Phi N, \delta\Phi N]$ code $C_\Phi$ over $\Phi = \mathbb{F}^k$ (outer code).
Concatenated Codes

[Forney ’66] Ingredients:

- A linear \([\Delta, k=r\Delta, \theta\Delta]\) code \(C\) over \(\mathbb{F} = \text{GF}(q)\) (inner code).
- A linear \([N, R_{\Phi}N, \delta_{\Phi}N]\) code \(C_{\Phi}\) over \(\Phi = \mathbb{F}^k\) (outer code).
- A linear one-to-one mapping \(E : \Phi \rightarrow C\).
Concatenated Codes

[Forney '66] Ingredients:

- A linear $[\Delta, k=r\Delta, \theta\Delta]$ code $C$ over $\mathbb{F} = GF(q)$ (*inner code*).
- A linear $[N, R_{\Phi}N, \delta_{\Phi}N]$ code $C_{\Phi}$ over $\Phi = \mathbb{F}^k$ (*outer code*).
- A linear one-to-one mapping $E : \Phi \rightarrow C$.

Concatenated code $C$ of length $N = \Delta n$ over $\mathbb{F}$ is defined as

$$C = \left\{ (c_1|c_2| \cdots |c_n) \in \mathbb{F}^{\Delta n} : c_i = E(a_i) , \right.$$ for $i \in 1, 2, \cdots, n$, and $(a_1a_2 \cdots a_n) \in C_{\Phi} \right\}.$$
[Forney ’66] Ingredients:

- A linear $[\Delta, k=r\Delta, \theta\Delta]$ code $C$ over $\mathbb{F} = GF(q)$ (inner code).
- A linear $[N, R_\Phi N, \delta_\Phi N]$ code $C_\Phi$ over $\Phi = \mathbb{F}^k$ (outer code).
- A linear one-to-one mapping $E : \Phi \to C$.

Concatenated code $C$ of length $N = \Delta n$ over $\mathbb{F}$ is defined as

$$C = \left\{ (c_1|c_2|\cdots|c_n) \in \mathbb{F}^{\Delta n} : c_i = E(a_i), \right. $$

where $i \in \{1, 2, \ldots, n\}$, and $(a_1a_2\cdots a_n) \in C_\Phi$.

- The rate of $C$: $R = rR_\Phi$. 

Vitaly Skachek
Minimum Distance Bounds
Concatenated Codes

[Forney '66] Ingredients:
- A linear $[\Delta, k=r\Delta, \theta\Delta]$ code $C$ over $\mathbb{F} = \text{GF}(q)$ (inner code).
- A linear $[N, R_\Phi N, \delta_\Phi N]$ code $C_\Phi$ over $\Phi = \mathbb{F}^k$ (outer code).
- A linear one-to-one mapping $\mathcal{E} : \Phi \rightarrow C$.

Concatenated code $C$ of length $N = \Delta n$ over $\mathbb{F}$ is defined as

$$C = \left\{ (c_1|c_2|\cdots|c_n) \in \mathbb{F}^{\Delta n} : c_i = \mathcal{E}(a_i), \quad\text{for } i \in 1, 2, \cdots, n, \text{ and } (a_1a_2\cdots a_n) \in C_\Phi \right\}.$$ 

- The rate of $C$: $R = rR_\Phi$.
- The relative minimum distance of $C$: $\delta \geq \theta \delta_\Phi$.  

Vitaly Skachek   Minimum Distance Bounds
Generalized minimum distance (GMD) decoder corrects any fraction of errors up to $\frac{1}{2}\delta$. 
Generalized minimum distance (GMD) decoder corrects any fraction of errors up to $\frac{1}{2}\delta$.

Justesen ’72 For a wide range of rates, concatenated codes attain the Zyablov bound:

$$\delta \geq \max_{\frac{R}{q} \leq r \leq 1} \left(1 - \frac{R}{r}\right) H^{-1}_q(1 - r).$$
Concatenated Codes (Cont.)

- **Generalized minimum distance** (GMD) decoder corrects any fraction of errors up to \( \frac{1}{2} \delta \).

- **[Justesen ’72]** For a wide range of rates, concatenated codes attain the **Zyablov bound**:

\[
\delta \geq \max_{\mathcal{R} \leq r \leq 1} \left( 1 - \frac{\mathcal{R}}{r} \right) \mathcal{H}^{-1}_q(1 - r).
\]

- **[Blokh-Zyablov ’82]** Multilevel concatenations of codes (almost) attain the **Blokh-Zyablov bound**:

\[
\mathcal{R} = 1 - \mathcal{H}_2(\delta) - \delta \int_0^{1 - \mathcal{H}_2(\delta)} \frac{dx}{\mathcal{H}_2^{-1}(1 - x)}.
\]
Consider a $\Delta$-regular graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. 
Consider a $\Delta$-regular graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$.

The largest eigenvalue of the adjacency matrix $A_{\mathcal{G}}$ of $\mathcal{G}$ equals $\Delta$. 

Graphs and Eigenvalues

- Consider a $\Delta$-regular graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$.
- The largest eigenvalue of the adjacency matrix $A_{\mathcal{G}}$ of $\mathcal{G}$ equals $\Delta$.
- Let $\lambda^*_\mathcal{G}$ be the second largest absolute value of eigenvalues of $A_{\mathcal{G}}$. 
Consider a $\Delta$-regular graph $G = (V, E)$.

The largest eigenvalue of the adjacency matrix $A_G$ of $G$ equals $\Delta$.

Let $\lambda^*_G$ be the second largest absolute value of eigenvalues of $A_G$.

Lower ratios of $\lambda^*_G/\Delta$ imply greater values of expansion [Alon ’86].
Consider a $\Delta$-regular graph $G = (V, E)$. The largest eigenvalue of the adjacency matrix $A_G$ of $G$ equals $\Delta$. Let $\lambda_G^*$ be the second largest absolute value of eigenvalues of $A_G$. Lower ratios of $\lambda_G^*/\Delta$ imply greater values of expansion \[\text{[Alon '86]}\].

Expander graphs with

$$\lambda_G^* \leq 2\sqrt{\Delta} - 1$$

are called a Ramanujan graphs. Constructions are due to \[\text{[Lubotsky Philips Sarnak '88]}, \text{[Margulis '88]}\].
Consider a $\Delta$-regular graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$.

The largest eigenvalue of the adjacency matrix $A_{\mathcal{G}}$ of $\mathcal{G}$ equals $\Delta$.

Let $\lambda^*_\mathcal{G}$ be the second largest absolute value of eigenvalues of $A_{\mathcal{G}}$.

Lower ratios of $\lambda^*_\mathcal{G}/\Delta$ imply greater values of expansion [Alon ’86].

Expander graphs with

$$\lambda^*_\mathcal{G} \leq 2\sqrt{\Delta} - 1$$

are called a Ramanujan graphs. Constructions are due to [Lubotsky Philips Sarnak ’88], [Margulis ’88].

Let $\lambda_{\mathcal{G}}$ be the second largest eigenvalues of $A_{\mathcal{G}}$ and $\gamma_{\mathcal{G}} = \lambda_{\mathcal{G}}/\Delta$. 
G is bipartite: $\mathcal{V} = A \cup B$, 
$A \cap B = \emptyset$, $|A| = |B| = n$.

Ordering on the vertices and the edges.

Denote by $(z)_{\mathcal{E}(u)}$ the sub-block of $z$ that is indexed by $\mathcal{E}(u)$.

Let $\mathcal{C}_A$ and $\mathcal{C}_B$ be two linear codes of length $\Delta$ over $\mathbb{F}$.

Denote $N = |\mathcal{E}| = \Delta n$. 
\( G \) is bipartite: \( V = A \cup B, \ A \cap B = \emptyset, \ |A| = |B| = n. \)

Ordering on the vertices and the edges.

Denote by \((z)_{\mathcal{E}(u)}\) the sub-block of \(z\) that is indexed by \(\mathcal{E}(u)\).

Let \(C_A\) and \(C_B\) be two linear codes of length \(\Delta\) over \(\mathbb{F}\).

Denote \(N = |\mathcal{E}| = \Delta n\).

The code \(C = (G, C_A : C_B)\):

\[
C = \left\{ c \in \mathbb{F}^N : (c)_{\mathcal{E}(u)} \in C_A \text{ for } v \in A \right. \\
\left. \text{ and } (c)_{\mathcal{E}(v)} \in C_B \text{ for } u \in B \right\}.
\]
\( G \) is bipartite: \( V = A \cup B \), \( A \cap B = \emptyset \), \( |A| = |B| = n \).

- Ordering on the vertices and the edges.
- Denote by \((z)_{E(u)}\) the sub-block of \( z \) that is indexed by \( E(u) \).
- Let \( C_A \) and \( C_B \) be two linear codes of length \( \Delta \) over \( \mathbb{F} \).
- Denote \( N = |E| = \Delta n \).

The code \( \mathcal{C} = (G, C_A : C_B) \):

\[
\mathcal{C} = \left\{ c \in \mathbb{F}^N : (c)_{E(u)} \in C_A \text{ for } v \in A \right. \\
\left. \quad \text{and } (c)_{E(v)} \in C_B \text{ for } u \in B \right\} .
\]
‘Dangling edges’ are introduced [Barg Zémor ’03].
‘Dangling edges’ are introduced [Barg Zémor ’03].

Mimics behavior of concatenated codes.
‘Dangling edges’ are introduced [Barg Zémor ’03].

Mimics behavior of concatenated codes.

Can be viewed as a concatenation of two codes [Roth Skachek ’04].
‘Dangling edges’ are introduced [Barg Zémor ’03].

Mimics behavior of concatenated codes.

Can be viewed as a concatenation of two codes [Roth Skachek ’04].

Another construction with similar properties [Guruswami Indyk ’02].
Analysis in [Barg Zémor ’04]

Analysis of the codes in [Barg Zémor ’02] and [Barg Zémor ’03].
Analysis in [Barg Zémor ’04]

Analysis of the codes in [Barg Zémor ’02] and [Barg Zémor ’03].

Lower bounds on the relative minimum distance

(i) \[
\delta(\mathcal{R}) \geq \frac{1}{4}(1 - \mathcal{R})^2 \cdot \min_{\delta_{GV}((1+\mathcal{R})/2)<B<\frac{1}{2}} \frac{g(B)}{H_2(B)},
\]

where the function \( g(B) \) is defined in the next slides.

(ii) \[
\delta(\mathcal{R}) \geq \max_{\mathcal{R} \leq r \leq 1} \left\{ \min_{\delta_{GV}(r)<B<\frac{1}{2}} \left( \delta_0(B, r) \cdot \frac{1 - \mathcal{R}/r}{H_2(B)} \right) \right\},
\]

where the function \( \delta_0(B, r) \) is defined in the next slides.
Definition of the Function $g(\mathcal{B})$

These two families of codes surpass the Zyablov bound.
Definition of the Function $g(B)$

These two families of codes surpass the Zyablov bound.

Let $\delta_{GV}(R) = H_2^{-1}(1 - R)$, and let $B_1$ be the largest root of the equation

$$H_2(B) = H_2(B) \left( B - H_2(B) \cdot \frac{\delta_{GV}(R)}{1 - R} \right) = -(B - \delta_{GV}(R)) \cdot \log_2(1 - B).$$

Moreover, let

$$a_1 = \frac{B_1}{H_2(B_1)} - \frac{\delta_{GV}(R)}{H_2(\delta_{GV}(R))},$$

and

$$b_1 = \frac{\delta_{GV}(R)}{H_2(\delta_{GV}(R))} \cdot B_1 - \frac{B_1}{H_2(B_1)} \cdot \delta_{GV}(R).$$
The function $g(B)$ is defined as

$$
g(B) = \begin{cases} 
\frac{\delta_{GV}(R)}{1 - R} & \text{if } B \leq \delta_{GV}(R) \\
B & \text{if } \delta_{GV}(R) \leq B \text{ and } R \leq 0.284 \\
\frac{B}{H_2(B)} & \text{if } \delta_{GV}(R) \leq B \leq B_1 \text{ and } 0.284 < R \leq 1 \\
\frac{a_1 B + b_1}{B_1 - \delta_{GV}(R)} & \text{if } B_1 < B \leq 1 \text{ and } 0.284 < R \leq 1 
\end{cases} \, .
$$
Definition of the Function $\delta_0(B, r)$

The function $\delta_0(B, r)$ is defined to be $\omega**(B)$ for $\delta_{GV}(r) \leq B \leq B_1$, where

$$\omega**(B) = rB + (1 - r)H_2^{-1} \left( 1 - \frac{r}{1 - r}H_2(B) \right),$$

and $B_1$ is the only root of the equation

$$\delta_{GV}(r) = w^*(B),$$

where

$$w^*(B) = (1-r) \left( (2^{H_2(B)/B} + 1)^{-1} + \frac{B}{H_2(B)} \left( 1 - H_2 \left( (2^{H_2(B)/B} + 1)^{-1} \right) \right) \right).$$

For $B_1 \leq B \leq \frac{1}{2}$, the function $\delta_0(B, r)$ is defined to be a tangent to the function $\omega**(B)$ drawn from the point $\left( \frac{1}{2}, \omega^*(\frac{1}{2}) \right)$. 
Minimum Distance Bounds

Comparison of Bounds

- Zyablov bound
- Barg–Zemor bound 1
- Barg–Zemor bound 2
- Blokh–Zyablov bound
- Gilbert–Varshamov bound

Vitaly Skachek
$\mathcal{G} = (\mathcal{V} = A \cup B, \mathcal{E})$ be a bipartite $\Delta$-regular, as before
Let $\mathcal{G} = (\mathcal{V} = A \cup B, \mathcal{E})$ be a bipartite $\Delta$-regular, as before.

Let $B = B^1 \cup B^2$, $B^1 \cap B^2 = \emptyset$. Let $|B^2| = \eta n$, $|B^1| = (1 - \eta)n$, $\eta \in [0, 1]$. 

Vitaly Skachek  Minimum Distance Bounds
Let $G = (\mathcal{V} = A \cup B, \mathcal{E})$ be a bipartite $\Delta$-regular, as before.

Let $B = B^1 \cup B^2$, $B^1 \cap B^2 = \emptyset$. Let $|B^2| = \eta n$, $|B^1| = (1-\eta)n$, $\eta \in [0,1]$.

$C_A$, $C_1$ and $C_2$ are linear $[\Delta, r_A \Delta, \delta_A \Delta]$, $[\Delta, r_1 \Delta, \delta_1 \Delta]$ and $[\Delta, r_2 \Delta, \delta_2 \Delta]$ codes over $\mathbb{F}$, respectively.
Generalized Expander Codes

- $\mathcal{G} = (\mathcal{V} = A \cup B, \mathcal{E})$ be a bipartite $\Delta$-regular, as before
- $B = B^1 \cup B^2$, $B^1 \cap B^2 = \emptyset$. Let $|B^2| = \eta n$, $|B^1| = (1 - \eta)n$, $\eta \in [0, 1]$.
- $\mathcal{C}_A$, $\mathcal{C}_1$ and $\mathcal{C}_2$ are linear $[\Delta, r_A \Delta, \delta_A \Delta]$, $[\Delta, r_1 \Delta, \delta_1 \Delta]$ and $[\Delta, r_2 \Delta, \delta_2 \Delta]$ codes over $\mathbb{F}$, respectively.

The code code $\mathcal{C} = (\mathcal{G}, \mathcal{C}_A, \mathcal{C}_1, \mathcal{C}_2)$:

$$\mathcal{C} = \left\{ \mathbf{c} \in \mathbb{F}^N : (\mathbf{c})_{\mathcal{E}(u)} \in \mathcal{C}_A \text{ for } u \in A, \right.$$ 

$$(\mathbf{c})_{\mathcal{E}(u)} \in \mathcal{C}_1 \text{ for } u \in B^1$$ 

and $$(\mathbf{c})_{\mathcal{E}(u)} \in \mathcal{C}_2 \text{ for } u \in B^2$$ $$\right\}$$
\[ \mathcal{G} = (\mathcal{V} = A \cup B, \mathcal{E}) \] be a bipartite \( \Delta \)-regular, as before

\[ B = B^1 \cup B^2, \quad B^1 \cap B^2 = \emptyset. \]
Let \( |B^2| = \eta n, \quad |B^1| = (1 - \eta)n, \quad \eta \in [0, 1]. \)

\( C_A, \ C_1 \) and \( C_2 \) are linear
\([\Delta, r_A \Delta, \delta_A \Delta], \ [\Delta, r_1 \Delta, \delta_1 \Delta] \) and
\([\Delta, r_2 \Delta, \delta_2 \Delta] \) codes over \( \mathbb{F} \), respectively.

The code code \( \mathbb{C} = (\mathcal{G}, C_A, C_1, C_2) \):

\[ \mathbb{C} = \left\{ \mathbf{c} \in \mathbb{F}^N \ :ight. \begin{array}{l}
(c)_{\mathcal{E}(u)} \in C_A \text{ for } u \in A, \\
(c)_{\mathcal{E}(u)} \in C_1 \text{ for } u \in B^1 \\
\text{and } (c)_{\mathcal{E}(u)} \in C_2 \text{ for } u \in B^2 \end{array} \left. \right\} \]
Properties of Generalized Expander Codes

- **The rate:** \( R \geq r_A + (1 - \eta)r_1 + \eta r_2 - 1. \)
Properties of Generalized Expander Codes

- **The rate:** \( R \geq r_A + (1 - \eta)r_1 + \eta r_2 - 1. \)

- Assume
  \[
  \eta < \frac{\delta_A - \gamma_g \sqrt{\delta_A/\delta_2}}{1 - \gamma_g} - \gamma_g^{2/3}.
  \]

  Then, the relative minimum distance:

  \[
  \delta > \delta_A (\delta_1 - \frac{1}{2} \gamma_g^{2/3}).
  \]

  \Rightarrow The code \( C \) attains the **Zyablov bound**.
Properties of Generalized Expander Codes

- **The rate:** $\mathcal{R} \geq r_A + (1 - \eta)r_1 + \eta r_2 - 1$.
- Assume
  \[
  \eta < \frac{\delta_A - \gamma G \sqrt{\delta_A/\delta_2}}{1 - \gamma G} - \gamma G^{2/3}.
  \]

Then, the relative minimum distance:

\[
\delta > \delta_A(\delta_1 - \frac{1}{2}\gamma G^{2/3}).
\]

$\Rightarrow$ The code $\mathbb{C}$ attains the **Zyablov bound**.

- **A linear-time decoding algorithm:** if $\delta_1 > 2\gamma G^{2/3}$ and $\eta$ as above, the decoder corrects any error pattern of size $J_{\mathbb{C}}$,

  \[
  J_{\mathbb{C}} \triangleq \frac{\frac{1}{2} \delta_1 - \gamma G^{2/3} \left(1 + \sqrt{2 \left(\delta_1 - 2\gamma G^{2/3}\right)}\right)}{1 - \gamma G} \cdot \delta_A \Delta n.
  \]

The number of correctable errors is (almost) half of the Zyablov bound.
Theorem

Let $|\mathbb{F}|$ be a power of 2. There exists a polynomial-time constructible family of binary linear codes $\mathbb{C}$ of length $N = n\Delta$, $n \to \infty$, and sufficiently large but constant $\Delta = \Delta(\varepsilon)$, whose relative minimum distance satisfies

$$\delta(R) \geq \max_{R \leq r_A \leq 1} \left\{ \min_{\delta_{GV}(r_A) \leq \beta \leq 1/2} \left( \delta_0(\beta, r_A) \frac{1 - R/r_A}{H_2(\beta)} \right) \right\} - \varepsilon.$$
Theorem

Let $|\mathbb{F}|$ be a power of 2. There exists a polynomial-time constructible family of binary linear codes $\mathbb{C}$ of length $N = n\Delta$, $n \to \infty$, and sufficiently large but constant $\Delta = \Delta(\varepsilon)$, whose relative minimum distance satisfies

$$\delta(\mathcal{R}) \geq \max_{\mathcal{R} \leq r_A \leq 1} \left\{ \min_{\delta_{GV}(r_A) \leq \beta \leq 1/2} \left( \delta_0(\beta, r_A) \frac{1 - \mathcal{R}/r_A}{H_2(\beta)} \right) \right\} - \varepsilon.$$

Consider a code $\mathbb{C}$ with parameter $\eta = 0$. Then, $|B^2| = 0$, and the code $\mathbb{C}$ coincides with the code in [Barg Zémor’02].
Theorem

Let $|\mathbb{F}|$ be a power of 2. There exists a polynomial-time constructible family of binary linear codes $C$ of length $N = n\Delta$, $n \to \infty$, and sufficiently large but constant $\Delta = \Delta(\varepsilon)$, whose relative minimum distance satisfies

$$\delta(\mathcal{R}) \geq \max_{\mathcal{R} \leq r_A \leq 1} \left\{ \min_{\delta_{GV}(r_A) \leq \beta \leq 1/2} \left( \delta_0(\beta, r_A) \frac{1 - \mathcal{R}/r_A}{H_2(\beta)} \right) \right\} - \varepsilon.$$

Consider a code $C$ with parameter $\eta = 0$. Then, $|B^2| = 0$, and the code $C$ coincides with the code in [Barg Zémor’02]. The minimum distance:

$$\delta(\mathcal{R}) \geq \frac{1}{4} (1 - \mathcal{R})^2 \cdot \min_{\delta_{GV}((1+\mathcal{R})/2) < B < \frac{1}{2}} \frac{g(B)}{H_2(B)}.$$
Minimum Distance Bounds

Comparison of Bounds

- Zyablov bound
- Barg–Zemor bound 1
- Barg–Zemor bound 2
- Blokh–Zyablov bound
- Gilbert–Varshamov bound

Vitaly Skachek
Further improvements on the minimum distance bounds.
Further improvements on the **minimum distance bounds**.

Bounds on the **error-correcting capabilities** of the decoders.
Further improvements on the minimum distance bounds.

 Bounds on the error-correcting capabilities of the decoders.

 Could other types of expander graphs yield better properties?
Open Problems

- Further improvements on the **minimum distance bounds**.
- Bounds on the **error-correcting capabilities** of the decoders.
- Could **other types of expander graphs** yield better properties?
- Do the **generalized expander codes** have any **advantage** over the known expander codes?