Expander Codes: Constructions and Bounds

Vitaly Skachek
Under the supervision of Prof. Ronny Roth

Computer Science Department,
Technion, Haifa 32000, Israel.

Turbo Codes

Presented by Berrou, Glavieux and Thitimajshima in 1993.

- Very efficient in practice.
- Perform at rates very close to Shannon capacity.
- Hard to analyze.

LDPC Codes

Low-density parity-check codes.

- [Gallager '62] Presented for the first time. Seemed to be unpractical then.

LDPC Codes

Low-density parity-check codes.

- [Gallager '62] Presented for the first time. Seemed to be unpractical then.
- [MacKay '97] Similarity between turbo codes and low-density parity-check codes.

LDPC Codes

Low-density parity-check codes.

- [Gallager '62] Presented for the first time. Seemed to be unpractical then.
- [MacKay '97] Similarity between turbo codes and low-density parity-check codes.
- [McEliece MacKay Cheng '98] Turbo decoding can be viewed as a belief-propagation algorithm.

LDPC Codes

Low-density parity-check codes.

- [Gallager '62] Presented for the first time. Seemed to be unpractical then.
- [MacKay '97] Similarity between turbo codes and low-density parity-check codes.
- [McEliece MacKay Cheng '98] Turbo decoding can be viewed as a belief-propagation algorithm.
- [Richardson Urbanke '01] Good *average* behavior over binary memoryless channels.

LDPC Codes

Low-density parity-check codes.

- [Gallager '62] Presented for the first time. Seemed to be unpractical then.
- [MacKay '97] Similarity between turbo codes and low-density parity-check codes.
- [McEliece MacKay Cheng '98] Turbo decoding can be viewed as a belief-propagation algorithm.
- [Richardson Urbanke '01] Good *average* behavior over binary memoryless channels.
- [Richardson Shokrollahi Urbanke '01] Codes, which are extremely close to the capacity, found by the exhaustive search.

Explicit Constructions

- [Sipser Spielman '96] Correct constant fraction of errors, linear time encoding and decoding.

Explicit Constructions

- [Sipser Spielman '96] Correct constant fraction of errors, linear time encoding and decoding.
- [Barg Zémor '01–'04] Capacity-achieving codes for BSC with linear-time decoding, exponentially small decoding error.

Explicit Constructions

- [Sipser Spielman '96] Correct constant fraction of errors, linear time encoding and decoding.
- [Barg Zémor '01–'04] Capacity-achieving codes for BSC with linear-time decoding, exponentially small decoding error.
- [Guruswami Indyk '02] Linear-time encodable and decodable codes that attain the Zyablov bound, used concatenation with nearly-MDS code. Based on construction in [Zémor '01] as a building block.

Basic Definitions

Basic Definitions

Definition

Code $\mathcal{C}$ is a set of words of length n over an alphabet Σ.

Basic Definitions

Definition

Code $\mathcal{C}$ is a set of words of length n over an alphabet Σ.

Definition

- *The Hamming distance* between $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_n)$ in Σ^n, $\mathsf{d}(\boldsymbol{x}, \boldsymbol{y})$, 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 $\mathcal{C}$ is a set of words of length n over an alphabet Σ.

Definition

- *The Hamming distance* between $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_n)$ in Σ^n, $\mathsf{d}(\boldsymbol{x}, \boldsymbol{y})$, 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 $\mathcal{C}$ is

$$d = \min_{\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}} \mathsf{d}(\boldsymbol{x}, \boldsymbol{y}).$$

Basic Definitions

Definition

Code $\mathcal{C}$ is a set of words of length n over an alphabet Σ.

Definition

- *The Hamming distance* between $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_n)$ in Σ^n, $\mathsf{d}(\boldsymbol{x}, \boldsymbol{y})$, 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 $\mathcal{C}$ is

$$d = \min_{\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}} \mathsf{d}(\boldsymbol{x}, \boldsymbol{y}).$$

- *The relative minimum distance* of $\mathcal{C}$ is defined as $\delta = d/n$.

Linear Code

Definition

- A code $\mathcal{C}$ over field Φ 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
$$H\boldsymbol{x}^t = \bar{\mathbf{0}} \Leftrightarrow \boldsymbol{x} \in \mathcal{C}.$$
- The matrix H is called a *parity-check matrix*.
- The value k is called the *dimension* of the code $\mathcal{C}$.
- The ratio $r = k/n$ is called the *rate* of the code $\mathcal{C}$.
- The words of $\mathcal{C}$ can be obtained as linear combinations of rows of a *generating* $k \times n$ *matrix* G.

Concatenated Codes

[Forney '66] Ingredients:

- A linear $[n, k{=}rn, \delta_{in}n]$ code $\mathcal{C}_{in}$ over $F = \mathrm{GF}(q)$ (inner code).

Concatenated Codes

[Forney '66] Ingredients:

- A linear $[n, k{=}rn, \delta_{in}n]$ code $\mathcal{C}_{in}$ over $F = \mathrm{GF}(q)$ (inner code).
- A linear $[N, RN, \delta_{out}N]$ code $\mathcal{C}_{out}$ over $\Phi = F^k$ (outer code).

Concatenated Codes

[Forney '66] Ingredients:

- A linear $[n, k{=}rn, \delta_{in}n]$ code $\mathcal{C}_{in}$ over $F = \mathrm{GF}(q)$ (inner code).
- A linear $[N, RN, \delta_{out}N]$ code $\mathcal{C}_{out}$ over $\Phi = F^k$ (outer code).
- A linear one-to-one mapping $\mathcal{E}_0 \ : \ \Phi \rightarrow \mathcal{C}_{in}$.

Concatenated Codes

[Forney '66] Ingredients:

- A linear $[n, k{=}rn, \delta_{in}n]$ code $\mathcal{C}_{in}$ over $F = \mathrm{GF}(q)$ (inner code).
- A linear $[N, RN, \delta_{out}N]$ code $\mathcal{C}_{out}$ over $\Phi = F^k$ (outer code).
- A linear one-to-one mapping $\mathcal{E}_0 \ : \ \Phi \to \mathcal{C}_{in}$.

Concatenated code $\mathbb{C}_{cont}$ of length $n \cdot N$ over F is defined as

$$\mathbb{C}_{cont} = \Big\{ (\boldsymbol{c}_1|\boldsymbol{c}_2|\cdots|\boldsymbol{c}_n) \in F^{n\cdot N} : \boldsymbol{c}_i = \mathcal{E}_0(\Xi_i) \ , \\ \text{for } i \in 1, 2, \cdots, n, \quad \text{and } (\Xi_1\Xi_2\cdots\Xi_n) \in \mathcal{C}_{out} \Big\} \ .$$

Concatenated Codes

[Forney '66] Ingredients:

- A linear $[n, k{=}rn, \delta_{in}n]$ code $\mathcal{C}_{in}$ over $F = \mathrm{GF}(q)$ (inner code).
- A linear $[N, RN, \delta_{out}N]$ code $\mathcal{C}_{out}$ over $\Phi = F^k$ (outer code).
- A linear one-to-one mapping $\mathcal{E}_0 \ : \ \Phi \to \mathcal{C}_{in}$.

Concatenated code $\mathbb{C}_{cont}$ of length $n \cdot N$ over F is defined as

$$\mathbb{C}_{cont} = \Big\{ (\boldsymbol{c}_1|\boldsymbol{c}_2|\cdots|\boldsymbol{c}_n) \in F^{n\cdot N} : \boldsymbol{c}_i = \mathcal{E}_0(\Xi_i) \ , \\ \text{for } i \in 1, 2, \cdots, n, \quad \text{and } (\Xi_1\Xi_2\cdots\Xi_n) \in \mathcal{C}_{out} \Big\} \ .$$

The rate $R_{cont} = r \cdot R$. The relative minimum distance $\delta \geq \delta_{in} \cdot \delta_{out}$.

Concatenated Codes (Cont.)

- Generalized minimum distance (GMD) decoder corrects any fraction of errors up to a half of the code minimum distance.

Concatenated Codes (Cont.)

- Generalized minimum distance (GMD) decoder corrects any fraction of errors up to a half of the code minimum distance.
- For any rate $\mathcal{R}$ less than channel capacity $\mathsf{C}_q(p)$, the decoding error probability of the concatenated code $\mathbb{C}_{cont}$ (under the GMD decoder) is upper-bounded by

$$\mathsf{Prob}_e(\mathbb{C}_{cont}) \leq \max_{\mathcal{R} \leq r \leq \mathsf{C}_q(p)} \mathsf{e}^{-NE(r)(1-\frac{\mathcal{R}}{r})},$$

Concatenated Codes (Cont.)

- Generalized minimum distance (GMD) decoder corrects any fraction of errors up to a half of the code minimum distance.
- For any rate $\mathcal{R}$ less than channel capacity $\mathsf{C}_q(p)$, the decoding error probability of the concatenated code $\mathbb{C}_{cont}$ (under the GMD decoder) is upper-bounded by

$$\mathsf{Prob}_e(\mathbb{C}_{cont}) \leq \max_{\mathcal{R} \leq r \leq \mathsf{C}_q(p)} \mathsf{e}^{-NE(r)(1-\frac{\mathcal{R}}{r})},$$

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

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

LDPC Code Definition

[Gallager '62]

- Matrix H: the number of non-zero entries in each column (row) of H is typically *bounded by a small constant*.

LDPC Code Definition

[Gallager '62]

- Matrix H: the number of non-zero entries in each column (row) of H is typically *bounded by a small constant.*

Alternative Description

Bipartite undirected graph $\mathcal{G} = (V, E)$.

- Vertex set $V = V_m \cup V_c$, $|V_m| = n$, $|V_c| = n - k$.
- Edge set E. There is an edge between the message vertex i and the check vertex j if and only if $(H)_{i,j} \neq 0$.

Low-Complexity Codes

[Tanner '81]

- A Δ-regular undirected graph $\mathcal{G} = (V, E)$.

Low-Complexity Codes

[Tanner '81]

- A Δ-regular undirected graph $\mathcal{G} = (V, E)$.
- Linear $[\Delta, k{=}r\Delta, d{=}\delta\Delta]$ code $\mathcal{C}$ over $\mathrm{GF}(q)$.

$\mathbb{C} = (\mathcal{G}, \mathcal{C})$ is the following linear $[N, K, D]$ code over $\mathrm{GF}(q)$:

$$\mathbb{C} = \left\{ \boldsymbol{c} \in (\mathrm{GF}(q))^N \ : \ (\boldsymbol{c})_{E(v)} \in \mathcal{C} \text{ for every } v \in V \right\} \ ,$$

$(\boldsymbol{c})_{E(v)}$ = the sub-word of $\boldsymbol{c}$ that is indexed by the set of edges incident with v.

Low-Complexity Codes

[Tanner '81]

- A Δ-regular undirected graph $\mathcal{G} = (V, E)$.
- Linear $[\Delta, k{=}r\Delta, d{=}\delta\Delta]$ code $\mathcal{C}$ over $\mathrm{GF}(q)$.

$\mathbb{C} = (\mathcal{G}, \mathcal{C})$ is the following linear $[N, K, D]$ code over $\mathrm{GF}(q)$:

$$\mathbb{C} = \left\{ \boldsymbol{c} \in (\mathrm{GF}(q))^N \,:\, (\boldsymbol{c})_{E(v)} \in \mathcal{C} \text{ for every } v \in V \right\} ,$$

$(\boldsymbol{c})_{E(v)}$ = the sub-word of $\boldsymbol{c}$ that is indexed by the set of edges incident with v.

- The code $\mathbb{C} = (\mathcal{G}, \mathcal{C})$ is a *low-complexity* code.

Low-Complexity Codes – Example

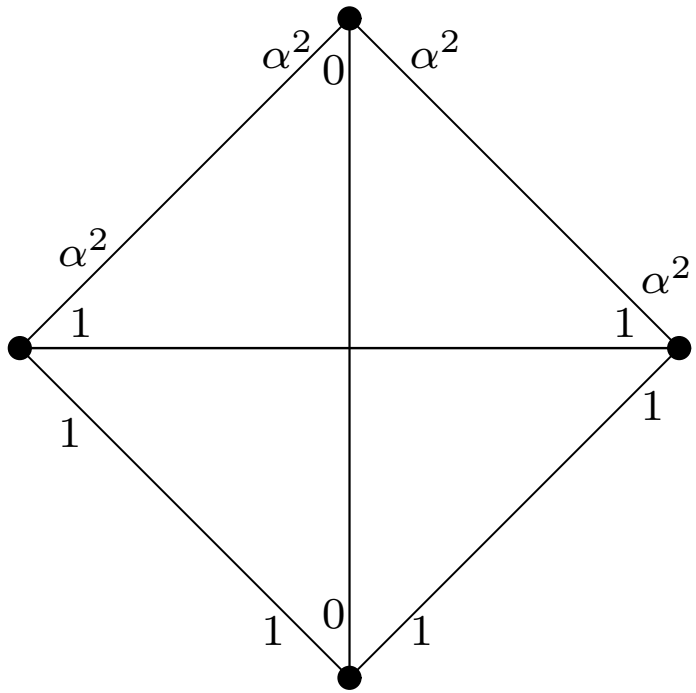
Take $\Delta = 3$, $k = 2$, $|V| = 4$.
Let G be a generating matrix of $\mathcal{C}$ over $F = \mathrm{GF}(2^2) = \{0, 1, \alpha, \alpha^2\}$:

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{pmatrix} .$$

Low-Complexity Codes – Example

Take $\Delta = 3$, $k = 2$, $|V| = 4$.
Let G be a generating matrix of $\mathcal{C}$ over $F = \mathrm{GF}(2^2) = \{0, 1, \alpha, \alpha^2\}$:

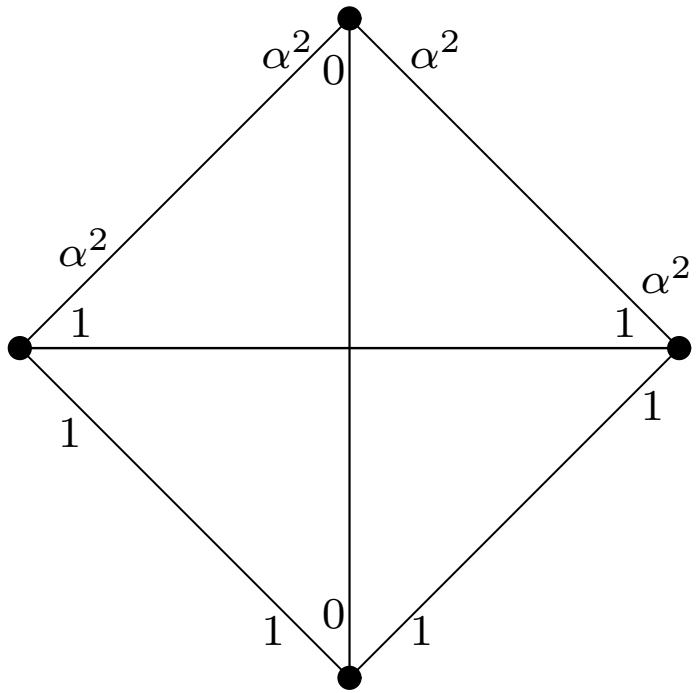
$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{pmatrix}.$$



Low-Complexity Codes – Example

Take $\Delta = 3$, $k = 2$, $|V| = 4$.
Let G be a generating matrix of $\mathcal{C}$ over $F = \mathrm{GF}(2^2) = \{0, 1, \alpha, \alpha^2\}$:

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{pmatrix}.$$



The resulting code $\mathbb{C}$ is of length $N = 6$. For instance,

$$(1\ 1\ \alpha^2\ 0\ \alpha^2\ 1) \in \mathbb{C}.$$

Expander Graph

- Consider a Δ-regular graph $\mathcal{G} = (V, E)$.

Expander Graph

- Consider a Δ-regular graph $\mathcal{G} = (V, E)$.
- A subset $S \subseteq V$ *expands by a factor of* ζ, $0 < \zeta \leq 1$, if

$$|\{v \in V : \exists \tilde{v} \in S \text{ such that } \{v, \tilde{v}\} \in E\}| \geq \zeta\Delta \cdot |S|.$$

Expander Graph

- Consider a Δ-regular graph $\mathcal{G} = (V, E)$.
- A subset $S \subseteq V$ *expands by a factor of* ζ, $0 < \zeta \leq 1$, if

$$|\{v \in V : \exists \tilde{v} \in S \text{ such that } \{v, \tilde{v}\} \in E\}| \geq \zeta\Delta \cdot |S|.$$

- The graph $\mathcal{G}$ is an (α, ζ)-*expander* if every subset of at most $\alpha|V|$ vertices expands by a factor of ζ.

Eigenvalues of Expander Graph

- Consider a graph $\mathcal{G}$ where each vertex has degree Δ. The largest eigenvalue of the adjacency matrix $A_{\mathcal{G}}$ of $\mathcal{G}$ is Δ.

Eigenvalues of Expander Graph

- Consider a graph $\mathcal{G}$ where each vertex has degree Δ. The largest eigenvalue of the adjacency matrix $A_{\mathcal{G}}$ of $\mathcal{G}$ is Δ.
- Let $\lambda_{\mathcal{G}}$ be the second largest eigenvalue of $A_{\mathcal{G}}$.

Eigenvalues of Expander Graph

- Consider a graph $\mathcal{G}$ where each vertex has degree Δ. The largest eigenvalue of the adjacency matrix $A_{\mathcal{G}}$ of $\mathcal{G}$ is Δ.
- Let $\lambda_{\mathcal{G}}$ be the second largest eigenvalue of $A_{\mathcal{G}}$.
- Lower ratios of $\gamma_{\mathcal{G}} = \frac{\lambda_{\mathcal{G}}}{\Delta}$ imply greater values ζ of expansion. [Alon '86]

Eigenvalues of Expander Graph

- Consider a graph $\mathcal{G}$ where each vertex has degree Δ. The largest eigenvalue of the adjacency matrix $A_{\mathcal{G}}$ of $\mathcal{G}$ is Δ.
- Let $\lambda_{\mathcal{G}}$ be the second largest eigenvalue of $A_{\mathcal{G}}$.
- Lower ratios of $\gamma_{\mathcal{G}} = \frac{\lambda_{\mathcal{G}}}{\Delta}$ imply greater values ζ of expansion. [Alon '86]
- Expander graph with

$$\lambda_{\mathcal{G}} \leq 2\sqrt{\Delta - 1}$$

is called a *Ramanujan graph*. Constructions are due to [Lubotsky Philips Sarnak '88], [Margulis '88].

Expander Codes

[Sipser Spielman '96], [Zémor '01].

- A Δ-regular *bipartite* undirected Ramanujan graph $\mathcal{G} = (V, E)$.

Expander Codes

[Sipser Spielman '96], [Zémor '01].

- A Δ-regular *bipartite* undirected Ramanujan graph $\mathcal{G} = (V, E)$.
  - Vertex set $V = A \cup B$ such that $A \cap B = \emptyset$ and $|A| = |B| = n$.

Expander Codes

[Sipser Spielman '96], [Zémor '01].

- A Δ-regular *bipartite* undirected Ramanujan graph $\mathcal{G} = (V, E)$.
  - Vertex set $V = A \cup B$ such that $A \cap B = \emptyset$ and $|A| = |B| = n$.
  - Edge set E of size $N = n\Delta$ such that every edge in E has one endpoint in A and one endpoint in B.

Expander Codes

[Sipser Spielman '96], [Zémor '01].

- A Δ-regular *bipartite* undirected Ramanujan graph $\mathcal{G} = (V, E)$.
  - Vertex set $V = A \cup B$ such that $A \cap B = \emptyset$ and $|A| = |B| = n$.
  - Edge set E of size $N = n\Delta$ such that every edge in E has one endpoint in A and one endpoint in B.
- A linear $[\Delta, k{=}r\Delta, d{=}\delta\Delta]$ code $\mathcal{C}$ over $F = \mathrm{GF}(q)$.

Expander Codes

[Sipser Spielman '96], [Zémor '01].

- A Δ-regular *bipartite* undirected Ramanujan graph $\mathcal{G} = (V, E)$.
  - Vertex set $V = A \cup B$ such that $A \cap B = \emptyset$ and $|A| = |B| = n$.
  - Edge set E of size $N = n\Delta$ such that every edge in E has one endpoint in A and one endpoint in B.
- A linear $[\Delta, k{=}r\Delta, d{=}\delta\Delta]$ code $\mathcal{C}$ over $F = \mathrm{GF}(q)$.
- Let $\mathbb{C} = (\mathcal{G}, \mathcal{C})$ be the low-complexity linear $[N, \mathcal{R}N, D]$ code.

Example

Take the graph $\mathcal{G}$ with $\Delta = 3$ and $n = 4$. ($\mathcal{G}$ as on the slide is both $(1/8, 1)$-expander and $(1/4, 2/3)$-expander.)

Let $k = 2$, and pick $F = \mathrm{GF}(2)$.

Take $\mathcal{C}$ parity code over F:

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

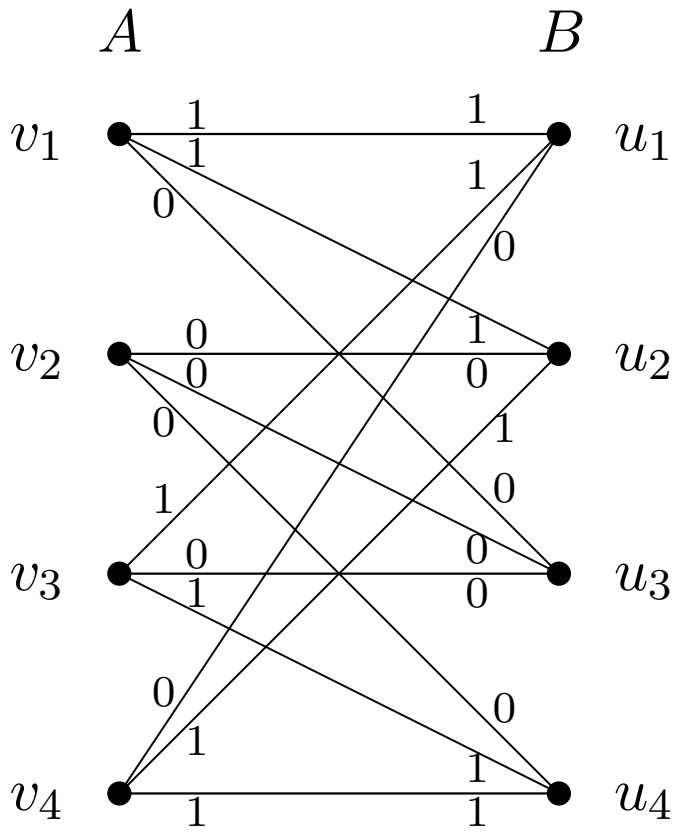
Example

Take the graph $\mathcal{G}$ with $\Delta = 3$ and $n = 4$. ($\mathcal{G}$ as on the slide is both $(1/8, 1)$-expander and $(1/4, 2/3)$-expander.)

Let $k = 2$, and pick $F = \mathrm{GF}(2)$.

Take $\mathcal{C}$ parity code over F:

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$



Example

Take the graph $\mathcal{G}$ with $\Delta = 3$ and $n = 4$. ($\mathcal{G}$ as on the slide is both $(1/8, 1)$-expander and $(1/4, 2/3)$-expander.)

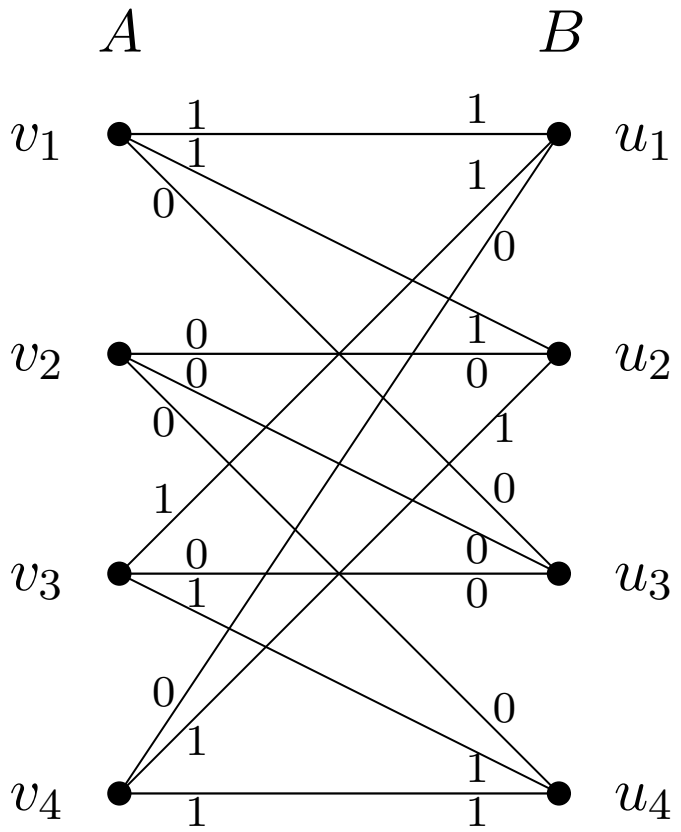
Let $k = 2$, and pick $F = \mathrm{GF}(2)$.

Take $\mathcal{C}$ parity code over F:

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Thus,

$$(\,1\,1\,0\;\;0\,0\,0\;\;1\,0\,1\;\;0\,1\,1\,) \in \mathbb{C}.$$



Parameters of Expander Codes

The Code Rate

Each sub-code vertex contributes $\Delta - k$ parity-check equations. Thus,

$$N(1-\mathcal{R}) \leq (\Delta - k) \cdot 2n,$$

$$\Rightarrow \quad \mathcal{R} \geq 1 - (\Delta - k)\frac{2n}{N} = 1 - 2\frac{\Delta - k}{\Delta} = 2r - 1.$$

Parameters of Expander Codes

The Code Rate

Each sub-code vertex contributes $\Delta - k$ parity-check equations. Thus,

$$N(1-\mathcal{R}) \leq (\Delta - k) \cdot 2n,$$

$$\Rightarrow \quad \mathcal{R} \geq 1 - (\Delta - k)\frac{2n}{N} = 1 - 2\frac{\Delta - k}{\Delta} = 2r - 1.$$

Relative Minimum Distance

[Sipser Spielman '96]

$$D \geq N\left(\frac{\delta - \gamma_{\mathcal{G}}}{1 - \gamma_{\mathcal{G}}}\right)^2 .$$

Linear-time Decoder of Zémor

Input: Received word $\boldsymbol{y} = (y_e)_{e \in E}$.

Let $\boldsymbol{z} \leftarrow \boldsymbol{y}$.

For $t \leftarrow 1$ **to** m **do** {

Let X stand for A if t is odd, and for B otherwise.

Iteration t: For every $v \in X$ let $(\boldsymbol{z})_{E(v)} \leftarrow \mathcal{D}\left((\boldsymbol{z})_{E(v)}\right)$.

`/* Decoder for` $\mathcal{C}$ `*/`

}

Output: $\boldsymbol{z}$.

Number of Correctable Errors

- Zémor's decoder:

$$J_Z \approx \frac{1}{4} \cdot N \left(\delta^2 - O(\gamma_{\mathcal{G}}) \right) \ .$$

Number of Correctable Errors

- Zémor's decoder:

$$J_Z \approx \frac{1}{4} \cdot N \left(\delta^2 - O(\gamma_{\mathcal{G}}) \right) \ .$$

- Using combination of Zémor and GMD decoding [Forney '66] the number of correctable errors becomes [Skachek Roth '03]:

$$J_{SR} \approx \frac{1}{2} \cdot N \left(\delta^2 - O(\gamma_{\mathcal{G}}) \right) \ .$$

Decoder Analysis

Let S_i be the set of corrupted vertices in A (in B) in i-th iteration for odd i (even i).

- Using expansion property, Zémor shows:

$$|S_{i+1}| \leq \rho |S_i|,$$

for some constant $\rho < 1$.

Decoder Analysis

Let S_i be the set of corrupted vertices in A (in B) in i-th iteration for odd i (even i).

- Using expansion property, Zémor shows:

$$|S_{i+1}| \leq \rho |S_i|,$$

  for some constant $\rho < 1$.
- There are only $O(\log n)$ iterations needed to correct all errors.

Time Complexity

- During each iteration, the algorithm will construct a list of pointers to all constraints that could be unsatisfied.

Time Complexity

- During each iteration, the algorithm will construct a list of pointers to all constraints that could be unsatisfied.
- On next iteration, only vertices that have neighbors, which value was changed during the last iteration, could be unsatisfied.

Time Complexity

- During each iteration, the algorithm will construct a list of pointers to all constraints that could be unsatisfied.
- On next iteration, only vertices that have neighbors, which value was changed during the last iteration, could be unsatisfied.
- The amount of work to be done is:

$$\begin{aligned} \Delta|S_0|(1+\rho+\rho^2+\rho^3+\cdots+\rho^{m-1}) &= \Delta|S_0|\frac{1-\rho^m}{1-\rho} \\ &< \Delta|S_0|\frac{1}{1-\rho} = O(N)\,. \end{aligned}$$

Code Modification in [Barg Zémor '02]

- Graph $\mathcal{G} = (V, E)$ is a Δ-regular bipartite undirected graph.

Code Modification in [Barg Zémor '02]

- Graph $\mathcal{G} = (V, E)$ is a Δ-regular bipartite undirected graph.
  - Vertex set $V = A \cup B$ such that $A \cap B = \emptyset$ and $|A| = |B| = n$.
  - Edge set E of size $n\Delta$ such that every edge in E has one endpoint in A and one endpoint in B.

Code Modification in [Barg Zémor '02]

- Graph $\mathcal{G} = (V, E)$ is a Δ-regular bipartite undirected graph.
  - Vertex set $V = A \cup B$ such that $A \cap B = \emptyset$ and $|A| = |B| = n$.
  - Edge set E of size $n\Delta$ such that every edge in E has one endpoint in A and one endpoint in B.
- Linear $[\Delta, k{=}r_A\Delta, \delta_A\Delta]$ and $[\Delta, r_B\Delta, \delta_B\Delta]$ codes $\mathcal{C}_A$ and $\mathcal{C}_B$, respectively, over $F = \mathrm{GF}(q)$.

Barg-Zémor's Construction

$\mathbb{C}$ is a linear code of length $|E|$ over F:

$$\mathbb{C} = \left\{ \boldsymbol{c} \in F^{|E|} \ : \ \begin{array}{c} (\boldsymbol{c})_{E(u)} \in \mathcal{C}_A \text{ for every } u \in A \text{ and} \\ (\boldsymbol{c})_{E(u)} \in \mathcal{C}_B \text{ for every } u \in B \end{array} \right\},$$

where $(\boldsymbol{c})_{E(u)}$ = the sub-word of $\boldsymbol{c}$ that is indexed by the set of edges incident with u.

Example

Take $k = 2$, $\Delta = 3$, $n = 4$.
Let G_A and G_B be generating matrices of $\mathcal{C}_A$ and $\mathcal{C}_B$ (respectively) over $F = \mathrm{GF}(2^2) = \{0, 1, \alpha, \alpha^2\}$:

$$G_A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & 0 \end{pmatrix},$$

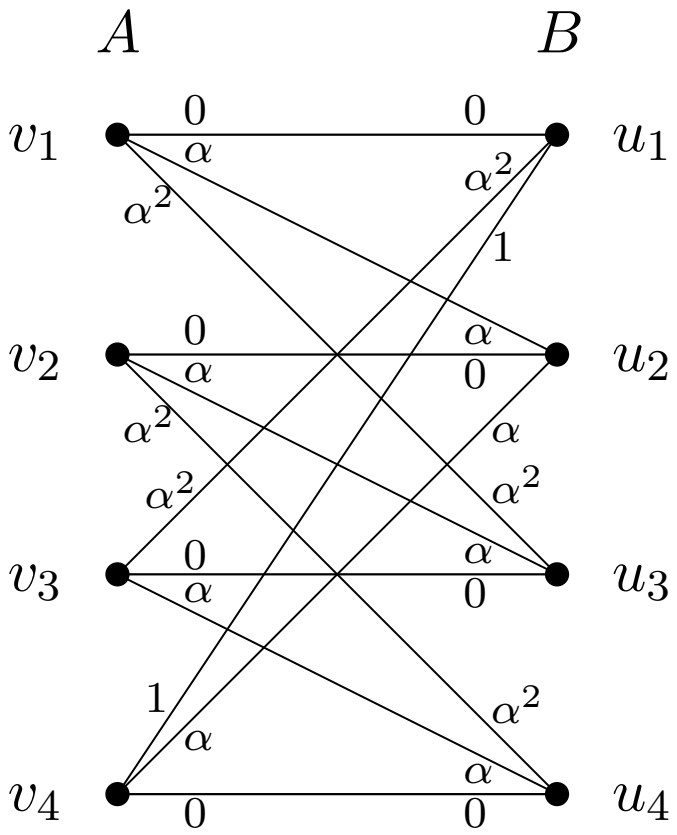
$$G_B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{pmatrix}.$$

Example

Take $k = 2$, $\Delta = 3$, $n = 4$.
Let G_A and G_B be generating matrices of $\mathcal{C}_A$ and $\mathcal{C}_B$ (respectively) over $F = \mathrm{GF}(2^2) = \{0, 1, \alpha, \alpha^2\}$:

$$G_A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & 0 \end{pmatrix},$$

$$G_B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{pmatrix}.$$



Results in [Barg Zémor '03]

In the presented construction:

- Codes $\mathcal{C}_A$ and $\mathcal{C}_B$ are random codes;
- Code $\mathbb{C}$ achieves the capacity of BSC under the linear-time expander iterative decoding. The decoding error probability decreases exponentially with the overall length.

Results in [Barg Zémor '03]

In the presented construction:

- Codes $\mathcal{C}_A$ and $\mathcal{C}_B$ are random codes;
- Code $\mathbb{C}$ achieves the capacity of BSC under the linear-time expander iterative decoding. The decoding error probability decreases exponentially with the overall length.

Further modified construction [Barg Zémor '03]

Results in [Barg Zémor '03]

In the presented construction:

- Codes $\mathcal{C}_A$ and $\mathcal{C}_B$ are random codes;
- Code $\mathbb{C}$ achieves the capacity of BSC under the linear-time expander iterative decoding. The decoding error probability decreases exponentially with the overall length.

Further modified construction [Barg Zémor '03]

- The error exponent similar to the error exponent of concatenated codes [Forney '66].

Results in [Barg Zémor '03]

In the presented construction:

- Codes $\mathcal{C}_A$ and $\mathcal{C}_B$ are random codes;
- Code $\mathbb{C}$ achieves the capacity of BSC under the linear-time expander iterative decoding. The decoding error probability decreases exponentially with the overall length.

Further modified construction [Barg Zémor '03]

- The error exponent similar to the error exponent of concatenated codes [Forney '66].
- The trade-offs between the code rate and the minimum distance attain the Zyablov bound.

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)

$$\delta(\mathcal{R}) \geq \frac{1}{4}(1-\mathcal{R})^2 \cdot \min_{\delta_{GV}((1+\mathcal{R})/2)<\mathsf{B}<\frac{1}{2}} \frac{g(\mathsf{B})}{\mathsf{H}_2(\mathsf{B})} \ ,$$

where the function $g(\mathsf{B})$ is defined in the next slides.

(ii)

$$\delta(\mathcal{R}) \geq \max_{\mathcal{R}\leq r\leq 1} \left\{ \min_{\delta_{GV}(r)<\mathsf{B}<\frac{1}{2}} \left(\delta_0(\mathsf{B},r) \cdot \frac{1-\mathcal{R}/r}{\mathsf{H}_2(\mathsf{B})} \right) \right\} \ ,$$

where the function $\delta_0(\mathsf{B},r)$ is defined in the next slides.

Definition of the Function $g(\mathsf{B})$

These two families of codes surpass the Zyablov bound.

Definition of the Function $g(\mathsf{B})$

These two families of codes surpass the Zyablov bound.

Let $\delta_{GV}(\mathcal{R}) = \mathsf{H}_2^{-1}(1-\mathcal{R})$, and let B_1 be the largest root of the equation

$$\mathsf{H}_2(\mathsf{B}) = \mathsf{H}_2(\mathsf{B}) \left(\mathsf{B} - \mathsf{H}_2(\mathsf{B}) \cdot \frac{\delta_{GV}(\mathcal{R})}{1-\mathcal{R}} \right) = -\left(\mathsf{B} - \delta_{GV}(\mathcal{R})\right) \cdot \log_2(1-\mathsf{B}) \ .$$

Moreover, let

$$a_1 = \frac{\mathsf{B}_1}{\mathsf{H}_2(\mathsf{B}_1)} - \frac{\delta_{GV}(\mathcal{R})}{\mathsf{H}_2(\delta_{GV}(\mathcal{R}))} \ ,$$

and

$$b_1 = \frac{\delta_{GV}(\mathcal{R})}{\mathsf{H}_2(\delta_{GV}(\mathcal{R}))} \cdot \mathsf{B}_1 - \frac{\mathsf{B}_1}{\mathsf{H}_2(\mathsf{B}_1)} \cdot \delta_{GV}(\mathcal{R})) \ .$$

Definition of the Function $g(\mathsf{B})$ (Cont.)

The function $g(\mathsf{B})$ is defined as

$$g(\mathsf{B}) = \begin{cases} \dfrac{\delta_{GV}(\mathcal{R})}{1-\mathcal{R}} & \text{if } \mathsf{B} \leq \delta_{GV}(\mathcal{R}) \\ \dfrac{\mathsf{B}}{\mathsf{H}_2(\mathsf{B})} & \text{if } \delta_{GV}(\mathcal{R}) \leq \mathsf{B} \text{ and } \mathcal{R} \leq 0.284 \\ \dfrac{a_1\mathsf{B}+b_1}{\mathsf{B}_1-\delta_{GV}(\mathcal{R})} & \text{if } \delta_{GV}(\mathcal{R}) \leq \mathsf{B} \leq \mathsf{B}_1 \text{ and } 0.284 < \mathcal{R} \leq 1 \\ \dfrac{\mathsf{B}}{\mathsf{H}_2(\mathsf{B})} & \text{if } \mathsf{B}_1 < \mathsf{B}_1 \leq 1 \text{ and } 0.284 < \mathcal{R} \leq 1 \end{cases}.$$

Definition of the Function $\delta_0(\mathsf{B}, r)$

The function $\delta_0(\mathsf{B}, r)$ is defined to be $\omega^{\star\star}(\mathsf{B})$ for $\delta_{GV}(r) \leq \mathsf{B} \leq \mathsf{B}_1$, where

$$\omega^{\star\star}(\mathsf{B}) = r\mathsf{B} + (1-r)\mathsf{H}_2^{-1}\left(1 - \frac{r}{1-r}\mathsf{H}_2(\mathsf{B})\right) ,$$

and B_1 is the only root of the equation

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

where

$$w^{\star}(\mathsf{B}) = (1-r)\left((2^{\mathsf{H}_2(\mathsf{B})/\mathsf{B}}+1)^{-1} + \frac{\mathsf{B}}{\mathsf{H}_2(\mathsf{B})}\left(1 - \mathsf{H}_2\left((2^{\mathsf{H}_2(\mathsf{B})/\mathsf{B}}+1)^{-1}\right)\right)\right) .$$

For $\mathsf{B}_1 \leq \mathsf{B} \leq \frac{1}{2}$, the function $\delta_0(\mathsf{B}, r)$ is defined to be a tangent to the function $\omega^{\star\star}(\mathsf{B})$ drawn from the point $\left(\frac{1}{2}, \omega^{\star}(\frac{1}{2})\right)$.

Nearly-MDS Codes of Guruswami and Indyk

- Used codes in [Zémor '01] as building blocks.

Nearly-MDS Codes of Guruswami and Indyk

- Used codes in [Zémor '01] as building blocks.
- The presented codes are linear-time *encodable* and decodable.

Nearly-MDS Codes of Guruswami and Indyk

- Used codes in [Zémor '01] as building blocks.
- The presented codes are linear-time *encodable* and decodable.
- Nearly-MDS: codes of rate $\mathcal{R}$ and relative minimum distance δ such that for any small ϵ:

$$\mathcal{R} + \delta \geq 1 - \epsilon \ .$$

Nearly-MDS Codes of Guruswami and Indyk

- Used codes in [Zémor '01] as building blocks.
- The presented codes are linear-time *encodable* and decodable.
- Nearly-MDS: codes of rate $\mathcal{R}$ and relative minimum distance δ such that for any small ϵ:

$$\mathcal{R} + \delta \geq 1 - \epsilon \ .$$

- The alphabet size is

$$\exp\left\{O\left((\log(1/\epsilon))/\mathcal{R}\epsilon^4\right)\right\} \ .$$

List of Results

- Nearly-MDS linear-time encodable and decodable expander codes.
  - Improvement on the minimum distance in [Barg Zémor '03].
  - Improvement on the number of correctable errors over [Barg Zémor '03].
  - Nearly-MDS codes that improve on the alphabet size in [Guruswami Indyk '02].
  - Suitable for a variety of channels.
  - Polynomiality of the decoding complexity as a function of the degree Δ.

List of Results

- Nearly-MDS linear-time encodable and decodable expander codes.
  - Improvement on the minimum distance in [Barg Zémor '03].
  - Improvement on the number of correctable errors over [Barg Zémor '03].
  - Nearly-MDS codes that improve on the alphabet size in [Guruswami Indyk '02].
  - Suitable for a variety of channels.
  - Polynomiality of the decoding complexity as a function of the degree Δ.
- Decoding over non-bipartite expanders.

List of Results (Cont.)

- Analysis of generalized expander codes.

List of Results (Cont.)

- Analysis of generalized expander codes.
- For capacity-approaching codes: reduction of the decoding error probability (polynomial $\rightarrow$ exponential), while preserving linear-time (in the length) and polynomial (in the gap to capacity) decoding.

List of Results (Cont.)

- Analysis of generalized expander codes.
- For capacity-approaching codes: reduction of the decoding error probability (polynomial $\rightarrow$ exponential), while preserving linear-time (in the length) and polynomial (in the gap to capacity) decoding.
- Bounds on the minimum distance of expander codes with *weak* constituent codes.

Our Construction

- Let $\Phi = F^k$. Fix a linear 1–1 mapping $\mathcal{E}_A : \Phi \to \mathcal{C}_A$ over F.

Our Construction

- Let $\Phi = F^k$. Fix a linear 1–1 mapping $\mathcal{E}_A : \Phi \to \mathcal{C}_A$ over F.
- Consider the mapping $\psi : \mathbb{C} \to \Phi^n$ given by

$$\psi(\boldsymbol{c}) = \left(\mathcal{E}_A^{-1}\left((\boldsymbol{c})_{E(u)}\right)\right)_{u \in A} , \quad \boldsymbol{c} \in \mathbb{C} .$$

Our Construction

- Let $\Phi = F^k$. Fix a linear 1–1 mapping $\mathcal{E}_A : \Phi \to \mathcal{C}_A$ over F.
- Consider the mapping $\psi : \mathbb{C} \to \Phi^n$ given by

$$\psi(\boldsymbol{c}) = \left(\mathcal{E}_A^{-1}\left((\boldsymbol{c})_{E(u)}\right)\right)_{u \in A} , \quad \boldsymbol{c} \in \mathbb{C} .$$

- Define the code $\mathbb{C}_\Phi$

$$\mathbb{C}_\Phi = \{\psi(\boldsymbol{c}) \ : \ \boldsymbol{c} \in \mathbb{C}\} \ \subseteq \ \Phi^n .$$

$\mathbb{C}_\Phi$ is linear over F.

Our Construction

- Let $\Phi = F^k$. Fix a linear 1–1 mapping $\mathcal{E}_A : \Phi \to \mathcal{C}_A$ over F.
- Consider the mapping $\psi : \mathbb{C} \to \Phi^n$ given by

$$\psi(\boldsymbol{c}) = \left(\mathcal{E}_A^{-1}\left((\boldsymbol{c})_{E(u)}\right)\right)_{u \in A} , \quad \boldsymbol{c} \in \mathbb{C} .$$

- Define the code $\mathbb{C}_\Phi$

$$\mathbb{C}_\Phi = \{\psi(\boldsymbol{c}) \ : \ \boldsymbol{c} \in \mathbb{C}\} \ \subseteq \ \Phi^n .$$

  $\mathbb{C}_\Phi$ is linear over F.
- The Barg-Zémor construction can be represented as a concatenated code with $\mathbb{C}_\Phi$ as the outer code and the inner code taken over a sub-field of F.

Example

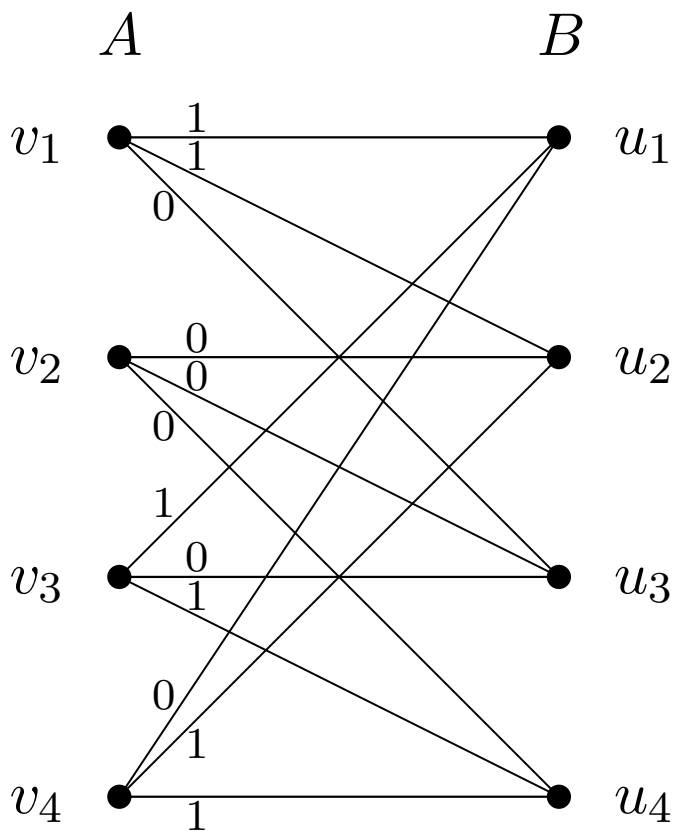
Let $k = 2$, $\Delta = 3$, $n = 4$.
Pick $F = \mathrm{GF}(2)$ and $\Phi = F^2$.
Take $\mathcal{C}_A = \mathcal{C}_B =$ parity code over F.
Let $\mathcal{E}_A(\boldsymbol{x}) = \boldsymbol{x}G_A$,

$$G_A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Example

Let $k = 2$, $\Delta = 3$, $n = 4$.
Pick $F = \mathrm{GF}(2)$ and $\Phi = F^2$.
Take $\mathcal{C}_A = \mathcal{C}_B =$ parity code over F.
Let $\mathcal{E}_A(\boldsymbol{x}) = \boldsymbol{x}G_A$,

$$G_A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$



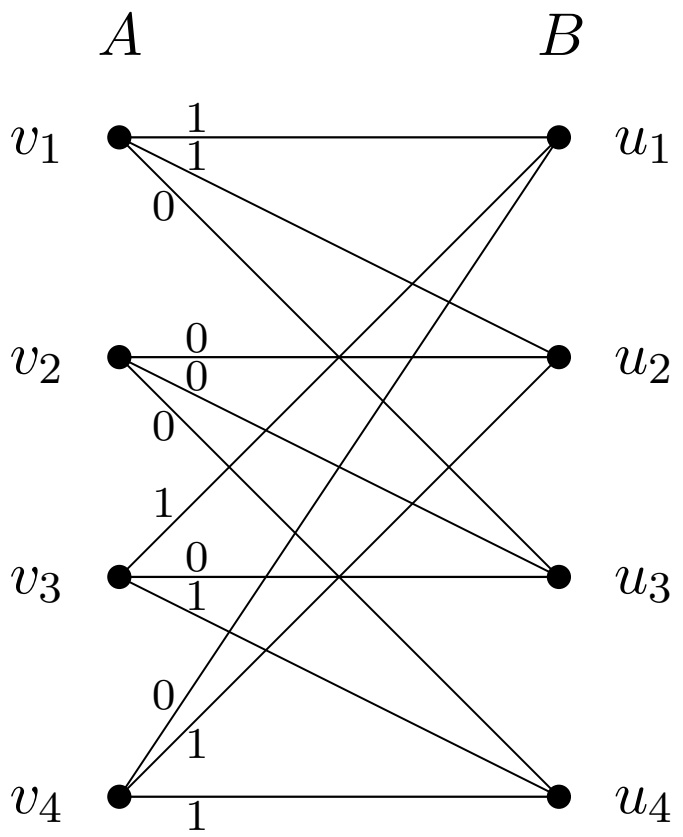
Example

Let $k = 2$, $\Delta = 3$, $n = 4$.
Pick $F = \mathrm{GF}(2)$ and $\Phi = F^2$.
Take $\mathcal{C}_A = \mathcal{C}_B =$ parity code over F.
Let $\mathcal{E}_A(\boldsymbol{x}) = \boldsymbol{x}G_A$,

$$G_A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} .$$

Then,

$$\begin{aligned} \boldsymbol{c} &= (\,1\,1\,0\,|\,0\,0\,0\,|\,1\,0\,1\,|\,0\,1\,1\,)\ , \\ \psi(\boldsymbol{c}) &= (\,\mathcal{E}_A^{-1}(110)\quad \mathcal{E}_A^{-1}(000) \\ &\qquad\quad \mathcal{E}_A^{-1}(101)\quad \mathcal{E}_A^{-1}(011)\,) \\ &= (\,11\ \ 00\ \ 10\ \ 01\,). \end{aligned}$$



Minimum Distance of $\mathbb{C}_\Phi$

- Let $\lambda_{\mathcal{G}}$ be the second largest eigenvalue of the adjacency matrix of $\mathcal{G}$, and let $\gamma_{\mathcal{G}} = \lambda_{\mathcal{G}}/\Delta$.

Minimum Distance of $\mathbb{C}_\Phi$

- Let $\lambda_\mathcal{G}$ be the second largest eigenvalue of the adjacency matrix of $\mathcal{G}$, and let $\gamma_\mathcal{G} = \lambda_\mathcal{G}/\Delta$.
- Relative minimum distance of $\mathbb{C}_\Phi$:

$$\delta_\Phi \geq \frac{\delta_B - \gamma_\mathcal{G}\sqrt{\delta_B/\delta_A}}{1-\gamma_\mathcal{G}} \; ;$$

in particular, $\delta_\Phi \to \delta_B$ whenever $\gamma_\mathcal{G} \to 0$.

Alphabet size

- For any design rate $\mathcal{R} < 1$ and $\epsilon > 0$ we obtain arbitrarily long codes $\mathbb{C}_\Phi$ such that $R_\Phi > \mathcal{R}$ and $\delta_\Phi \geq 1 - \mathcal{R} - \epsilon$ (thus approaching the Singleton bound when $\epsilon \to 0$).

Alphabet size

- For any design rate $\mathcal{R} < 1$ and $\epsilon > 0$ we obtain arbitrarily long codes $\mathbb{C}_\Phi$ such that $R_\Phi > \mathcal{R}$ and $\delta_\Phi \geq 1 - \mathcal{R} - \epsilon$ (thus approaching the Singleton bound when $\epsilon \to 0$).
- The alphabet size of $\mathbb{C}_\Phi$ is

$$\exp\left\{O\left((\log(1/\epsilon))/\epsilon^3\right)\right\} ,$$

compared with

$$\exp\left\{O\left((\log(1/\epsilon))/R\epsilon^4\right)\right\}$$

in [Guruswami Indyk '02].

Error-Erasure Decoder for $\mathbb{C}_\Phi$

Input: Received word $\boldsymbol{y} = (\boldsymbol{y}_u)_{u \in A}$ in $(\Phi \cup \{?\})^n$.

For $u \in A$ **do** $\quad (\boldsymbol{z})_{E(u)} \leftarrow \begin{cases} \mathcal{E}_A(\boldsymbol{y}_u) & \text{if } \boldsymbol{y}_u \in \Phi \\ ?? \cdots ? & \text{if } \boldsymbol{y}_u = ? \end{cases}$.

For $i \leftarrow 1, 2, \ldots, m$ **do** {

If i is even **then** $X \equiv A$, $\mathcal{D} \equiv \mathcal{D}_A$, **else** $X \equiv B$, $\mathcal{D} \equiv \mathcal{D}_B$.

For $u \in X$ **do** $(\boldsymbol{z})_{E(u)} \leftarrow \mathcal{D}((\boldsymbol{z})_{E(u)})$.

}

Output: $\psi(\boldsymbol{z})$ if $\boldsymbol{z} \in \mathbb{C}$ (and declare 'error' otherwise).

Error-Erasure Decoder for $\mathbb{C}_\Phi$ (Cont.)

- The algorithm makes use of a word $\boldsymbol{z} = (z_e)_{e \in E}$ over $F \cup \{?\}$, initialized by the contents of the received word $\boldsymbol{y}$ over $\Phi \cup \{?\}$.

Error-Erasure Decoder for $\mathbb{C}_\Phi$ (Cont.)

- The algorithm makes use of a word $\boldsymbol{z} = (z_e)_{e \in E}$ over $F \cup \{?\}$, initialized by the contents of the received word $\boldsymbol{y}$ over $\Phi \cup \{?\}$.
- Iterations $i = 2, 4, 6, \ldots$ use a decoder $\mathcal{D}_A : F^\Delta \to \mathcal{C}_A$ that recovers correctly any pattern of less than $\delta_A \Delta / 2$ errors (over F).

Error-Erasure Decoder for $\mathbb{C}_\Phi$ (Cont.)

- The algorithm makes use of a word $\boldsymbol{z} = (z_e)_{e \in E}$ over $F \cup \{?\}$, initialized by the contents of the received word $\boldsymbol{y}$ over $\Phi \cup \{?\}$.
- Iterations $i = 2, 4, 6, \ldots$ use a decoder $\mathcal{D}_A : F^\Delta \to \mathcal{C}_A$ that recovers correctly any pattern of less than $\delta_A \Delta / 2$ errors (over F).
- Iterations $i = 1, 3, 5, \ldots$ use a decoder $\mathcal{D}_B : (F \cup \{?\})^\Delta \to \mathcal{C}_B$ that recovers correctly any pattern of θ errors and ν erasures, provided that $2\theta + \nu < \delta_B \Delta$.

Error-Correcting Capabilities

- The decoder corrects any pattern of μ errors and ρ erasures, provided that $\mu + \frac{1}{2}\rho < \alpha n$, where

$$\alpha = \frac{(\delta_B/2) - \gamma_{\mathcal{G}}\sqrt{\delta_B/\delta_A}}{1 - \gamma_{\mathcal{G}}} \; ;$$

  in particular, $\alpha \to \delta_B/2$ when $\gamma_{\mathcal{G}} \to 0$.

Error-Correcting Capabilities

- The decoder corrects any pattern of μ errors and ρ erasures, provided that $\mu + \frac{1}{2}\rho < \alpha n$, where

$$\alpha = \frac{(\delta_B/2) - \gamma_{\mathcal{G}}\sqrt{\delta_B/\delta_A}}{1 - \gamma_{\mathcal{G}}} \; ;$$

  in particular, $\alpha \to \delta_B/2$ when $\gamma_{\mathcal{G}} \to 0$.
- The value of m is logarithmic in n.

Error-Correcting Capabilities

- The decoder corrects any pattern of μ errors and ρ erasures, provided that $\mu + \frac{1}{2}\rho < \alpha n$, where

$$\alpha = \frac{(\delta_B/2) - \gamma_{\mathcal{G}}\sqrt{\delta_B/\delta_A}}{1 - \gamma_{\mathcal{G}}} \; ;$$

  in particular, $\alpha \to \delta_B/2$ when $\gamma_{\mathcal{G}} \to 0$.
- The value of m is logarithmic in n.
- The overall time complexity of the algorithm is linear in n.

Applications

Pick $\mathbb{C}_\Phi$ to replace an MDS outer code in asymptotic concatenated code constructions. This leads to codes attaining:

- the Zyablov bound — our bound on the minimum distance and the number of correctable errors improves on the analysis of Barg-Zemor;

Applications

Pick $\mathbb{C}_\Phi$ to replace an MDS outer code in asymptotic concatenated code constructions. This leads to codes attaining:

- the Zyablov bound — our bound on the minimum distance and the number of correctable errors improves on the analysis of Barg-Zemor;
- the capacity of the memoryless symmetric channel with linear-time decoding and exponentially decaying error probability.

Linear Encoding

Using $\mathbb{C}_\Phi$ as a building block, we were able to construct a nearly-MDS code family that is *linear-time encodable and decodable*. The alphabet size of the new codes is again

$$\exp\left\{O\left((\log(1/\epsilon))/\epsilon^3\right)\right\} ,$$

compared with

$$\exp\left\{O\left((\log(1/\epsilon))/\mathcal{R}\epsilon^4\right)\right\}$$

in the construction of linear-time encodable and decodable code of [Guruswami Indyk '02].

Decoding over Non-bipartite Graph

- Recall that the relative minimum distance of the expander code based on a constituent code $\mathcal{C}$ of minimum distance δ is $\delta^2 + o_\Delta(1)$.

Decoding over Non-bipartite Graph

- Recall that the relative minimum distance of the expander code based on a constituent code $\mathcal{C}$ of minimum distance δ is $\delta^2 + o_\Delta(1)$.
- Fraction of correctable errors in [Sipser Spielman '96] is around $\frac{1}{48} \cdot \delta^2$.

Decoding over Non-bipartite Graph

- Recall that the relative minimum distance of the expander code based on a constituent code $\mathcal{C}$ of minimum distance δ is $\delta^2 + o_\Delta(1)$.
- Fraction of correctable errors in [Sipser Spielman '96] is around $\frac{1}{48} \cdot \delta^2$.
- By using *a bipartite graph*, this fraction was improved up to almost $\frac{1}{4} \cdot \delta^2$ and $\frac{1}{2} \cdot \delta^2$, respectively ([Zémor '01], [Skachek Roth '03]).

Decoding over Non-bipartite Graph

- Recall that the relative minimum distance of the expander code based on a constituent code $\mathcal{C}$ of minimum distance δ is $\delta^2 + o_\Delta(1)$.
- Fraction of correctable errors in [Sipser Spielman '96] is around $\frac{1}{48} \cdot \delta^2$.
- By using *a bipartite graph*, this fraction was improved up to almost $\frac{1}{4} \cdot \delta^2$ and $\frac{1}{2} \cdot \delta^2$, respectively ([Zémor '01], [Skachek Roth '03]).

Problem

Could the fraction of correctable errors become close to a half of the minimum distance when using a non-bipartite graph?

Reduction

- Let $\mathcal{G} = (V, E)$ be a non-bipartite underlying graph. Define a new graph $\widehat{\mathcal{G}} = (\widehat{V}, \widehat{E})$.

Reduction

- Let $\mathcal{G} = (V, E)$ be a non-bipartite underlying graph. Define a new graph $\widehat{\mathcal{G}} = (\widehat{V}, \widehat{E})$.
  - For each vertex $v \in V$ we define vertices $v_1 \in V_1$, $v_2 \in V_2$.
  - For each edge $e = a—b$ in $\mathcal{G}$, we let $\widehat{\mathcal{G}}$ contain two edges:

$$e_1 = a_1—b_2 \ , \qquad e_2 = a_2—b_1 \ .$$

  - The second largest eigenvalue of the adjacency matrix of $\widehat{\mathcal{G}}$ equals $\lambda_{\mathcal{G}}$.

Reduction

- Let $\mathcal{G} = (V, E)$ be a non-bipartite underlying graph. Define a new graph $\widehat{\mathcal{G}} = (\widehat{V}, \widehat{E})$.
  - For each vertex $v \in V$ we define vertices $v_1 \in V_1$, $v_2 \in V_2$.
  - For each edge $e = a—b$ in $\mathcal{G}$, we let $\widehat{\mathcal{G}}$ contain two edges:

$$e_1 = a_1—b_2 \ , \qquad e_2 = a_2—b_1 \ .$$

  - The second largest eigenvalue of the adjacency matrix of $\widehat{\mathcal{G}}$ equals $\lambda_{\mathcal{G}}$.
- Define the code $\widehat{\mathbb{C}}$ of length $n\Delta$ over F using the graph $\widehat{\mathcal{G}}$:

$$\widehat{\mathbb{C}} = \left\{ \boldsymbol{c} \in F^{n\Delta} \ : \ (\boldsymbol{c})_{\widehat{E}(u)} \in \mathcal{C} \text{ for every } u \in \widehat{E} \right\} .$$

Reduction

- Let $\mathcal{G} = (V, E)$ be a non-bipartite underlying graph. Define a new graph $\widehat{\mathcal{G}} = (\widehat{V}, \widehat{E})$.
  - For each vertex $v \in V$ we define vertices $v_1 \in V_1$, $v_2 \in V_2$.
  - For each edge $e = a—b$ in $\mathcal{G}$, we let $\widehat{\mathcal{G}}$ contain two edges:

$$e_1 = a_1—b_2 \ , \qquad e_2 = a_2—b_1 \ .$$

  - The second largest eigenvalue of the adjacency matrix of $\widehat{\mathcal{G}}$ equals $\lambda_{\mathcal{G}}$.
- Define the code $\widehat{\mathbb{C}}$ of length $n\Delta$ over F using the graph $\widehat{\mathcal{G}}$:

$$\widehat{\mathbb{C}} = \left\{ \boldsymbol{c} \in F^{n\Delta} \ : \ (\boldsymbol{c})_{\widehat{E}(u)} \in \mathcal{C} \text{ for every } u \in \widehat{E} \right\} .$$

- Define mapping $\widehat{\varphi}$, such that for $\boldsymbol{y} \in F^{|E|}$,

$$\left(\widehat{\varphi}(\boldsymbol{y})\right)_{e_1} = \left(\widehat{\varphi}(\boldsymbol{y})\right)_{e_2} = y_e \ .$$

Decoding

Input: Received word $\boldsymbol{y} = (y_e)_{e \in E}$ in $F^{|E|}$.

Let $\boldsymbol{z} \leftarrow \widehat{\varphi}(\boldsymbol{y})$.

Let $\boldsymbol{z} \leftarrow \mathcal{D}(\boldsymbol{z})$.

Output: $\widehat{\varphi}^{-1}(\boldsymbol{z})$ if there exists $\boldsymbol{c} \in \mathbb{C}$ such that $\boldsymbol{z} = \widehat{\varphi}(\boldsymbol{c})$ (and declare 'error' otherwise).

Generalized Expander Codes

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

Generalized Expander Codes

- Let $B^1 \cap B^2 = \emptyset$, $B^1 \cup B^2 = B$, and let $|B^2| = \eta n$, where $\eta \in [0, 1]$.
- Take F be the field $\mathrm{GF}(q)$ and let $\mathcal{C}_A$, $\mathcal{C}_1$ and $\mathcal{C}_2$ be 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 F, respectively.

Generalized Expander Codes

- Let $B^1 \cap B^2 = \emptyset$, $B^1 \cup B^2 = B$, and let $|B^2| = \eta n$, where $\eta \in [0, 1]$.
- Take F be the field $\mathrm{GF}(q)$ and let $\mathcal{C}_A$, $\mathcal{C}_1$ and $\mathcal{C}_2$ be 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 F, respectively.

We define the linear code of length $|E|$ over F:

$$\mathbb{C} = \Big\{ \boldsymbol{c} \in F^{|E|} \ : \ (\boldsymbol{c})_{E(u)} \in \mathcal{C}_A \text{ for every } u \in A,$$

$$(\boldsymbol{c})_{E(u)} \in \mathcal{C}_1 \text{ for every } u \in B^1 \ , \text{ and } (\boldsymbol{c})_{E(u)} \in \mathcal{C}_2 \text{ for every } u \in B^2 \Big\}$$

(for $\eta = 0, 1$ or, alternatively, for $\mathcal{C}_1 = \mathcal{C}_2$, $\mathbb{C}$ coincides with the code discussed before).

Generalized Expander Codes (Cont.)

- It is possible to select parameters of the code $\mathbb{C}$ so the Zyablov bound is attained.

Generalized Expander Codes (Cont.)

- It is possible to select parameters of the code $\mathbb{C}$ so the Zyablov bound is attained.
- Linear-time decoding algorithm that corrects number of errors close to a half of that minimum distance.

Generalized Expander Codes (Cont.)

- It is possible to select parameters of the code $\mathbb{C}$ so the Zyablov bound is attained.
- Linear-time decoding algorithm that corrects number of errors close to a half of that minimum distance.
- More sophisticated analysis leads to the bound on the minimum distance that coincides with the bound in [Barg Zémor '04].

Generalized Expander Codes (Cont.)

- It is possible to select parameters of the code $\mathbb{C}$ so the Zyablov bound is attained.
- Linear-time decoding algorithm that corrects number of errors close to a half of that minimum distance.
- More sophisticated analysis leads to the bound on the minimum distance that coincides with the bound in [Barg Zémor '04].

Conclusion

The presented codes are a generalization of the known expander codes (yet they are different), and have parameters as good as those of the best known expander codes. Could the generalized expander codes have better parameters than the known expander codes have?

Problem Statement

Consider codes of rate $\mathcal{R}$ transmitted over a communication channel of capacity C. Let $\mathcal{R} = (1 - \varepsilon)C$.

Problem Statement

Consider codes of rate $\mathcal{R}$ transmitted over a communication channel of capacity C. Let $\mathcal{R} = (1 - \varepsilon)C$.

Our Goal

Codes with the following properties:

- Attain the capacity of a variety of memoryless symmetric channels.

Problem Statement

Consider codes of rate $\mathcal{R}$ transmitted over a communication channel of capacity C. Let $\mathcal{R} = (1 - \varepsilon)C$.

Our Goal

Codes with the following properties:

- Attain the capacity of a variety of memoryless symmetric channels.
- Decoding error probability decreases exponentially with the code length.

Problem Statement

Consider codes of rate $\mathcal{R}$ transmitted over a communication channel of capacity C. Let $\mathcal{R} = (1 - \varepsilon)C$.

Our Goal

Codes with the following properties:

- Attain the capacity of a variety of memoryless symmetric channels.
- Decoding error probability decreases exponentially with the code length.
- Decoding time complexity is linear in the length and polynomial in $1/\varepsilon$.

LDPC Codes

- √ Attain the capacity of BEC [Luby Mitzenmacher Shokrollahi Spielman '01], [Oswald Shokrollahi '02], and a variety of other communication channels [Richardson Shokrollahi Urbanke '01].

LDPC Codes

- ✓ Attain the capacity of BEC [Luby Mitzenmacher Shokrollahi Spielman '01], [Oswald Shokrollahi '02], and a variety of other communication channels [Richardson Shokrollahi Urbanke '01].
- × Decoding error probability is believed to decrease polynomially with the code length.

LDPC Codes

- ✓ Attain the capacity of BEC [Luby Mitzenmacher Shokrollahi Spielman '01], [Oswald Shokrollahi '02], and a variety of other communication channels [Richardson Shokrollahi Urbanke '01].
- × Decoding error probability is believed to decrease polynomially with the code length.
- ✓ Decoding complexity per bit:
  - Conjectured in [Khandekar McEliece '01] for any 'typical' channel as $O\left(\log(1/\pi) + 1/\varepsilon \cdot \log(1/\varepsilon)\right)$, where π is a decoded error probability.
  - LDPC over BEC: $O\left(\log(1/\varepsilon)\right)$ [Luby Mitzenmacher Shokrollahi Spielman '01], [Oswald Shokrollahi '02].
  - IRA over BEC: a bounded constant [Pfister Sason Urbanke '04].

Expander Codes

- $\surd$ Attain the capacity of a variety of memoryless symmetric channels [Barg Zémor '02, '03], [Roth Skachek '04], [Feldman Stein '04].

Expander Codes

- √ Attain the capacity of a variety of memoryless symmetric channels [Barg Zémor '02, '03], [Roth Skachek '04], [Feldman Stein '04].
- √ Decoding error probability is shown to decrease exponentially with the code length.

Expander Codes

- √ Attain the capacity of a variety of memoryless symmetric channels [Barg Zémor '02, '03], [Roth Skachek '04], [Feldman Stein '04].
- √ Decoding error probability is shown to decrease exponentially with the code length.
- ? Decoding time complexity
  - is linear in a code length;
  - how does it depend on $1/\varepsilon$?

Our Approach

Memoryless BSC with crossover probability p, and capacity $C = 1 - \mathsf{H}_2(p)$.

Our Approach

Memoryless BSC with crossover probability p, and capacity $C = 1 - \mathsf{H}_2(p)$.

We consider concatenated codes $\mathbb{C}_{cont}$ with:

- A family of the nearly-MDS expander codes $\mathbb{C}_\Phi$ as outer codes.

Our Approach

Memoryless BSC with crossover probability p, and capacity $C = 1 - \mathsf{H}_2(p)$.

We consider concatenated codes $\mathbb{C}_{cont}$ with:

- A family of the nearly-MDS expander codes $\mathbb{C}_\Phi$ as outer codes.
- A 'typical' binary LDPC codes $\mathcal{C}_{in}$ of (constant for a fixed ε) length n_{in} as an inner code.

We derive a condition on the parameters of LDPC codes, sufficient for exponential decay of error probability of $\mathbb{C}_{cont}$.

Characteristics of 'Typical' LDPC Codes

Decoding Complexity

We assume that for LDPC (or other) codes over BSC it is given by:

$$O\left(n_{in}^{s} \cdot \frac{1}{\varepsilon^{r}}\right) .$$

(r is a positive constant, for LDPC codes essentially $s = 1$).

Characteristics of 'Typical' LDPC Codes

Decoding Complexity

We assume that for LDPC (or other) codes over BSC it is given by:

$$O\left(n_{in}^{s} \cdot \frac{1}{\varepsilon^{r}}\right) .$$

(r is a positive constant, for LDPC codes essentially $s = 1$).

Decoding error probability $\mathsf{Prob}_e(\mathcal{C}_{in})$

- No satisfying results on asymptotic behavior for LDPC codes over BEC or other channels.
- We obtain a sufficient condition to guarantee that $\mathsf{Prob}_e(\mathbb{C}_{cont})$ decreases exponentially.

Sufficient Condition

Notation $\mathcal{C}_{in}\,[\mathcal{R}_{in}, n_{in}]$ is for the code $\mathcal{C}_{in}$ of rate $\mathcal{R}_{in}$ and length n_{in}.

Sufficient Condition

Notation $\mathcal{C}_{in}\,[\mathcal{R}_{in}, n_{in}]$ is for the code $\mathcal{C}_{in}$ of rate $\mathcal{R}_{in}$ and length n_{in}.

Theorem

Consider a BSC, and let C be its capacity. Suppose that:

(i) *There exist constants $\mathsf{b} > 0$, $\vartheta > 0$, $\varepsilon_1 \in (0,1)$, such that for any ϵ, $0 < \epsilon < \varepsilon_1$, and for a sequence of alphabets $\{\Phi_i\}_{i=1}^{\infty}$ where the sequence $\{\log_2 |\Phi_i|\}_{i=1}^{\infty}$ is dense, there exists a family of codes $\mathbb{C}_\Phi$ of rate $1-\epsilon$ (with their respective decoders) that can correct a fraction $\vartheta\epsilon^{\mathsf{b}}$ of errors.*

Sufficient Condition

Notation $\mathcal{C}_{in}\,[\mathcal{R}_{in}, n_{in}]$ is for the code $\mathcal{C}_{in}$ of rate $\mathcal{R}_{in}$ and length n_{in}.

Theorem

Consider a BSC, and let C be its capacity. Suppose that:

(i) *There exist constants $\mathsf{b} > 0$, $\vartheta > 0$, $\varepsilon_1 \in (0,1)$, such that for any ϵ, $0 < \epsilon < \varepsilon_1$, and for a sequence of alphabets $\{\Phi_i\}_{i=1}^{\infty}$ where the sequence $\{\log_2 |\Phi_i|\}_{i=1}^{\infty}$ is dense, there exists a family of codes $\mathbb{C}_\Phi$ of rate $1-\epsilon$ (with their respective decoders) that can correct a fraction $\vartheta\epsilon^{\mathsf{b}}$ of errors.*

(ii) *There exist constants $\varepsilon_2 \in (0,1)$ and $h_0 > 0$, such that for any ϵ, $0 < \epsilon < \varepsilon_2$, the decoding error probability of a family of codes $\mathcal{C}_{in}$ satisfies*

$$\mathsf{Prob}_e\left(\mathcal{C}_{in}\left[(1-\epsilon)C,\ \frac{1}{\epsilon^{h_0}}\right]\right) < \epsilon^{\mathsf{b}}\ .$$

Sufficient Condition (Cont.)

Then, for any rate $\mathcal{R} < C$, there exist a family of the codes $\mathbb{C}_{cont}$ (with respective decoder) that has an exponentially decaying (in its length) error probability.

Sufficient Condition (Cont.)

Then, for any rate $\mathcal{R} < C$, there exist a family of the codes $\mathbb{C}_{cont}$ (with respective decoder) that has an exponentially decaying (in its length) error probability.

Time Complexity

We show that over a BSC, when taking code $\mathbb{C}_{cont}$ with the outer code $\mathbb{C}_{\Phi}$ and the inner code $\mathcal{C}_{in}$ as assumed, the decoding time complexity of is given by

$$N \cdot \textsc{Poly}(1/\varepsilon) \ .$$

Decoding in [Barg Zémor '02] and [Barg Zémor '03]

We show that the codes in [Barg Zémor '02] and [Barg Zémor '03] cannot be tuned to have all three aforementioned properties.

Asymptotic Goodness

Definition

A family of codes $\{C_i\}_{i=0}^{\infty}$, where each C_i is a $[n_i, k_i, d_i]$ linear code, is said to be *asymptotically good* if it satisfies the following conditions:

- The length n_i of C_i approaches infinity as $i \to \infty$.

Asymptotic Goodness

Definition

A family of codes $\{C_i\}_{i=0}^{\infty}$, where each C_i is a $[n_i, k_i, d_i]$ linear code, is said to be *asymptotically good* if it satisfies the following conditions:

- The length n_i of C_i approaches infinity as $i \to \infty$.
- $\lim_{i\to\infty} \frac{d_i}{n_i} = \delta > 0$

Asymptotic Goodness

Definition

A family of codes $\{C_i\}_{i=0}^{\infty}$, where each C_i is a $[n_i, k_i, d_i]$ linear code, is said to be *asymptotically good* if it satisfies the following conditions:

- The length n_i of C_i approaches infinity as $i \to \infty$.
- $\lim_{i\to\infty} \frac{d_i}{n_i} = \delta > 0$
- $\lim_{i\to\infty} \frac{k_i}{n_i} = \mathcal{R} > 0$

Asymptotic Goodness

Definition

A family of codes $\{C_i\}_{i=0}^{\infty}$, where each C_i is a $[n_i, k_i, d_i]$ linear code, is said to be *asymptotically good* if it satisfies the following conditions:

- The length n_i of C_i approaches infinity as $i \to \infty$.
- $\lim_{i\to\infty} \frac{d_i}{n_i} = \delta > 0$
- $\lim_{i\to\infty} \frac{k_i}{n_i} = \mathcal{R} > 0$

Problem Statement

How weak the constituent codes $\mathcal{C}_A$ and $\mathcal{C}_B$ could be such that the overall expander code will be asymptotically good?

Asymptotic Goodness – Some Answers

The known bound on the minimum distance of $\mathbb{C}$:

$$\delta \geq \frac{\delta_A \delta_B - \gamma_{\mathcal{G}} \sqrt{\delta_A \delta_B}}{1 - \gamma_{\mathcal{G}}} \, .$$

Asymptotic Goodness – Some Answers

The known bound on the minimum distance of $\mathbb{C}$:

$$\delta \geq \frac{\delta_A \delta_B - \gamma_{\mathcal{G}} \sqrt{\delta_A \delta_B}}{1 - \gamma_{\mathcal{G}}} \, .$$

This yields the sufficient condition $\sqrt{d_A d_B} > \gamma_{\mathcal{G}} \Delta = \lambda_{\mathcal{G}}$.

Asymptotic Goodness – Some Answers

The known bound on the minimum distance of $\mathbb{C}$:

$$\delta \geq \frac{\delta_A \delta_B - \gamma_{\mathcal{G}} \sqrt{\delta_A \delta_B}}{1 - \gamma_{\mathcal{G}}} .$$

This yields the sufficient condition $\sqrt{d_A d_B} > \gamma_{\mathcal{G}} \Delta = \lambda_{\mathcal{G}}$.

[Barg Zémor '04]

If $d_A \geq 3$ and $d_B \geq 3$, then for the random bipartite graph $\mathcal{G}$ with probability close to 1, the resulting code $\mathbb{C}$ is good asymptotically.

Codes of Minimum Distance 2

Theorem

Let $\mathcal{C}_A$ and $\mathcal{C}_B$ be codes of minimum distance 2, and let $\mathcal{G}$ be any Δ-regular bipartite graph. Then, the minimum distance of such code $\mathbb{C}$ is bounded from above by

$$D \leq O\left(\log_{\Delta-1}(n)\right) .$$

Moreover, if the underlying graph $\mathcal{G}$ is a Ramanujan graph as in [Lubotsky Philips Sarnak '88] or [Margulis '88], then the minimum distance of $\mathbb{C}$ is bounded from below by

$$D \geq \frac{4}{3}\log_{\Delta-1}(2n) .$$

Simple Lower Bound

Theorem

Consider the code $\mathbb{C}$ with the constituent codes $\mathcal{C}_A$ and $\mathcal{C}_B$ of minimum distance $d_A \geq 2$ and $d_B \geq 2$, respectively, with the underlying graph $\mathcal{G}$ as in [Lubotsky Philips Sarnak '88] or [Margulis '88]. Then, its relative minimum distance is bounded from below by

$$D \geq (2n)^{1/3 \cdot \log_{\Delta-1}(d_A-1)(d_B-1)} - 1 \, .$$

Sufficient Condition

Theorem

Let $\mathcal{C}_A$ and $\mathcal{C}_B(u)$ (for every $u \in B$) be linear codes with the minimum distance $d_A = \delta_A \Delta$ and d_B, respectively. Let $\mathcal{G}$ be a bipartite (α, ζ)-expander such that the degree of every $u \in A$ is Δ. If

$$\frac{\delta_A}{\zeta + \delta_A - 1} < d_B \ ,$$

then the relative minimum distance of $\mathbb{C}$ is $\geq \alpha \delta_A$.

Open Problems

- Further improvements on rate-distance trade-offs.

Open Problems

- Further improvements on rate-distance trade-offs.
- Further improvements on the alphabet size of nearly-MDS codes.

Open Problems

- Further improvements on rate-distance trade-offs.
- Further improvements on the alphabet size of nearly-MDS codes.
- Constructions using different types of expander graphs.

Open Problems

- Further improvements on rate-distance trade-offs.
- Further improvements on the alphabet size of nearly-MDS codes.
- Constructions using different types of expander graphs.
- Are the generalized expander codes have better parameters than any previously known expander codes?

Open Problems

- Further improvements on rate-distance trade-offs.
- Further improvements on the alphabet size of nearly-MDS codes.
- Constructions using different types of expander graphs.
- Are the generalized expander codes have better parameters than any previously known expander codes?
- Improved criteria for asymptotic goodness of expander codes with weak constituent codes.

Open Problems

- Further improvements on rate-distance trade-offs.
- Further improvements on the alphabet size of nearly-MDS codes.
- Constructions using different types of expander graphs.
- Are the generalized expander codes have better parameters than any previously known expander codes?
- Improved criteria for asymptotic goodness of expander codes with weak constituent codes.
- Bounds on the minimum pseudo-code weight of expander codes over AWGN channel.

Open Problems

- Further improvements on rate-distance trade-offs.
- Further improvements on the alphabet size of nearly-MDS codes.
- Constructions using different types of expander graphs.
- Are the generalized expander codes have better parameters than any previously known expander codes?
- Improved criteria for asymptotic goodness of expander codes with weak constituent codes.
- Bounds on the minimum pseudo-code weight of expander codes over AWGN channel.
- Construction of constrained LDPC (expander) codes.

Conclusion

Combining classical techniques from coding theory, like GMD-decoding, concatenated code analysis, algebraic coding, and others, with expander-based constructions leads to interesting results, such as constructions of provably linear-time encodable and decodable LDPC codes that have better parameters.