Array BP-XOR Codes for Reliable Cloud Storage Systems

Yongge Wang

UNC Charlotte, USA

July 7–12, 2013 / IEEE ISIT / Istanbul, Turkey

Outline

Outline

Outline

Outline

Outline

Outline

Slogan for Cloud Computing

Moving Computation Is Easy Than Moving Data

EaaS and Remote Computation on Data

- IaaS, PaaS, SaaS, NaaS, EaaS, etc.
- data (services) are stored at remote client
- we may need the remote cloud server to process some query (processing) on these data instead of downloading the data to local computer and process the data

EaaS and Remote Computation on Data

- IaaS, PaaS, SaaS, NaaS, EaaS, etc.
- data (services) are stored at remote client
- we may need the remote cloud server to process some query (processing) on these data instead of downloading the data to local computer and process the data

EaaS and Remote Computation on Data

- IaaS, PaaS, SaaS, NaaS, EaaS, etc.
- data (services) are stored at remote client
- we may need the remote cloud server to process some query (processing) on these data instead of downloading the data to local computer and process the data

Where is the privacy?

- Data is stored on the remote server in clear?
- we do not trust the remote server
- what is the solution?
- encrypt the data and store the cipher text?
- how can do “computation on the data remotely”?

Where is the privacy?

- Data is stored on the remote server in clear?
- we do not trust the remote server
- what is the solution?
- encrypt the data and store the cipher text?
- how can do “computation on the data remotely”?

Where is the privacy?

- Data is stored on the remote server in clear?
- we do not trust the remote server
- what is the solution?
- encrypt the data and store the cipher text?
- how can do “computation on the data remotely”?

Where is the privacy?

- Data is stored on the remote server in clear?
- we do not trust the remote server
- what is the solution?
- encrypt the data and store the cipher text?
- how can do “computation on the data remotely”?

Where is the privacy?

- Data is stored on the remote server in clear?
- we do not trust the remote server
- what is the solution?
- encrypt the data and store the cipher text?
- how can do “computation on the data remotely”?

Examples

- many choices for personal cloud data storage
- Dropbox, SkyDrive, Google Drive, Amazon Cloud drive, Apple iCloud, Ubuntu One, etc.
- do you trust any one of these server and put your data (your memory) there?
- reliability? privacy?

Examples

- many choices for personal cloud data storage
- Dropbox, SkyDrive, Google Drive, Amazon Cloud drive, Apple iCloud, Ubuntu One, etc.
- do you trust any one of these server and put your data (your memory) there?
- reliability? privacy?

Examples

- many choices for personal cloud data storage
- Dropbox, SkyDrive, Google Drive, Amazon Cloud drive, Apple iCloud, Ubuntu One, etc.
- do you trust any one of these server and put your data (your memory) there?
- reliability? privacy?

Examples

- many choices for personal cloud data storage
- Dropbox, SkyDrive, Google Drive, Amazon Cloud drive, Apple iCloud, Ubuntu One, etc.
- do you trust any one of these server and put your data (your memory) there?
- reliability? privacy?

Our Solution

- XOR-MDS codes are converted to XOR-based Secret Sharing Schemes
- 2-out-of-6 SSS (or 2 out of 3 SSS)
- Register accounts at: Dropbox, SkyDrive, Google Drive, Amazon Cloud drive, Apple iCloud, Ubuntu One, etc.
- data from any two servers are sufficient, but each single server learns zero information about data

Our Solution

- XOR-MDS codes are converted to XOR-based Secret Sharing Schemes
- 2-out-of-6 SSS (or 2 out of 3 SSS)
- Register accounts at: Dropbox, SkyDrive, Google Drive, Amazon Cloud drive, Apple iCloud, Ubuntu One, etc.
- data from any two servers are sufficient, but each single server learns zero information about data

Our Solution

- XOR-MDS codes are converted to XOR-based Secret Sharing Schemes
- 2-out-of-6 SSS (or 2 out of 3 SSS)
- Register accounts at: Dropbox, SkyDrive, Google Drive, Amazon Cloud drive, Apple iCloud, Ubuntu One, etc.
- data from any two servers are sufficient, but each single server learns zero information about data

Our Solution

- XOR-MDS codes are converted to XOR-based Secret Sharing Schemes
- 2-out-of-6 SSS (or 2 out of 3 SSS)
- Register accounts at: Dropbox, SkyDrive, Google Drive, Amazon Cloud drive, Apple iCloud, Ubuntu One, etc.
- data from any two servers are sufficient, but each single server learns zero information about data

Array Codes

- Mainly used for data storae system
- example array codes
  - Blaum, et al: EVENODD (2 disk faults)
  - Blaum, et al: extended EVENODD (3 disk faults).
  - $[2k, k, d]$ chain code
  - Simple Product Code (SPC)
  - Row-Diagonal Parity (RDP)
  - Blaum $RDP(p, i)$ for $i \leq 8$

Array Codes

- Mainly used for data storae system
- example array codes
  - Blaum, et al: EVENODD (2 disk faults)
  - Blaum, et al: extended EVENODD (3 disk faults).
  - $[2k, k, d]$ chain code
  - Simple Product Code (SPC)
  - Row-Diagonal Parity (RDP)
  - Blaum $RDP(p, i)$ for $i \leq 8$

Array Codes

- Mainly used for data storae system
- example array codes
  - Blaum, et al: EVENODD (2 disk faults)
  - Blaum, et al: extended EVENODD (3 disk faults).
  - $[2k, k, d]$ chain code
  - Simple Product Code (SPC)
  - Row-Diagonal Parity (RDP)
  - Blaum $RDP(p, i)$ for $i \leq 8$

Array Codes

- Mainly used for data storae system
- example array codes
  - Blaum, et al: EVENODD (2 disk faults)
  - Blaum, et al: extended EVENODD (3 disk faults).
  - $[2k, k, d]$ chain code
  - Simple Product Code (SPC)
  - Row-Diagonal Parity (RDP)
  - Blaum $RDP(p, i)$ for $i \leq 8$

Array Codes

- Mainly used for data storae system
- example array codes
  - Blaum, et al: EVENODD (2 disk faults)
  - Blaum, et al: extended EVENODD (3 disk faults).
  - $[2k, k, d]$ chain code
  - Simple Product Code (SPC)
  - Row-Diagonal Parity (RDP)
  - Blaum $RDP(p, i)$ for $i \leq 8$

Array Codes

- Mainly used for data storae system
- example array codes
  - Blaum, et al: EVENODD (2 disk faults)
  - Blaum, et al: extended EVENODD (3 disk faults).
  - $[2k, k, d]$ chain code
  - Simple Product Code (SPC)
  - Row-Diagonal Parity (RDP)
  - Blaum $RDP(p, i)$ for $i \leq 8$

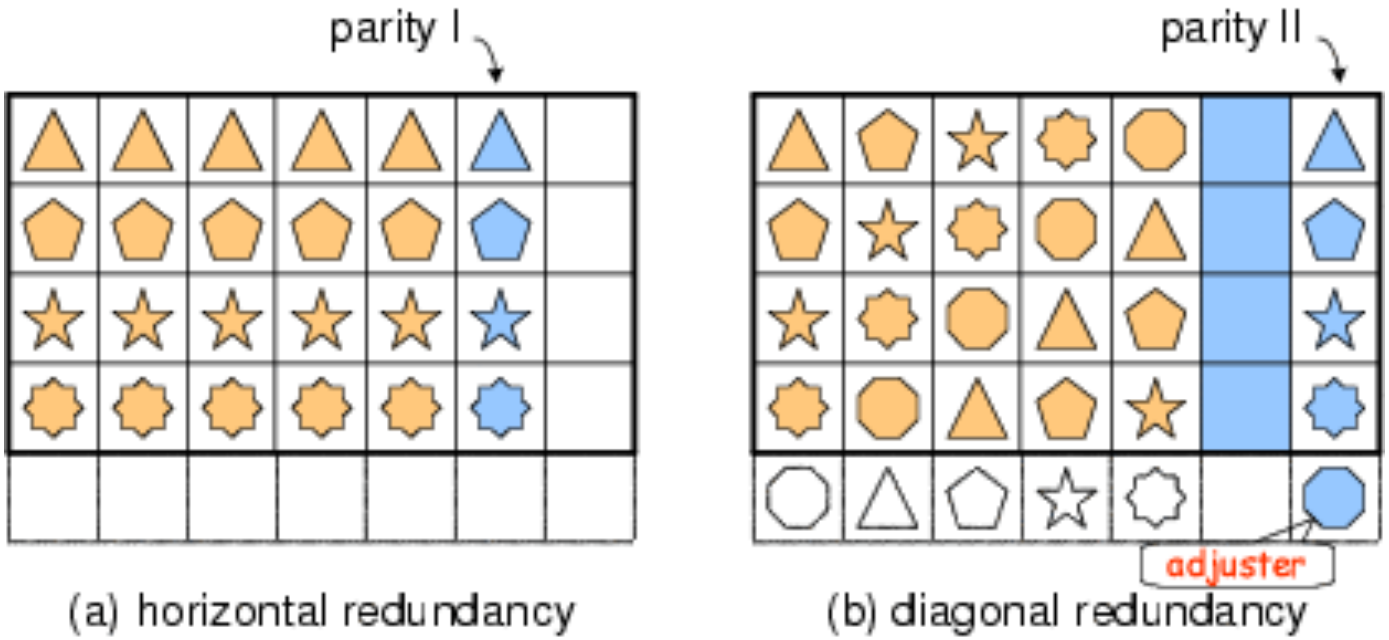
Array Codes

- Mainly used for data storae system
- example array codes
  - Blaum, et al: EVENODD (2 disk faults)
  - Blaum, et al: extended EVENODD (3 disk faults).
  - $[2k, k, d]$ chain code
  - Simple Product Code (SPC)
  - Row-Diagonal Parity (RDP)
  - Blaum $RDP(p, i)$ for $i \leq 8$

Array Codes

- Mainly used for data storae system
- example array codes
  - Blaum, et al: EVENODD (2 disk faults)
  - Blaum, et al: extended EVENODD (3 disk faults).
  - $[2k, k, d]$ chain code
  - Simple Product Code (SPC)
  - Row-Diagonal Parity (RDP)
  - Blaum $RDP(p, i)$ for $i \leq 8$

Sample EVENODD code



(a) horizontal redundancy

(b) diagonal redundancy

Array Code Definition

- Message set: $M = \{0, 1\}$ and fixed n, k, t, and b
- Information variables: let $v_1, \cdots, v_{bk}$
- A t-erasure tolerating $[n, k]$ array code is a $b \times n$ matrix

$$\mathbf{C} = [\alpha_{i,j}]_{1 \le i \le b, 1 \le j \le n}$$

- Each $\alpha_{i,j} \in \{0, 1\}$ is XOR of information symbols
- $v_1, \cdots, v_{bk}$ recovered from any $n - t$ columns of the matrix
- For $\alpha_{i,j} = v_{i_1} \oplus \cdots \oplus v_{i_\sigma}$, call v_{i_j} a neighbor of $\alpha_{i,j}$ and σ the degree of $\alpha_{i,j}$.
- A t-erasure tolerating $[n, k]$ $b \times n$ array code $\mathbf{C}$ is said to be maximum distance separable (MDS) if $k = n - t$.

Array Code Definition

- Message set: $M = \{0, 1\}$ and fixed n, k, t, and b
- Information variables: let $v_1, \cdots, v_{bk}$
- A t-erasure tolerating $[n, k]$ array code is a $b \times n$ matrix

$$\mathbf{C} = [\alpha_{i,j}]_{1 \le i \le b, 1 \le j \le n}$$

- Each $\alpha_{i,j} \in \{0, 1\}$ is XOR of information symbols
- $v_1, \cdots, v_{bk}$ recovered from any $n - t$ columns of the matrix
- For $\alpha_{i,j} = v_{i_1} \oplus \cdots \oplus v_{i_\sigma}$, call v_{i_j} a neighbor of $\alpha_{i,j}$ and σ the degree of $\alpha_{i,j}$.
- A t-erasure tolerating $[n, k]$ $b \times n$ array code $\mathbf{C}$ is said to be maximum distance separable (MDS) if $k = n - t$.

Array Code Definition

- Message set: $M = \{0, 1\}$ and fixed n, k, t, and b
- Information variables: let $v_1, \cdots, v_{bk}$
- A t-erasure tolerating $[n, k]$ array code is a $b \times n$ matrix

$$\mathbf{C} = [\alpha_{i,j}]_{1 \le i \le b, 1 \le j \le n}$$

- Each $\alpha_{i,j} \in \{0, 1\}$ is XOR of information symbols
- $v_1, \cdots, v_{bk}$ recovered from any $n - t$ columns of the matrix
- For $\alpha_{i,j} = v_{i_1} \oplus \cdots \oplus v_{i_\sigma}$, call v_{i_j} a neighbor of $\alpha_{i,j}$ and σ the degree of $\alpha_{i,j}$.
- A t-erasure tolerating $[n, k]$ $b \times n$ array code $\mathbf{C}$ is said to be maximum distance separable (MDS) if $k = n - t$.

Array Code Definition

- Message set: $M = \{0, 1\}$ and fixed n, k, t, and b
- Information variables: let $v_1, \cdots, v_{bk}$
- A t-erasure tolerating $[n, k]$ array code is a $b \times n$ matrix

$$\mathbf{C} = [\alpha_{i,j}]_{1 \le i \le b, 1 \le j \le n}$$

- Each $\alpha_{i,j} \in \{0, 1\}$ is XOR of information symbols
- $v_1, \cdots, v_{bk}$ recovered from any $n - t$ columns of the matrix
- For $\alpha_{i,j} = v_{i_1} \oplus \cdots \oplus v_{i_\sigma}$, call v_{i_j} a neighbor of $\alpha_{i,j}$ and σ the degree of $\alpha_{i,j}$.
- A t-erasure tolerating $[n, k]$ $b \times n$ array code $\mathbf{C}$ is said to be maximum distance separable (MDS) if $k = n - t$.

Array Code Definition

- Message set: $M = \{0, 1\}$ and fixed n, k, t, and b
- Information variables: let $v_1, \cdots, v_{bk}$
- A t-erasure tolerating $[n, k]$ array code is a $b \times n$ matrix

$$\mathbf{C} = [\alpha_{i,j}]_{1 \le i \le b, 1 \le j \le n}$$

- Each $\alpha_{i,j} \in \{0, 1\}$ is XOR of information symbols
- $v_1, \cdots, v_{bk}$ recovered from any $n - t$ columns of the matrix
- For $\alpha_{i,j} = v_{i_1} \oplus \cdots \oplus v_{i_\sigma}$, call v_{i_j} a neighbor of $\alpha_{i,j}$ and σ the degree of $\alpha_{i,j}$.
- A t-erasure tolerating $[n, k]$ $b \times n$ array code $\mathbf{C}$ is said to be maximum distance separable (MDS) if $k = n - t$.

Array Code Definition

- Message set: $M = \{0, 1\}$ and fixed n, k, t, and b
- Information variables: let $v_1, \cdots, v_{bk}$
- A t-erasure tolerating $[n, k]$ array code is a $b \times n$ matrix

$$\mathbf{C} = [\alpha_{i,j}]_{1 \le i \le b, 1 \le j \le n}$$

- Each $\alpha_{i,j} \in \{0, 1\}$ is XOR of information symbols
- $v_1, \cdots, v_{bk}$ recovered from any $n - t$ columns of the matrix
- For $\alpha_{i,j} = v_{i_1} \oplus \cdots \oplus v_{i_\sigma}$, call v_{i_j} a neighbor of $\alpha_{i,j}$ and σ the degree of $\alpha_{i,j}$.
- A t-erasure tolerating $[n, k]$ $b \times n$ array code $\mathbf{C}$ is said to be maximum distance separable (MDS) if $k = n - t$.

Array Code Definition

- Message set: $M = \{0, 1\}$ and fixed n, k, t, and b
- Information variables: let $v_1, \cdots, v_{bk}$
- A t-erasure tolerating $[n, k]$ array code is a $b \times n$ matrix

$$\mathbf{C} = [\alpha_{i,j}]_{1 \le i \le b, 1 \le j \le n}$$

- Each $\alpha_{i,j} \in \{0, 1\}$ is XOR of information symbols
- $v_1, \cdots, v_{bk}$ recovered from any $n - t$ columns of the matrix
- For $\alpha_{i,j} = v_{i_1} \oplus \cdots \oplus v_{i_\sigma}$, call v_{i_j} a neighbor of $\alpha_{i,j}$ and σ the degree of $\alpha_{i,j}$.
- A t-erasure tolerating $[n, k]$ $b \times n$ array code $\mathbf{C}$ is said to be maximum distance separable (MDS) if $k = n - t$.

Iterative Message Passing (Belief Propagation Decoding)

- Iterative Message Passing (Belief Propagation Decoding)

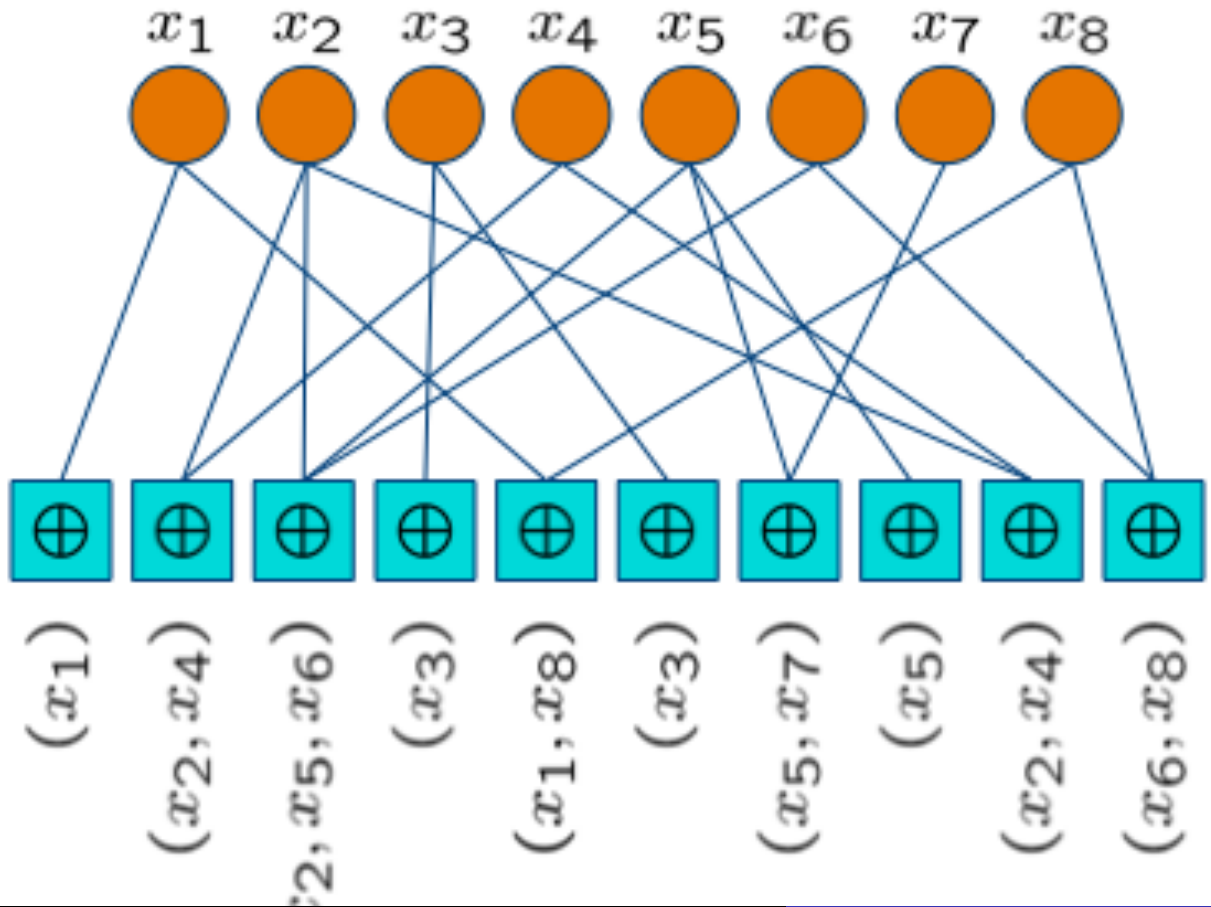
If there is at least one encoding symbol that has exactly one neighbor then the neighbor can be recovered immediately. The value of the recovered information symbol is XORed into any remaining encoding symbols that have this information symbol as a neighbor. The recovered information symbol is removed as a neighbor of these encoding symbols and the degree of each such encoding symbol is decreased by one to reflect this removal.

Iterative Message Passing (Belief Propagation Decoding)

- Iterative Message Passing (Belief Propagation Decoding)

  If there is at least one encoding symbol that has exactly one neighbor then the neighbor can be recovered immediately. The value of the recovered information symbol is XORed into any remaining encoding symbols that have this information symbol as a neighbor. The recovered information symbol is removed as a neighbor of these encoding symbols and the degree of each such encoding symbol is decreased by one to reflect this removal.

Iterative Message Passing (Belief Propagation Decoding)



Array BP-XOR Code

Definition

A t-erasure tolerating $[n,k]$ array code $\mathbf{C} = [\alpha_{i,j}]_{1\leq i\leq b, 1\leq j\leq n}$ is called an $[n,k]$ array BP-XOR code if all information symbols $v_1, \cdots, v_{bk}$ can be recovered from any $n-t$ columns of encoding symbols using the BP-decoding process on the BEC.

Degree 2 Array BP-XOR Code

Theorem

If each encoding symbol in $\mathbf{C} = [\alpha_{i,j}]_{1 \le i \le b, 1 \le j \le n}$ *has degree at most 2, then the restricted array BP-XOR codes are equivalent to edge-colored graphs introduced by Wang and Desmedt for tolerating network homogeneous faults.*

Edge-lolored Graph Definition

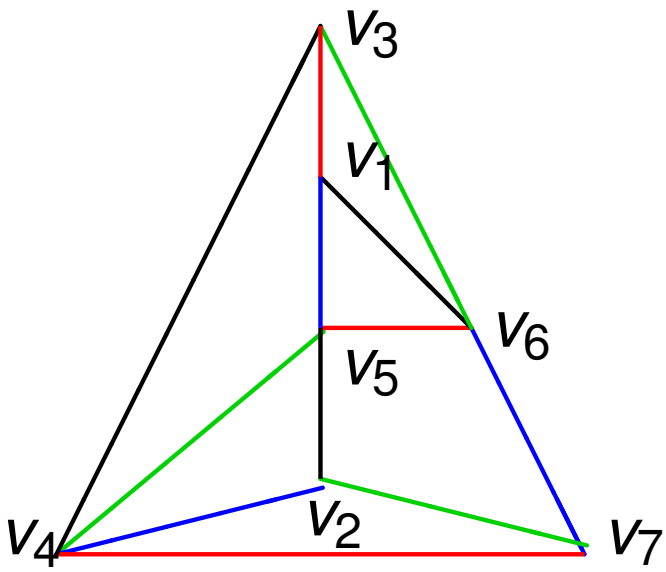
Definition

(Wang and Desmedt) An edge-colored graph is a tuple $G = (V, E, C, f)$, with V the node set, E the edge set, C the color set, and f a map from E onto C. The structure

$$\mathscr{Z}_{C,t} = \{Z : Z \subseteq E \text{ and } |f(Z)| \leq t\}.$$

is called a *t-color* adversary structure. Let $A, B \in V$ be distinct nodes of G. A and B are called $(t+1)$-*color connected* for $t \geq 1$ if for any color set $C_t \subseteq C$ of size t, there is a path p from A to B in G such that the edges on p do not contain any color in C_t. An edge-colored graph G is $(t+1)$-*color connected* if and only if for any two nodes A and B in G, they are $(t+1)$-color connected.

Edge-lolored Graph Example



3-color connected graph $G_{4,2}$ with 7 nodes, 12 edges, and 4 colors. Removal of any two colors in the graph will not disconnect the graph.

black	green	red	blue
$\langle v_1, v_6 \rangle$	$\langle v_2, v_7 \rangle$	$\langle v_3, v_1 \rangle$	$\langle v_4, v_2 \rangle$
$\langle v_2, v_5 \rangle$	$\langle v_3, v_6 \rangle$	$\langle v_4, v_7 \rangle$	$\langle v_5, v_1 \rangle$
$\langle v_3, v_4 \rangle$	$\langle v_4, v_5 \rangle$	$\langle v_5, v_6 \rangle$	$\langle v_6, v_7 \rangle$

Definition

Definition

Let $K_n = (V, E)$ be the complete graph with n nodes. For an even n, a one-factor of K_n is a spanning 1-regular subgraph (or a perfect matching) of K_n. A one-factorization of K_n (n is even) is a set of one-factors that partition the set of edges E. A one-factorization is called perfect (or P1F) if the union of every two distinct one-factors is a Hamiltonian circuit.

P1F

Perfect one-factorizations for K_{p+1}, K_{2p}, and certain K_{2n} do exist, where p is a prime number. It is conjectured that P1F exist for all K_{2n}.

P1F Example

Example

P1F for K_{p+1}: Let $\langle a \rangle_p = b$ where t $b \equiv a \bmod p$. Let $V = \{v_0, v_1, \cdots, v_p\}$ and for $i = 0, \cdots, p-1$

$$F_i = \{\langle v_i, v_p \rangle\} \cup \{\langle v_{\langle j_1+i \rangle_p}, v_{\langle j_2+i \rangle_p} \rangle : \langle j_1 + j_2 \rangle_p = 0 \text{ and } 0 \leq j_1 \neq j_2 < p\}$$

Then $F_0, F_1, \cdots, F_{p-1}$ is a perfect one factorization of K_{p+1}.

P1F Example

Example

P1F for K_{2p}: Let $V = \{v_0, \cdots, v_{2p-1}\}$. For even i, let

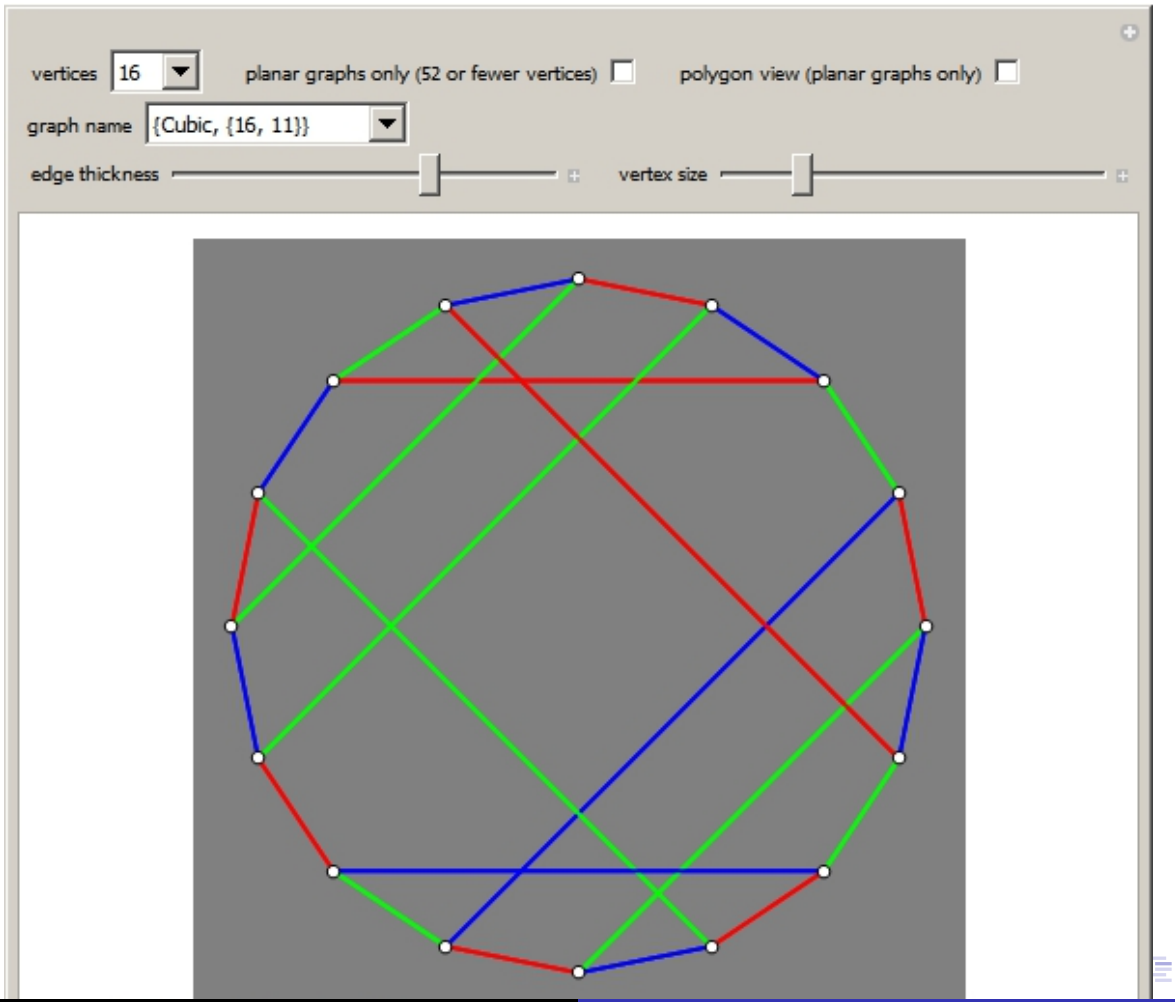
$$F_i = \{\langle v_{j_1}, v_{j_2}\rangle : j_1 + j_2 = i \bmod 2p\} \cup \{\langle v_{\frac{i}{2}}, v_{\frac{i}{2}+p}\rangle\},$$

and for odd $i \neq p$, let

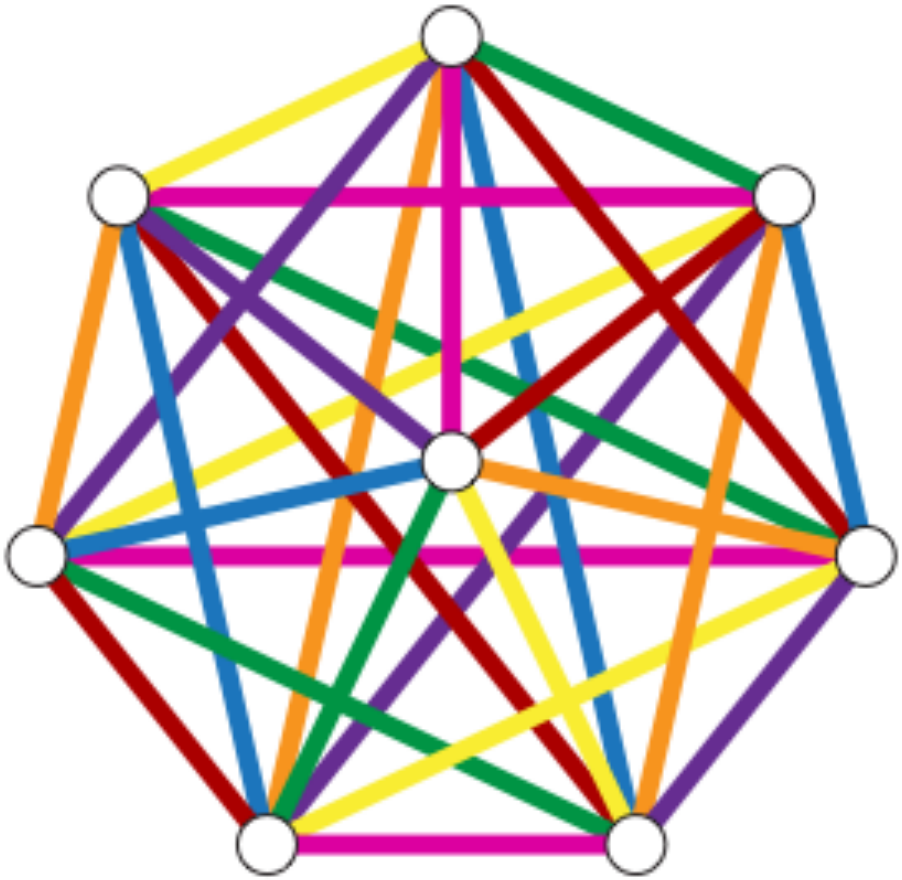
$$F_i = \{\langle v_{j_1}, v_{j_2}\rangle : j_1 \text{ is odd}, j_1 - j_2 = i \bmod 2p\}.$$

Then $F_0, F_1, \cdots, F_{p-1}, F_{p+1}, \cdots, F_{2p-2}$ is a perfect one factorization of K_{2p}.

P1F Example)


vertices
16
planar graphs only (52 or fewer vertices)
polygon view (planar graphs only)
graph name
{Cubic, {16, 11}}
edge thickness
vertex size

P1F of K_8



Edge-colored graphs from P1F

Theorem

Let n be an odd number such that there is a perfect one-factorization $F_1, \cdots, F_n$ for K_{n+1}. For each $t \leq n-2$, there exists a $(t+1)$-color connected edge-colored graph G with n nodes, $(t+2)(n-1)/2$ edges, and $t+2$ colors.

Edge-colored graphs from P1F: Proof

Proof. Let $v_1, \ldots, v_{n+1}$ be a list of nodes for K_{n+1} and $V = \{v_1, \cdots, v_n\}$. Let $F'_i = F_i \setminus \{\langle v_{n+1}, v_j \rangle : j = 1, \cdots, n\}$, $E = F'_1 \cup \cdots \cup F'_{t+2}$, and color all edges in F'_i with the color c_i for $i \leq t+2$. Then it is straightforward to check that the edge-colored graph (V, E) is $(t+1)$-color connected, $|V| = n$, and $|E| = (t+2)(n-1)/2$. □

Edge-colored graphs and array BP-XOR code

Choose a fixed node v_7 and remove all occurrences of v_7 to get the $[4,2]$ 3×4 array BP-XOR code:

black	green	red	blue
$\langle v_1, v_6 \rangle$	$\langle v_2, v_7 \rangle$	$\langle v_3, v_1 \rangle$	$\langle v_4, v_2 \rangle$
$\langle v_2, v_5 \rangle$	$\langle v_3, v_6 \rangle$	$\langle v_4, v_7 \rangle$	$\langle v_5, v_1 \rangle$
$\langle v_3, v_4 \rangle$	$\langle v_4, v_5 \rangle$	$\langle v_5, v_6 \rangle$	$\langle v_6, v_7 \rangle$

$v_1 \oplus v_6$	v_2	$v_3 \oplus v_1$	$v_4 \oplus v_2$
$v_2 \oplus v_5$	$v_3 \oplus v_6$	v_4	$v_5 \oplus v_1$
$v_3 \oplus v_4$	$v_4 \oplus v_5$	$v_5 \oplus v_6$	v_6

Edge-colored graphs and array BP-XOR code

Choose a fixed node v_7 and remove all occurrences of v_7 to get the $[4,2]$ 3×4 array BP-XOR code:

-

black	green	red	blue
$\langle v_1, v_6 \rangle$	$\langle v_2, v_7 \rangle$	$\langle v_3, v_1 \rangle$	$\langle v_4, v_2 \rangle$
$\langle v_2, v_5 \rangle$	$\langle v_3, v_6 \rangle$	$\langle v_4, v_7 \rangle$	$\langle v_5, v_1 \rangle$
$\langle v_3, v_4 \rangle$	$\langle v_4, v_5 \rangle$	$\langle v_5, v_6 \rangle$	$\langle v_6, v_7 \rangle$

-

$v_1 \oplus v_6$	v_2	$v_3 \oplus v_1$	$v_4 \oplus v_2$
$v_2 \oplus v_5$	$v_3 \oplus v_6$	v_4	$v_5 \oplus v_1$
$v_3 \oplus v_4$	$v_4 \oplus v_5$	$v_5 \oplus v_6$	v_6

Edge-colored graphs from array BP-XOR code

$G=(V,E,C,f)$ be a $(t+1)$-color connected edge-colored graph with $V=\{v_1,\cdots,v_{bk},v_{bk+1}\}$ and $C=\{c_1,c_2,\cdots,c_n\}$ and $b=\max_{c\in C}\{|Z|:Z\subseteq E,f(Z)=c\}$.

1. For $1\leq i\leq n$, let β_i be defined as

$$\begin{aligned}\beta_i = \quad & \{v_{j_1}\oplus v_{j_2}:\langle v_{j_1},v_{j_2}\rangle\in E, f(\langle v_{j_1},v_{j_2}\rangle)=c_i,\\ & \text{and } j_1,j_2\neq bk+1\}\cup\\ & \{v_j:\langle v_j,v_{bk+1}\rangle\in E, f(\langle v_j,v_{bk+1}\rangle)=c_i\}\end{aligned}$$

2. If $|\beta_i|$ is smaller than b, duplicate elements in β_i to make it a b-element set.
3. The array BP-XOR code is specified by the $b\times n$ matrix $\mathbf{C}_G=(\beta_1^T,\cdots,\beta_n^T)$.

Edge-colored graphs from array BP-XOR code

$G=(V,E,C,f)$ be a $(t+1)$-color connected edge-colored graph with $V=\{v_1,\cdots,v_{bk},v_{bk+1}\}$ and $C=\{c_1,c_2,\cdots,c_n\}$ and $b=\max_{c\in C}\{|Z|:Z\subseteq E,f(Z)=c\}$.

1. For $1\leq i\leq n$, let β_i be defined as

$$\begin{aligned}\beta_i = \quad & \{v_{j_1}\oplus v_{j_2}:\langle v_{j_1},v_{j_2}\rangle\in E, f(\langle v_{j_1},v_{j_2}\rangle)=c_i,\\ & \text{and } j_1,j_2\neq bk+1\}\cup\\ & \{v_j:\langle v_j,v_{bk+1}\rangle\in E, f(\langle v_j,v_{bk+1}\rangle)=c_i\}\end{aligned}$$

2. If $|\beta_i|$ is smaller than b, duplicate elements in β_i to make it a b-element set.
3. The array BP-XOR code is specified by the $b\times n$ matrix $\mathbf{C}_G=(\beta_1^T,\cdots,\beta_n^T)$.

Edge-colored graphs from array BP-XOR code

$G=(V,E,C,f)$ be a $(t+1)$-color connected edge-colored graph with $V=\{v_1,\cdots,v_{bk},v_{bk+1}\}$ and $C=\{c_1,c_2,\cdots,c_n\}$ and $b=\max_{c\in C}\{|Z|:Z\subseteq E,f(Z)=c\}$.

1. For $1\leq i\leq n$, let β_i be defined as

$$\begin{aligned}\beta_i = \quad & \{v_{j_1}\oplus v_{j_2}:\langle v_{j_1},v_{j_2}\rangle\in E, f(\langle v_{j_1},v_{j_2}\rangle)=c_i,\\ & \text{and } j_1,j_2\neq bk+1\}\cup\\ & \{v_j:\langle v_j,v_{bk+1}\rangle\in E, f(\langle v_j,v_{bk+1}\rangle)=c_i\}\end{aligned}$$

2. If $|\beta_i|$ is smaller than b, duplicate elements in β_i to make it a b-element set.
3. The array BP-XOR code is specified by the $b\times n$ matrix $\mathbf{C}_G=(\beta_1^T,\cdots,\beta_n^T)$.

Array BP-XOR codes from edge-colored graphs

Theorem

Let $\mathbf{C}$ *be an* $b \times n$ *array BP-XOR code with the following properties:*

1. $\mathbf{C}$ *is* t*-erasure tolerating;*
2. $\mathbf{C}$ *contains* bk *information symbols; and*
3. $\mathbf{C}$ *contains only degree one and two encoding symbols.*

Then there exists a $(t+1)$*-color connected edge-colored graph* $G = (V, E, C, f)$ *with* $|V| = bk+1$, $|E| = bn$, *and* $|C| = n$.

Array BP-XOR codes from edge-colored graphs

Theorem

Let $\mathbf{C}$ *be an* $b \times n$ *array BP-XOR code with the following properties:*

1. $\mathbf{C}$ *is* t*-erasure tolerating;*
2. $\mathbf{C}$ *contains* bk *information symbols; and*
3. $\mathbf{C}$ *contains only degree one and two encoding symbols.*

Then there exists a $(t+1)$*-color connected edge-colored graph* $G = (V, E, C, f)$ *with* $|V| = bk+1$, $|E| = bn$, *and* $|C| = n$.

Array BP-XOR codes from edge-colored graphs

Theorem

Let $\mathbf{C}$ *be an* $b \times n$ *array BP-XOR code with the following properties:*

1. $\mathbf{C}$ *is* t*-erasure tolerating;*
2. $\mathbf{C}$ *contains* bk *information symbols; and*
3. $\mathbf{C}$ *contains only degree one and two encoding symbols.*

Then there exists a $(t+1)$*-color connected edge-colored graph* $G = (V, E, C, f)$ *with* $|V| = bk+1$, $|E| = bn$, *and* $|C| = n$.

Array BP-XOR codes from edge-colored graphs

Theorem

Let $\mathbf{C}$ *be an* $b \times n$ *array BP-XOR code with the following properties:*

1. $\mathbf{C}$ *is* t*-erasure tolerating;*
2. $\mathbf{C}$ *contains* bk *information symbols; and*
3. $\mathbf{C}$ *contains only degree one and two encoding symbols.*

Then there exists a $(t+1)$*-color connected edge-colored graph* $G = (V, E, C, f)$ *with* $|V| = bk+1$, $|E| = bn$, *and* $|C| = n$.

MDS $[n,2]$ array BP-XOR codes

First find the smallest p (or $2p$) such that $n \leq p$ (or $n \leq 2p-1$), where p is an odd prime. Using P1F of K_{p+1} to construct the edge-colored graphs and then design the following array BP-XOR code

$v_1 \oplus v_{p-1}$	$\cdots$	$v_{p-1} \oplus v_{p-3}$	v_{p-2}
$v_2 \oplus v_{p-2}$	$\cdots$	v_{p-4}	$v_1 \oplus v_{p-3}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$v_b \oplus v_{b+1}$	$\cdots$	$v_{b-2} \oplus v_{b-1}$	$v_{b-1} \oplus v_b$

SSS

- As an example, design SSS based on the previous codes $\mathscr{C}_{b,n,2}$.
- Let secret data file

$$F = v_1 \oplus v_{p-1} || v_2 \oplus v_{p-2} || \cdots || v_b \oplus v_{b+1}$$

where $v_i \in \{0,1\}^l$.

- Now assume that the first bit of F is flipped. This is equivalent to flipping the first bit of v_{p-1}. Thus the data owner only needs to inform each server to flip one bit at certain location without leaking any other information.
- Other remote computation is possible also (e.g., remote search or database query)

SSS

- As an example, design SSS based on the previous codes $\mathscr{C}_{b,n,2}$.
- Let secret data file

$$F = v_1 \oplus v_{p-1} || v_2 \oplus v_{p-2} || \cdots || v_b \oplus v_{b+1}$$

where $v_i \in \{0,1\}^l$.

- Now assume that the first bit of F is flipped. This is equivalent to flipping the first bit of v_{p-1}. Thus the data owner only needs to inform each server to flip one bit at certain location without leaking any other information.
- Other remote computation is possible also (e.g., remote search or database query)

SSS

- As an example, design SSS based on the previous codes $\mathscr{C}_{b,n,2}$.
- Let secret data file

$$F = v_1 \oplus v_{p-1} || v_2 \oplus v_{p-2} || \cdots || v_b \oplus v_{b+1}$$

  where $v_i \in \{0,1\}^l$.
- Now assume that the first bit of F is flipped. This is equivalent to flipping the first bit of v_{p-1}. Thus the data owner only needs to inform each server to flip one bit at certain location without leaking any other information.
- Other remote computation is possible also (e.g., remote search or database query)

SSS

- As an example, design SSS based on the previous codes $\mathscr{C}_{b,n,2}$.
- Let secret data file

$$F = v_1 \oplus v_{p-1} || v_2 \oplus v_{p-2} || \cdots || v_b \oplus v_{b+1}$$

where $v_i \in \{0,1\}^l$.

- Now assume that the first bit of F is flipped. This is equivalent to flipping the first bit of v_{p-1}. Thus the data owner only needs to inform each server to flip one bit at certain location without leaking any other information.
- Other remote computation is possible also (e.g., remote search or database query)

Flat BP-XOR codes

A $b \times n$ array BP-XOR code is called a flat BP-XOR code if $b = 1$. Furthermore, a $1 \times n$ BP-XOR code with k information symbols and distance d is called an $[n, k, d]$ BP-XOR code.

Fact

Let $n \geq k+2$, $k \geq 2$, and $d = n-k+1$. Then there is no flat $[n, k, d]$ BP-XOR code.

Tolerating one erasure fault

Let $\alpha \in \{1\}^k$. Then the generator matrix $\left[I_k | \alpha^T\right]$ corresponds to an MDS flat $[k+1, k, 2]$ BP-XOR code that could tolerate one erasure fault.

Tolerating two erasure faults

The previous fact shows that two parity check symbols are not sufficient for tolerating two erasure faults for flat BP-XOR codes. In order to tolerate two erasure, we have to consider codes with $n \geq k+3$.

Theorem

For $n \geq k+3$ and $k \geq 3$, there exists a flat $[n,k,3]$ BP-XOR code if and only if $k \leq 2^{n-k} - (n-k) - 1$.

Proof. The truncated version (or non-truncated version if $k = 2^{n-k} - (n-k) - 1$) of the Hamming code could be used to prove the theorem. □

Tolerating three erasure faults

Theorem

For $n \geq k+4$, there exists a systematic flat XOR $[n,k,4]$ code if and only if

$$k \leq \begin{cases} 2^{n-k-1} - n + k & \text{if } n-k \text{ is even} \\ 2^{n-k-1} - n + k - 1 & \text{if } n-k \text{ is odd} \end{cases}$$

Tolerating three erasure faults

Proof. Let

$$X = \{\beta : \beta \in \{0,1\}^{n-k}, wt(\beta) = 3,5,7,\cdots\}.$$

Then

$$\begin{aligned} |X| &= \sum_{i\geq 3, i \text{ is odd}} \binom{n-k}{i} \\ &= \sum_{i\geq 3, i \text{ is odd}} \left(\binom{n-k-1}{i-1} + \binom{n-k-1}{i}\right) \\ &= \begin{cases} 2^{n-k-1} - n + k & \text{if } n-k \text{ is even} \\ 2^{n-k-1} - n + k - 1 & \text{if } n-k \text{ is odd} \end{cases} \end{aligned}$$

Define an $(n-k)\times k$ matrix $A = (\beta_1^T, \cdots, \beta_k^T)$ where β_i are distinct elements from X

Tolerating four or more erasure faults

Theorem

For $n \geq k+5$, there exists a systematic flat XOR $[n,k,5]$ code if k is less than

$$\left\lfloor \frac{n-k-2}{2} \right\rfloor + 2\left\lfloor \left(\left\lceil \frac{n-k}{2} \right\rceil - 2 \right) /2 \right\rfloor + 2\left\lfloor \left(\left\lceil \frac{n-k}{4} \right\rceil - 2 \right) /2 \right\rfloor .$$

Q&A

Q&A?