Improved Private Information Retrieval Rate for Noncolluding Coded Distributed Storage

Hsuan-Yin Lin

Simula UiB, Bergen, Norway

Joint work with S. Kumar, E. Rosnes, and A. Graell i Amat

Joint Estonian-Latvian Theory Days 2022

May 08, 2022

Key ingredient in BigData and IoT: Distributed Storage

- Distributed storage using coding techniques:[1]
  - data is encoded by an $[n, k]$ linear code, and then distributed and stored across n storage servers

[1] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. S. Suh, "A survey on network codes for distributed storage," Proc. IEEE, vol. 99, no. 3, pp. 476–489, Mar. 2011.

Key ingredient in BigData and IoT: Distributed Storage

- Distributed storage using coding techniques:[1]
  - data is encoded by an $[n, k]$ linear code, and then distributed and stored across n storage servers

  $\Rightarrow$ a coded distributed storage systems (DSSs)

[1] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. S. Suh, "A survey on network codes for distributed storage," Proc. IEEE, vol. 99, no. 3, pp. 476–489, Mar. 2011.

Key ingredient in BigData and IoT: Distributed Storage

- Distributed storage using coding techniques:[1]
  - data is encoded by an $[n, k]$ linear code, and then distributed and stored across n storage servers

  $\Rightarrow$ a coded distributed storage systems (DSSs)

- Coded DSSs can be made reliable, robust, efficient, and secure[2]

[1] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. S. Suh, "A survey on network codes for distributed storage," Proc. IEEE, vol. 99, no. 3, pp. 476–489, Mar. 2011.
[2] A. S. Rawat, O. O. Koyluoglu, N. Silberstein, and S. Vishwanath, "Optimal locally repairable and secure codes for distributed storage systems," IEEE Trans. Inf. Theory, vol. 60, no. 1, pp. 212–236, Jan. 2014.

Key ingredient in BigData and IoT: Distributed Storage

- Distributed storage using coding techniques:[1]
  - data is encoded by an $[n, k]$ linear code, and then distributed and stored across n storage servers

  $\Rightarrow$ a coded distributed storage systems (DSSs)

- Coded DSSs can be made reliable, robust, efficient, and secure[2]
  - E.g., locally repairable codes (LRCs)

[1] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. S. Suh, "A survey on network codes for distributed storage," Proc. IEEE, vol. 99, no. 3, pp. 476–489, Mar. 2011.

[2] A. S. Rawat, O. O. Koyluoglu, N. Silberstein, and S. Vishwanath, "Optimal locally repairable and secure codes for distributed storage systems," IEEE Trans. Inf. Theory, vol. 60, no. 1, pp. 212–236, Jan. 2014.

Coded Data in DSSs

Data consists of M files, file index $m \in \{1, \ldots, M\} \triangleq [1 : M]$, and each file $\mathbf{X}^{(m)}$ has size/length β (file size or subpacketization)

Coded Data in DSSs

$$\mathbf{X}^{(m)}: \ \beta = \beta' k$$

$$\beta' \left\{ \underbrace{\begin{array}{|c|c|c|c|} \hline X_{1,1}^{(m)} & X_{1,2}^{(m)} & \cdots & X_{1,k}^{(m)} \\ \hline X_{2,1}^{(m)} & X_{2,2}^{(m)} & \cdots & X_{2,k}^{(m)} \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline X_{\beta',1}^{(m)} & X_{\beta',2}^{(m)} & \cdots & X_{\beta',k}^{(m)} \\ \hline \end{array}}_{k} \right.$$

Coded Data in DSSs

$\mathbf{X}^{(m)}: \ \beta = \beta' k$

$$\beta' \left\{ \underbrace{\begin{array}{|c|c|c|c|}
\hline
X^{(m)}_{1,1} & X^{(m)}_{1,2} & \cdots & X^{(m)}_{1,k} \\
\hline
X^{(m)}_{2,1} & X^{(m)}_{2,2} & \cdots & X^{(m)}_{2,k} \\
\hline
\vdots & \vdots & \cdots & \vdots \\
\hline
X^{(m)}_{\beta',1} & X^{(m)}_{\beta',2} & \cdots & X^{(m)}_{\beta',k} \\
\hline
\end{array}}_{k} \right.$$

a linear $[n, k]$ storage code $\mathscr{C}$

$C^{(m)}: \beta = \beta' \times n$

$$\begin{array}{|c|c|c|c|}
\hline
C^{(m)}_{1,1} & C^{(m)}_{1,2} & \cdots & C^{(m)}_{1,n} \\
\hline
C^{(m)}_{2,1} & C^{(m)}_{2,2} & \cdots & C^{(m)}_{2,n} \\
\hline
\vdots & \vdots & \cdots & \vdots \\
\hline
C^{(m)}_{\beta',1} & C^{(m)}_{\beta',2} & \cdots & C^{(m)}_{\beta',n} \\
\hline
\end{array}$$

coded data

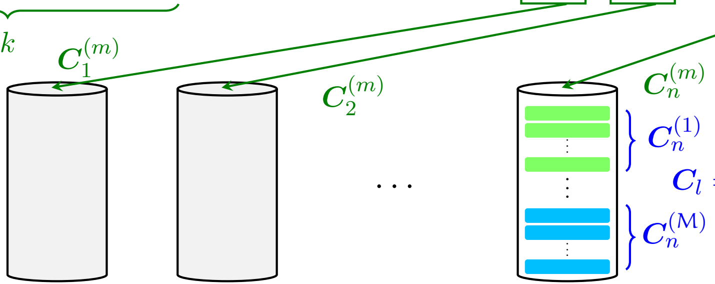
Coded Data in DSSs

$\mathbf{X}^{(m)}: \ \beta = \beta' k$

$$\beta' \left\{ \underbrace{\begin{array}{|c|c|c|c|} \hline X_{1,1}^{(m)} & X_{1,2}^{(m)} & \cdots & X_{1,k}^{(m)} \\ \hline X_{2,1}^{(m)} & X_{2,2}^{(m)} & \cdots & X_{2,k}^{(m)} \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline X_{\beta',1}^{(m)} & X_{\beta',2}^{(m)} & \cdots & X_{\beta',k}^{(m)} \\ \hline \end{array}}_{k} \right.$$

$C^{(m)}: \beta = \beta' \times n$

$$\begin{array}{|c|c|c|c|} \hline C_{1,1}^{(m)} & C_{1,2}^{(m)} & \cdots & C_{1,n}^{(m)} \\ \hline C_{2,1}^{(m)} & C_{2,2}^{(m)} & \cdots & C_{2,n}^{(m)} \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline C_{\beta',1}^{(m)} & C_{\beta',2}^{(m)} & \cdots & C_{\beta',n}^{(m)} \\ \hline \end{array}$$



$$C_l \triangleq \begin{pmatrix} C_l^{(1)} \\ \vdots \\ C_l^{(M)} \end{pmatrix}$$

Coded Data in DSSs

- Replicated data:
  - using an $[n, 1]$ repetition code to encode the data
  - each server stores all the files: high storage overhead!

Coded Data in DSSs

- Replicated data:
  - using an $[n, 1]$ repetition code to encode the data
  - each server stores all the files: high storage overhead!
- MDS-coded data:
  - using an $[n, k]$ MDS code to encode the data

Coded Data in DSSs

- Replicated data:
  - using an $[n, 1]$ repetition code to encode the data
  - each server stores all the files: high storage overhead!
- MDS-coded data:
  - using an $[n, k]$ MDS code to encode the data
  - k-out-of-n property: the data can be retrieved from any subset of k servers

Coded Data in DSSs

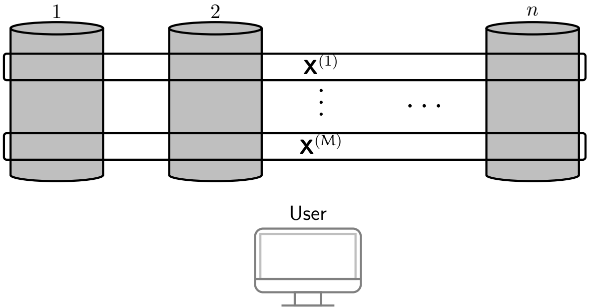
- Replicated data:
  - using an $[n,1]$ repetition code to encode the data
  - each server stores all the files: high storage overhead!
- MDS-coded data:
  - using an $[n,k]$ MDS code to encode the data
  - k-out-of-n property: the data can be retrieved from any subset of k servers
- linear-coded data:
  - using an arbitrary $[n,k]$ linear code to encode the data

Coded Data in DSSs

- Replicated data:
  - using an $[n, 1]$ repetition code to encode the data
  - each server stores all the files: high storage overhead!
- MDS-coded data:
  - using an $[n, k]$ MDS code to encode the data
  - k-out-of-n property: the data can be retrieved from any subset of k servers
- linear-coded data:
  - using an arbitrary $[n, k]$ linear code to encode the data
  - LRCs are (in general) not MDS codes

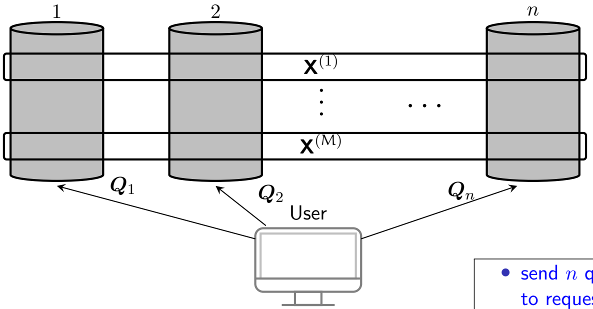
Private Information Retrieval (PIR) for Distributed Storage

- n non-colluding servers: $l \in [1:n]$
- M files: $\mathbf{X}^{(m)}$, $m \in [\mathrm{M}]$
- file size: β symbols



PIR: Upload

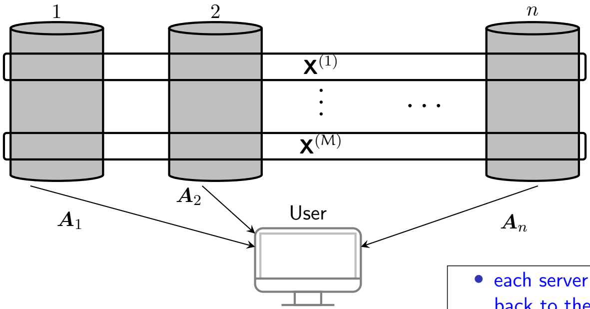
- n non-colluding servers: $l \in [1:n]$
- M files: $\mathbf{X}^{(m)}$, $m \in [\mathrm{M}]$
- file size: β symbols



- send n queries $\boldsymbol{Q}_l$ to request $M \in [\mathrm{M}]$
- M : uniformly distributed

PIR: Download

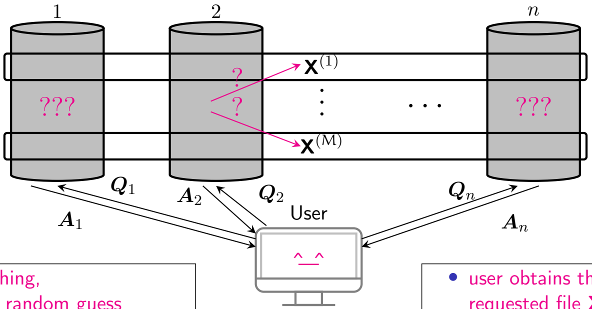
- n non-colluding servers: $l \in [1:n]$
- M files: $\mathbf{X}^{(m)}$, $m \in [\mathrm{M}]$
- file size: β symbols



- each server sends $\boldsymbol{A}_l$ back to the user

Requirements of PIR

- n non-colluding servers: $l \in [1:n]$
- M files: $\mathbf{X}^{(m)}$, $m \in [\mathrm{M}]$
- file size: β symbols

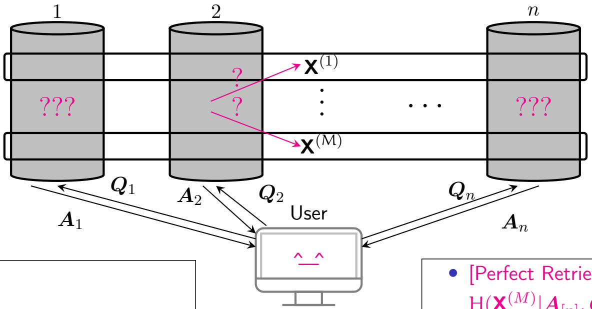


- servers learn nothing, only can make a random guess

- user obtains the complete requested file $\mathbf{X}^{(M)}$

Information-Theoretic PIR

- n non-colluding servers: $l \in [1:n]$
- M files: $\mathbf{X}^{(m)}$, $m \in [\mathrm{M}]$
- file size: β symbols



- [Strong Privacy]
  $M \perp\!\!\!\perp (\boldsymbol{Q}_l, \boldsymbol{A}_l)$

- [Perfect Retrievability]
  $\mathrm{H}(\mathbf{X}^{(M)} | \boldsymbol{A}_{[n]}, \boldsymbol{Q}_{[n]}, M) = 0$

Influential Previous Work

Chor, Goldreich, Kushilevitz, Sudan (1995):

- PIR schemes were firstly studied in the computer science community

Influential Previous Work

Chor, Goldreich, Kushilevitz, Sudan (1995):

- PIR schemes were firstly studied in the computer science community
- PIR for replicated data (2 servers) was proposed
  - in the case of a single server, the solution is to download the entire data

Influential Previous Work

Chor, Goldreich, Kushilevitz, Sudan (1995):

- PIR schemes were firstly studied in the computer science community
- PIR for replicated data (2 servers) was proposed
  - in the case of a single server, the solution is to download the entire data
- The efficiency of a classical PIR scheme is measured by the total amount of communication, i.e., the sum of the upload and download cost

Influential Previous Work

Chan, Ho, Yamamoto (2015):

- Started an information-theoretic re-formulation for PIR schemes in distributed storage systems (DSSs)

Influential Previous Work

Chan, Ho, Yamamoto (2015):

- Started an information-theoretic re-formulation for PIR schemes in distributed storage systems (DSSs)
- Upload cost $\ll$ download cost when the file size is very large

Influential Previous Work

Chan, Ho, Yamamoto (2015):

- Started an information-theoretic re-formulation for PIR schemes in distributed storage systems (DSSs)
- Upload cost $\ll$ download cost when the file size is very large
- Efficiency: PIR rate $\mathrm{R} \equiv \dfrac{\text{file size } (\beta \text{ symbols})}{\text{expected total number of downloaded symbols}}$

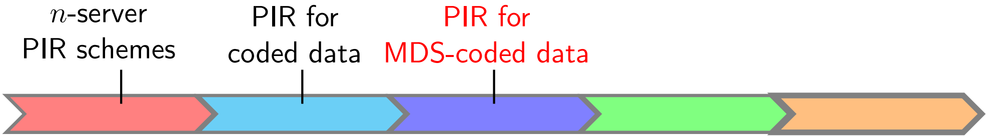
Influential Previous Work

Chan, Ho, Yamamoto (2015):

- Started an information-theoretic re-formulation for PIR schemes in distributed storage systems (DSSs)
- Upload cost $\ll$ download cost when the file size is very large
- Efficiency: PIR rate $\mathsf{R} \equiv \dfrac{\text{file size } (\beta \text{ symbols})}{\text{expected total number of downloaded symbols}}$

only the download cost is considered!!!

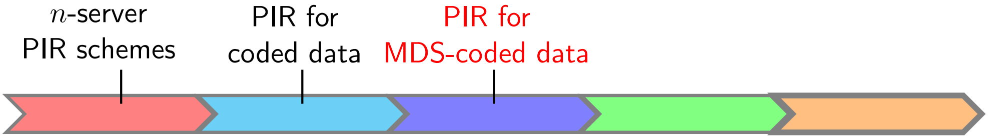
Influential Previous Work



Tajeddine and El Rouayheb (Feb. 2016):

- A practical PIR scheme for DSSs was proposed, where the data is encoded by an $[n, k]$ maximum distance separable (MDS) code $\mathscr{C}_{\text{MDS}}$

Influential Previous Work

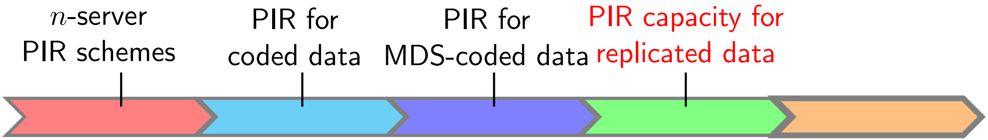


Tajeddine and El Rouayheb (Feb. 2016):

- A practical PIR scheme for DSSs was proposed, where the data is encoded by an $[n, k]$ maximum distance separable (MDS) code $\mathscr{C}_{\text{MDS}}$
- The PIR rate is independent of the number of files: a file-independent scheme

$$\mathrm{R}(\mathscr{C}_{\text{MDS}}) = 1 - \frac{k}{n}$$

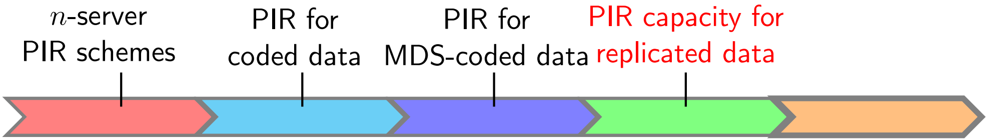
Influential Previous Work



Sun and Jafar (Feb. 2016):

- A Shannon-theoretic re-formulation of PIR
  - the concept of PIR capacity was firstly introduced

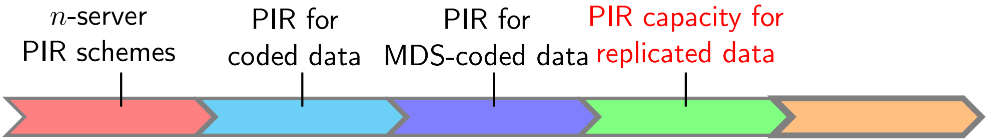
Influential Previous Work



Sun and Jafar (Feb. 2016):

- A Shannon-theoretic re-formulation of PIR
  - the concept of PIR capacity was firstly introduced
- PIR capacity $\mathsf{C} \equiv$ maximum possible PIR rate over all PIR schemes

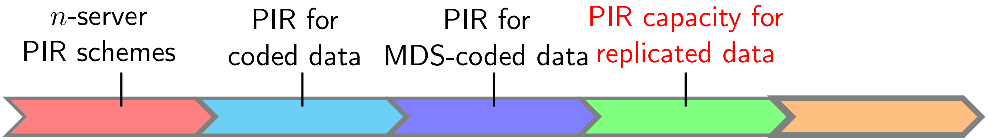
Influential Previous Work



Sun and Jafar (Feb. 2016):

- A Shannon-theoretic re-formulation of PIR
  - the concept of PIR capacity was firstly introduced
- PIR capacity $C \equiv$ maximum possible PIR rate over all PIR schemes
- The PIR capacity for replicated data is achieved by a file-dependent scheme

Influential Previous Work



Sun and Jafar (Feb. 2016):

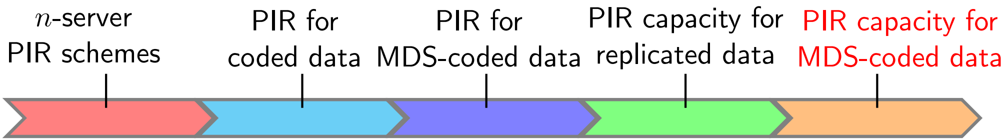
- A Shannon-theoretic re-formulation of PIR
  - the concept of PIR capacity was firstly introduced
- PIR capacity $\mathsf{C} \equiv$ maximum possible PIR rate over all PIR schemes
- The PIR capacity for replicated data is achieved by a file-dependent scheme

$$\mathsf{C}_{\mathrm{M},\mathsf{PIR}} \triangleq \frac{1-\frac{1}{n}}{1-\left(\frac{1}{n}\right)^{\mathrm{M}}}$$

Channel Capacity vs. PIR Capacity

- **Channel capacity.** $P_{\mathsf{e}} \to 0$ as the code blocklength $n \to \infty$
  - Achievability: What is the transmission rate that a coding scheme can achieve (lower bound)?
  - Converse: What is the maximum possible transmission rate that a coding scheme can achieve (upper bound)?
- **PIR capacity.** Ensure privacy and correctness (zero error) as the file size $\beta \to \infty$
  - Achievability: What is the PIR rate that a PIR scheme can achieve (lower bound)?
  - Converse: What is the maximum possible PIR rate that a PIR scheme can achieve (upper bound)?

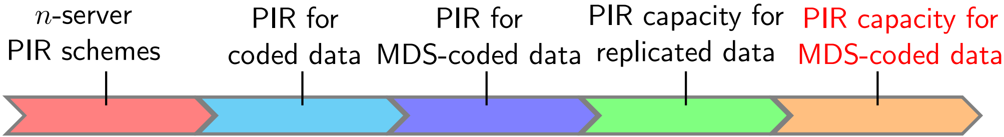
Influential Previous Work



Banawan and Ulukus (Sep. 2016):

- The PIR capacity for an $[n, k]$ MDS-coded data (MDS-PIR capacity) is equal to

Influential Previous Work

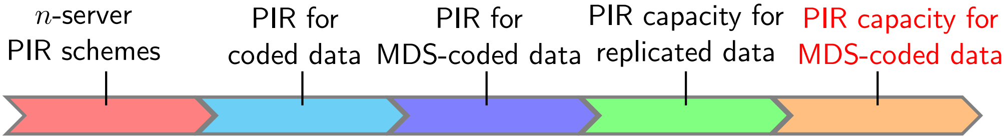


Banawan and Ulukus (Sep. 2016):

- The PIR capacity for an $[n, k]$ MDS-coded data (MDS-PIR capacity) is equal to

$$\mathsf{C}_{\mathsf{M}}^{[n,k]} \triangleq \frac{1-\frac{k}{n}}{1-\left(\frac{k}{n}\right)^{\mathsf{M}}}$$

Influential Previous Work



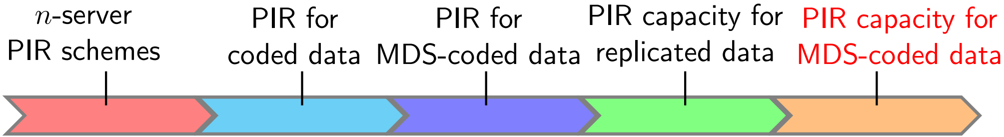
Banawan and Ulukus (Sep. 2016):

- The PIR capacity for an $[n, k]$ MDS-coded data (MDS-PIR capacity) is equal to

$$\mathsf{C}_{\mathrm{M}}^{[n,k]} \triangleq \frac{1-\frac{k}{n}}{1-\left(\frac{k}{n}\right)^{\mathrm{M}}} \searrow \underbrace{1-\frac{k}{n}} \quad \text{as } \mathrm{M} \to \infty$$

PIR rate of the file-independent scheme proposed by Tajeddine and El Rouayheb

Influential Previous Work



Banawan and Ulukus (Sep. 2016):

- The PIR capacity for an $[n, k]$ MDS-coded data (MDS-PIR capacity) is equal to

$$\mathrm{C}_{\mathrm{M}}^{[n,k]} \triangleq \frac{1-\frac{k}{n}}{1-\left(\frac{k}{n}\right)^{\mathrm{M}}} \searrow \underbrace{1-\frac{k}{n}} \quad \text{as } \mathrm{M} \to \infty$$

asymptotic MDS-PIR capacity

PIR rate of the file-independent scheme proposed by Tajeddine and El Rouayheb

A PIR Scheme Using Subpacketization [Shah et al. 2014]: n Servers, $\beta = n-1$

Data is encoded by an $[n,1]$ repetition code with $\beta = n-1$

Server 1	Server 2	$\cdots$	Server n
$\mathbf{X}^{(1)}$	$\mathbf{X}^{(1)}$	$\cdots$	$\mathbf{X}^{(1)}$
$\mathbf{X}^{(2)}$	$\mathbf{X}^{(2)}$	$\cdots$	$\mathbf{X}^{(2)}$
$\vdots$	$\vdots$	$\cdots$	
$\mathbf{X}^{(m)}$	$\mathbf{X}^{(m)}$	$\cdots$	$\mathbf{X}^{(m)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{X}^{(M)}$	$\mathbf{X}^{(M)}$	$\cdots$	$\mathbf{X}^{(M)}$

$\mathbf{X}^{(m)}$: $\beta = (n-1)\cdot 1$

$X^{(m)}_{1,1}$
$X^{(m)}_{2,1}$
$\vdots$
$X^{(m)}_{n-1,1}$

A PIR Scheme Using Subpacketization [Shah et al. 2014]: n Servers, $\beta = n - 1$

- To retrieve $\mathbf{X}^{(m)} = \left[X_{1,1}^{(m)}, \ldots, X_{n-1,1}^{(m)}\right]^{\mathsf{T}}$ of size $n - 1$

A PIR Scheme Using Subpacketization [Shah et al. 2014]: n Servers, $\beta = n-1$

- To retrieve $\mathbf{X}^{(m)} = \bigl[X_{1,1}^{(m)}, \ldots, X_{n-1,1}^{(m)}\bigr]^{\mathsf{T}}$ of size $n-1$
- Pick a random vector $\boldsymbol{U} = \bigl(U_{1,1}, \ldots, U_{1,n-1}, U_{2,1}, \ldots, U_{\mathsf{M},(n-1)}\bigr)$ with i.i.d. entries $\sim \mathsf{Uniform}(\mathsf{GF}(2))$

A PIR Scheme Using Subpacketization [Shah et al. 2014]: n Servers, $\beta = n-1$

- To retrieve $\mathbf{X}^{(m)} = \left[X_{1,1}^{(m)}, \ldots, X_{n-1,1}^{(m)}\right]^{\mathsf{T}}$ of size $n-1$
- Pick a random vector $\boldsymbol{U} = (U_{1,1}, \ldots, U_{1,n-1}, U_{2,1}, \ldots, U_{\mathrm{M},(n-1)})$ with i.i.d. entries $\sim$ Uniform(GF(2))
- Queries: Send $\boldsymbol{U}$ to Server 1, send $\boldsymbol{U} + \boldsymbol{e}_{(m-1)\cdot(n-1)+1}$ to Server 2,..., and send $\boldsymbol{U} + \boldsymbol{e}_{(m-1)\cdot(n-1)+(n-1)}$ to Server n

A PIR Scheme Using Subpacketization [Shah et al. 2014]: n Servers, $\beta = n-1$

- To retrieve $\mathbf{X}^{(m)} = \left[X^{(m)}_{1,1}, \ldots, X^{(m)}_{n-1,1}\right]^\mathsf{T}$ of size $n-1$
- Pick a random vector $\boldsymbol{U} = (U_{1,1}, \ldots, U_{1,n-1}, U_{2,1}, \ldots, U_{\mathsf{M},(n-1)})$ with i.i.d. entries $\sim \text{Uniform}(\text{GF}(2))$
- Queries: Send $\boldsymbol{U}$ to Server 1, send $\boldsymbol{U} + \boldsymbol{e}_{(m-1)\cdot(n-1)+1}$ to Server 2,..., and send $\boldsymbol{U} + \boldsymbol{e}_{(m-1)\cdot(n-1)+(n-1)}$ to Server n
- Answers:

$$\boldsymbol{A}_1 = \sum_{m'=1}^{\mathsf{M}} \sum_{j=1}^{n-1} U_{m',j} X^{(m')}_{j,1}, \qquad \boldsymbol{A}_2 = \sum_{m'=1}^{\mathsf{M}} \sum_{j=1}^{n-1} U_{m',j} X^{(m')}_{j,1} + X^{(m)}_{1,1} \quad \cdots$$

$$\boldsymbol{A}_n = \sum_{m'=1}^{\mathsf{M}} \sum_{j=1}^{n-1} U_{m',j} X^{(m')}_{j,1} + X^{(m)}_{n-1,1}$$

A PIR Scheme Using Subpacketization [Shah et al. 2014]: n Servers, $\beta = n-1$

- To retrieve $\mathbf{X}^{(m)} = \left[X_{1,1}^{(m)}, \ldots, X_{n-1,1}^{(m)}\right]^\mathsf{T}$ of size $n-1$
- Pick a random vector $\boldsymbol{U} = (U_{1,1}, \ldots, U_{1,n-1}, U_{2,1}, \ldots, U_{\mathsf{M},(n-1)})$ with i.i.d. entries $\sim$ Uniform$(\mathsf{GF}(2))$
- Queries: Send $\boldsymbol{U}$ to Server 1, send $\boldsymbol{U} + \boldsymbol{e}_{(m-1)\cdot(n-1)+1}$ to Server 2,..., and send $\boldsymbol{U} + \boldsymbol{e}_{(m-1)\cdot(n-1)+(n-1)}$ to Server n
- Answers:

$$\boldsymbol{A}_1 = \sum_{m'=1}^{\mathsf{M}} \sum_{j=1}^{n-1} U_{m',j} X_{j,1}^{(m')}, \qquad \boldsymbol{A}_2 = \sum_{m'=1}^{\mathsf{M}} \sum_{j=1}^{n-1} U_{m',j} X_{j,1}^{(m')} + X_{1,1}^{(m)} \quad \cdots$$

$$\boldsymbol{A}_n = \sum_{m'=1}^{\mathsf{M}} \sum_{j=1}^{n-1} U_{m',j} X_{j,1}^{(m')} + X_{n-1,1}^{(m)}$$

- Retrievability: $(\boldsymbol{A}_1 + \boldsymbol{A}_2, \boldsymbol{A}_1 + \boldsymbol{A}_3, \ldots, \boldsymbol{A}_1 + \boldsymbol{A}_n) \longrightarrow \mathbf{X}^{(m)}$

A PIR Scheme Using Subpacketization [Shah et al. 2014]: n Servers, $\beta = n-1$

- To retrieve $\mathbf{X}^{(m)} = \left[X_{1,1}^{(m)}, \ldots, X_{n-1,1}^{(m)}\right]^{\mathsf{T}}$ of size $n-1$
- Pick a random vector $\boldsymbol{U} = (U_{1,1}, \ldots, U_{1,n-1}, U_{2,1}, \ldots, U_{\mathsf{M},(n-1)})$ with i.i.d. entries $\sim$ Uniform(GF(2))
- Queries: Send $\boldsymbol{U}$ to Server 1, send $\boldsymbol{U} + \boldsymbol{e}_{(m-1)\cdot(n-1)+1}$ to Server 2,..., and send $\boldsymbol{U} + \boldsymbol{e}_{(m-1)\cdot(n-1)+(n-1)}$ to Server n
- Answers:

$$\boldsymbol{A}_1 = \sum_{m'=1}^{\mathsf{M}} \sum_{j=1}^{n-1} U_{m',j} X_{j,1}^{(m')}, \qquad \boldsymbol{A}_2 = \sum_{m'=1}^{\mathsf{M}} \sum_{j=1}^{n-1} U_{m',j} X_{j,1}^{(m')} + X_{1,1}^{(m)} \quad \cdots$$

$$\boldsymbol{A}_n = \sum_{m'=1}^{\mathsf{M}} \sum_{j=1}^{n-1} U_{m',j} X_{j,1}^{(m')} + X_{n-1,1}^{(m)}$$

- Retrievability: $(\boldsymbol{A}_1 + \boldsymbol{A}_2, \boldsymbol{A}_1 + \boldsymbol{A}_3, \ldots, \boldsymbol{A}_1 + \boldsymbol{A}_n) \longrightarrow \mathbf{X}^{(m)}$
- $\boxed{\mathsf{R} = \frac{(n-1)\cdot 1}{n} = 1 - \frac{1}{n}}$

The PIR Capacity-Achieving Scheme for Replicated Data

- For any given number of files M, none of previously mentioned schemes achieves the maximum possible PIR rate (the PIR capacity)

The PIR Capacity-Achieving Scheme for Replicated Data

- For any given number of files M, none of previously mentioned schemes achieves the maximum possible PIR rate (the PIR capacity)
- Sun and Jafar (2016):
    - after two decades, a breakthrough work that achieves the PIR capacity for replicated data was presented

The PIR Capacity-Achieving Scheme for Replicated Data

- For any given number of files M, none of previously mentioned schemes achieves the maximum possible PIR rate (the PIR capacity)

- Sun and Jafar (2016):

  - after two decades, a breakthrough work that achieves the PIR capacity for replicated data was presented

  - requires a large subpacketization parameter β that is exponential in the number of files M

The PIR Capacity-Achieving Scheme for Replicated Data

- For any given number of files M, none of previously mentioned schemes achieves the maximum possible PIR rate (the PIR capacity)

- Sun and Jafar (2016):
  - after two decades, a breakthrough work that achieves the PIR capacity for replicated data was presented
  - requires a large subpacketization parameter β that is exponential in the number of files M
  - a Shannon-theoretic re-formulation of converse bound is proposed

The PIR Capacity-Achieving Scheme for Replicated Data

- For any given number of files M, none of previously mentioned schemes achieves the maximum possible PIR rate (the PIR capacity)

- Tian, Sun, and Chen (2018):
  - the minimum upload cost of all possible PIR capacity-achieving linear PIR schemes is equal to

$$n(M-1)\log_2 n$$

The PIR Capacity-Achieving Scheme for Replicated Data

- For any given number of files M, none of previously mentioned schemes achieves the maximum possible PIR rate (the PIR capacity)

- Tian, Sun, and Chen (2018):
  - the minimum upload cost of all possible PIR capacity-achieving linear PIR schemes is equal to

$$n(M-1)\log_2 n$$

  - the minimum file size of all possible PIR capacity-achieving linear PIR schemes is equal to $n-1$

The PIR Scheme with Any Number of Files for Coded Data

We propose a PIR scheme for linear-coded data with any number of files:

- It reduces to the PIR capacity-achieving scheme for replicated data, i.e., the Sun-Jafar Scheme, 2016

The PIR Scheme with Any Number of Files for Coded Data

We propose a PIR scheme for linear-coded data with any number of files:

- It reduces to the PIR capacity-achieving scheme for replicated data, i.e., the Sun-Jafar Scheme, 2016
- It reduces to the MDS-PIR capacity-achieving scheme for MDS-coded data, i.e., the Banawan-Ulukus Scheme, 2016

The PIR Scheme with Any Number of Files for Coded Data

We propose a PIR scheme for linear-coded data with any number of files:

- It reduces to the PIR capacity-achieving scheme for replicated data, i.e., the Sun-Jafar Scheme, 2016
- It reduces to the MDS-PIR capacity-achieving scheme for MDS-coded data, i.e., the Banawan-Ulukus Scheme, 2016
- It achieves the MDS-PIR capacity for a particular class of non-MDS storage codes

The PIR Scheme with Any Number of Files for Coded Data

We propose a PIR scheme for linear-coded data with any number of files:

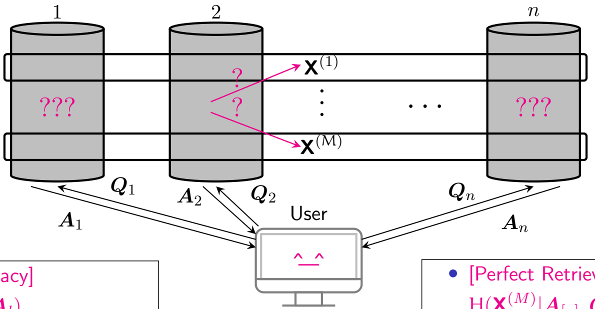
- It reduces to the PIR capacity-achieving scheme for replicated data, i.e., the Sun-Jafar Scheme, 2016
- It reduces to the MDS-PIR capacity-achieving scheme for MDS-coded data, i.e., the Banawan-Ulukus Scheme, 2016
- It achieves the MDS-PIR capacity for a particular class of non-MDS storage codes
    - those codes are referred to as **MDS-PIR capacity-achieving codes**

The PIR Scheme with Any Number of Files for Coded Data

We propose a PIR scheme for linear-coded data with any number of files:

- It reduces to the PIR capacity-achieving scheme for replicated data, i.e., the Sun-Jafar Scheme, 2016
- It reduces to the MDS-PIR capacity-achieving scheme for MDS-coded data, i.e., the Banawan-Ulukus Scheme, 2016
- It achieves the MDS-PIR capacity for a particular class of non-MDS storage codes
  - those codes are referred to as **MDS-PIR capacity-achieving codes**
  - a generalization of the Sun-Jafar scheme and Banawan-Ulukus scheme

Review: Information-Theoretic PIR



- [Strong Privacy]
  $M \perp\!\!\!\perp (\boldsymbol{Q}_l, \boldsymbol{A}_l)$

- [Perfect Retrievability]
  $\mathrm{H}(\mathbf{X}^{(M)} | \boldsymbol{A}_{[n]}, \boldsymbol{Q}_{[n]}, M) = 0$

Retrievability: Use Information Sets

$X^{(m)}: \ \beta = \beta' \times k$

$$\beta' \left\{ \underbrace{\begin{array}{|c|c|c|c|} \hline X^{(m)}_{1,1} & X^{(m)}_{1,2} & \cdots & X^{(m)}_{1,k} \\ \hline X^{(m)}_{2,1} & X^{(m)}_{2,2} & \cdots & X^{(m)}_{2,k} \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline X^{(m)}_{\beta',1} & X^{(m)}_{\beta',2} & \cdots & X^{(m)}_{\beta',k} \\ \hline \end{array}}_{k} \right.$$

$C^{(m)}: \beta = \beta' \times n$

$$\begin{array}{|c|c|c|c|} \hline C^{(m)}_{1,1} & C^{(m)}_{1,2} & \cdots & C^{(m)}_{1,n} \\ \hline C^{(m)}_{2,1} & C^{(m)}_{2,2} & \cdots & C^{(m)}_{2,n} \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline C^{(m)}_{\beta',1} & C^{(m)}_{\beta',2} & \cdots & C^{(m)}_{\beta',n} \\ \hline \end{array}$$

Goal: reconstruct all β' stripes of $X^{(m)}$

Retrievability: Use Information Sets

$X^{(m)} : \beta = \beta' \times k$

$$\beta' \left\{ \underbrace{\begin{array}{|c|c|c|c|} \hline X^{(m)}_{1,1} & X^{(m)}_{1,2} & \cdots & X^{(m)}_{1,k} \\ \hline \boxed{X^{(m)}_{2,1}} & X^{(m)}_{2,2} & \cdots & X^{(m)}_{2,k} \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline X^{(m)}_{\beta',1} & X^{(m)}_{\beta',2} & \cdots & X^{(m)}_{\beta',k} \\ \hline \end{array}}_{k} \right. \xrightarrow{\text{a linear } [n,k] \text{ storage code } \mathscr{C}}$$

$C^{(m)} : \beta = \beta' \times n$

$$\underbrace{\begin{array}{|c|c|c|c|} \hline C^{(m)}_{1,1} & C^{(m)}_{1,2} & \cdots & C^{(m)}_{1,n} \\ \hline C^{(m)}_{2,1} & C^{(m)}_{2,2} & \cdots & C^{(m)}_{2,n} \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline C^{(m)}_{\beta',1} & C^{(m)}_{\beta',2} & \cdots & C^{(m)}_{\beta',n} \\ \hline \end{array}}_{(\mathbf{C}^{(m)}_{i,j_1}, C^{(m)}_{i,j_2}, \ldots, C^{(m)}_{i,j_k})}$$

Goal: reconstruct all β' stripes of $X^{(m)}$

Retrievability: Use Information Sets

$X^{(m)}: \beta = \beta' \times k$

$$\beta' \left\{ \underbrace{\begin{array}{|c|c|c|c|} \hline X^{(m)}_{1,1} & X^{(m)}_{1,2} & \cdots & X^{(m)}_{1,k} \\ \hline \boxed{X^{(m)}_{2,1}} & X^{(m)}_{2,2} & \cdots & X^{(m)}_{2,k} \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline X^{(m)}_{\beta',1} & X^{(m)}_{\beta',2} & \cdots & X^{(m)}_{\beta',k} \\ \hline \end{array}}_{k} \right.$$

a linear $[n, k]$ storage code $\mathscr{C}$

$C^{(m)}: \beta = \beta' \times n$

$$\underbrace{\begin{array}{|c|c|c|c|} \hline C^{(m)}_{1,1} & C^{(m)}_{1,2} & \cdots & C^{(m)}_{1,n} \\ \hline C^{(m)}_{2,1} & C^{(m)}_{2,2} & \cdots & C^{(m)}_{2,n} \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline C^{(m)}_{\beta',1} & C^{(m)}_{\beta',2} & \cdots & C^{(m)}_{\beta',n} \\ \hline \end{array}}_{(\mathbf{C}^{(m)}_{i,j_1}, C^{(m)}_{i,j_2}, \ldots, C^{(m)}_{i,j_k})}$$

recover

Goal: reconstruct all β' stripes of $X^{(m)}$

- **Information set:** a set $\mathcal{I} = \{j_1, \ldots, j_k\} \subseteq [1 : n]$ such that the code symbols $(C_{j_1}, C_{j_2}, \ldots, C_{j_k})$ determine the k information symbols

MDS-PIR Capacity-Achieving Codes

- For any $[n, k]$ code $\mathscr{C}$, one can always find two parameters ν and κ such that
  - **each coordinate $j \in [1:n]$ appears exactly κ times in ν sets $\{\mathcal{S}_i\}_{i=1}^{\nu}$**
  - **each set $\mathcal{S}_i$ contains an inforamtion set of $\mathscr{C}$**

MDS-PIR Capacity-Achieving Codes

- For any $[n, k]$ code $\mathscr{C}$, one can always find two parameters ν and κ such that
  - **each coordinate $j \in [1:n]$ appears exactly κ times in ν sets $\{\mathcal{S}_i\}_{i=1}^{\nu}$**
  - **each set $\mathcal{S}_i$ contains an inforamtion set of $\mathscr{C}$**
- An $[n, k]$ code $\mathscr{C}^*$ (not necessarily be MDS) is called an **MDS-PIR capacity-achieving code** if
  - $\boxed{\exists\, \nu, \kappa \text{ such that } \frac{\kappa}{\nu} = \frac{k}{n}}$

MDS-PIR Capacity-Achieving Codes

- For any $[n,k]$ code $\mathscr{C}$, one can always find two parameters ν and κ such that
  - **each coordinate $j \in [1:n]$ appears exactly κ times in ν sets $\{\mathcal{S}_i\}_{i=1}^{\nu}$**
  - **each set $\mathcal{S}_i$ contains an inforamtion set of $\mathscr{C}$**
- An $[n,k]$ code $\mathscr{C}^*$ (not necessarily be MDS) is called an **MDS-PIR capacity-achieving code** if
  - $\boxed{\exists\, \nu, \kappa \text{ such that } \frac{\kappa}{\nu} = \frac{k}{n}}$
- **Theorem.** The PIR rate $\mathrm{R}(\mathscr{C}^*) = \mathrm{C}_{\mathrm{M}}^{[n,k]}$ is achievable

MDS-PIR Capacity-Achieving Codes

- For any $[n, k]$ code $\mathscr{C}$, one can always find two parameters ν and κ such that
  - **each coordinate $j \in [1:n]$ appears exactly κ times in ν sets $\{\mathcal{S}_i\}_{i=1}^{\nu}$**
  - **each set $\mathcal{S}_i$ contains an inforamtion set of $\mathscr{C}$**
- An $[n, k]$ code $\mathscr{C}^*$ (not necessarily be MDS) is called an **MDS-PIR capacity-achieving code** if
  - $\boxed{\exists\, \nu, \kappa \text{ such that } \frac{\kappa}{\nu} = \frac{k}{n}}$
- **Theorem.** The PIR rate $\mathrm{R}(\mathscr{C}^*) = \mathrm{C}_{\mathrm{M}}^{[n,k]}$ is achievable
- There exist n information sets $\{\mathcal{I}_i\}_{i=1}^{n}$ of $\mathscr{C}_{\mathsf{MDS}}$ such that each coordinate $j \in [1:n]$ appears exactly k times in the collection $\{\mathcal{I}_i\}_{i=1}^{n}$

MDS-PIR Capacity-Achieving Codes

- For any $[n, k]$ code $\mathscr{C}$, one can always find two parameters ν and κ such that
  - **each coordinate $j \in [1:n]$ appears exactly κ times in ν sets $\{\mathcal{S}_i\}_{i=1}^{\nu}$**
  - **each set $\mathcal{S}_i$ contains an inforamtion set of $\mathscr{C}$**
- An $[n, k]$ code $\mathscr{C}^*$ (not necessarily be MDS) is called an **MDS-PIR capacity-achieving code** if
  - $\boxed{\exists\, \nu, \kappa \text{ such that } \frac{\kappa}{\nu} = \frac{k}{n}}$
- **Theorem.** The PIR rate $\mathrm{R}(\mathscr{C}^*) = \mathrm{C}_{\mathrm{M}}^{[n,k]}$ is achievable
- There exist n information sets $\{\mathcal{I}_i\}_{i=1}^{n}$ of $\mathscr{C}_{\mathsf{MDS}}$ such that each coordinate $j \in [1:n]$ appears exactly k times in the collection $\{\mathcal{I}_i\}_{i=1}^{n}$
- $\mathscr{C}_{\mathsf{MDS}} \subset \mathscr{C}^* : (\nu, \kappa) = (n, k)$

MDS-PIR Capacity-Achieving Codes

- **Theorem. The PIR capacity for MDS-PIR capacity-achieving codes is equal to the MDS-PIR capacity $\mathsf{C}_{\mathsf{M}}^{[n,k]}$**

MDS-PIR Capacity-Achieving Codes

- **Theorem. The PIR capacity for MDS-PIR capacity-achieving codes is equal to the MDS-PIR capacity $\mathsf{C}_M^{[n,k]}$**

- The first family of non-MDS codes for which the PIR capacity is known

MDS-PIR Capacity-Achieving Codes

- **Theorem. The PIR capacity for MDS-PIR capacity-achieving codes is equal to the MDS-PIR capacity $\mathsf{C}_{M}^{[n,k]}$**

- The first family of non-MDS codes for which the PIR capacity is known

- Only the PIR capacity of non-MDS-PIR capacity-achieving codes is not yet determined!

Example: An MDS-PIR Capacity-Achieving $[5, 3, 2]$ Code

- Consider a $[5, 3, 2]$ binary non-MDS code $\mathscr{C}$ with generator matrix

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

Example: An MDS-PIR Capacity-Achieving $[5, 3, 2]$ Code

- Consider a $[5, 3, 2]$ binary non-MDS code $\mathscr{C}$ with generator matrix

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

- There exist 5 information sets of $\mathscr{C}$ such that $((\nu, \kappa) = (5, 3))$

information sets	code coordinates				
$\mathcal{S}_1 = \mathcal{I}_1$	1	2	3		
$\mathcal{S}_2 = \mathcal{I}_2$	1			4	5
$\mathcal{S}_3 = \mathcal{I}_3$		2		4	5
$\mathcal{S}_4 = \mathcal{I}_4$		2	3	4	
$\mathcal{S}_5 = \mathcal{I}_5$	1		3		5

Stack

code coordinates				
1	2	3	4	5
1	2	3	4	5
1	2	3	4	5

Example: An MDS-PIR Capacity-Achieving $[5,3,2]$ Code

- Consider a $[5,3,2]$ binary non-MDS code $\mathscr{C}$ with generator matrix

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

- There exist 5 information sets of $\mathscr{C}$ such that $((\nu,\kappa)=(5,3))$

information sets	code coordinates				
$\mathcal{S}_1 = \mathcal{I}_1$	1	2	3		
$\mathcal{S}_2 = \mathcal{I}_2$	1			4	5
$\mathcal{S}_3 = \mathcal{I}_3$		2		4	5
$\mathcal{S}_4 = \mathcal{I}_4$		2	3	4	
$\mathcal{S}_5 = \mathcal{I}_5$	1		3		5

Stack

code coordinates				
1	2	3	4	5
1	2	3	4	5
1	2	3	4	5

$$\frac{\kappa}{\nu} = \frac{k}{n} = \frac{3}{5}$$

Example: A Non-MDS-PIR Capacity-Achieving $[5, 3, 2]$ Code

- Consider a $[5, 3, 2]$ binary non-MDS code $\mathscr{C}'$ with generator matrix

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

Example: A Non-MDS-PIR Capacity-Achieving $[5, 3, 2]$ Code

- Consider a $[5, 3, 2]$ binary non-MDS code $\mathscr{C}'$ with generator matrix

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

- We can only find 3 sets of $\mathscr{C}'$ and each conatins an information set, such that

information sets	sets	code coordinates				
$\mathcal{I}'_1 = \{2, 3, 4\}$	$\mathcal{S}'_1$		2	3	4	5
$\mathcal{I}'_2 = \{1, 4, 5\}$	$\mathcal{S}'_2$	1			4	5
$\mathcal{I}'_3 = \{1, 2, 3\}$	$\mathcal{S}'_3$	1	2	3		

Stack

code coordinates				
1	2	3	4	5
1	2	3	4	5

Example: A Non-MDS-PIR Capacity-Achieving $[5, 3, 2]$ Code

- Consider a $[5, 3, 2]$ binary non-MDS code $\mathscr{C}'$ with generator matrix

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

- We can only find 3 sets of $\mathscr{C}'$ and each conatins an information set, such that

information sets	sets	code coordinates				
$\mathcal{I}'_1 = \{2, 3, 4\}$	$\mathcal{S}'_1$		2	3	4	5
$\mathcal{I}'_2 = \{1, 4, 5\}$	$\mathcal{S}'_2$	1			4	5
$\mathcal{I}'_3 = \{1, 2, 3\}$	$\mathcal{S}'_3$	1	2	3		

Stack $\longrightarrow$

code coordinates				
1	2	3	4	5
1	2	3	4	5

$(\nu, \kappa) = (3, 2)$

Symmetric vs. Asymmetric PIR Protocols

- Consider the binary $[5, 3, 2]$ non-MDS-PIR capacity-achieving code $\mathscr{C}'$
- Define the interference symbols: $I_{h,l} \triangleq \boldsymbol{u}_h^{\mathsf{T}} \boldsymbol{c}_l$, $h \in \mathbb{N}$, $l \in [1 : n]$
- $\boldsymbol{u}$ is a vector of length βM with i.i.d. uniformly distributed components

Symmetric vs. Asymmetric PIR Protocols

- Consider the binary $[5, 3, 2]$ non-MDS-PIR capacity-achieving code $\mathscr{C}'$
- Define the interference symbols: $I_{h,l} \triangleq \boldsymbol{u}_h^\top \boldsymbol{c}_l$, $h \in \mathbb{N}$, $l \in [1 : n]$
- $\boldsymbol{u}$ is a vector of length βM with i.i.d. uniformly distributed components
- **Symmetric Protocol:** $\mathsf{H}(A_1) = \cdots = \mathsf{H}(A_5) = 2$ $\qquad$ $\mathsf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

Responses	Server 1	Server 2	Server 3	Server 4	Server 5
$\mathsf{H}(A_l)$	$I_{1,1} + x_{1,1}^{(m)}$	$I_{1,2}$	$I_{1,3}$	$I_{1,4}$	$I_{1,5}$
	$I_{2,1}$	$I_{2,2} + x_{1,2}^{(m)}$	$I_{2,3} + x_{1,3}^{(m)}$	$I_{2,4}$	$I_{2,5}$

Symmetric vs. Asymmetric PIR Protocols

- Consider the binary $[5,3,2]$ non-MDS-PIR capacity-achieving code $\mathscr{C}'$
- Define the interference symbols: $I_{h,l} \triangleq \boldsymbol{u}_h^\mathsf{T}\boldsymbol{c}_l$, $h \in \mathbb{N}$, $l \in [1:n]$
- $\boldsymbol{u}$ is a vector of length βM with i.i.d. uniformly distributed components
- **Symmetric Protocol:** $\mathsf{H}(A_1) = \cdots = \mathsf{H}(A_5) = 2$ $\qquad \mathsf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

Responses	Server 1	Server 2	Server 3	Server 4	Server 5
$\mathsf{H}(A_l)$	$I_{1,1} + x_{1,1}^{(m)}$	$I_{1,2}$	$I_{1,3}$	$I_{1,4}$	$I_{1,5}$
	$I_{2,1}$	$I_{2,2} + x_{1,2}^{(m)}$	$I_{2,3} + x_{1,3}^{(m)}$	$I_{2,4}$	$I_{2,5}$

- $\mathcal{I}'_1 = \{2,3,4\} \subseteq \mathcal{S}'_1 = \{2,3,4,5\} \Longrightarrow$ obtain $x_{1,1}^{(m)}$

Symmetric vs. Asymmetric PIR Protocols

- Consider the binary $[5, 3, 2]$ non-MDS-PIR capacity-achieving code $\mathscr{C}'$
- Define the interference symbols: $I_{h,l} \triangleq \boldsymbol{u}_h^{\mathsf{T}} \boldsymbol{c}_l$, $h \in \mathbb{N}$, $l \in [1:n]$
- $\boldsymbol{u}$ is a vector of length $\beta \mathrm{M}$ with i.i.d. uniformly distributed components
- **Symmetric Protocol:** $\mathsf{H}(A_1) = \cdots = \mathsf{H}(A_5) = 2$ $\qquad \mathsf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

Responses	Server 1	Server 2	Server 3	Server 4	Server 5
$\mathsf{H}(A_l)$	$I_{1,1} + x_{1,1}^{(m)}$	$I_{1,2}$	$I_{1,3}$	$I_{1,4}$	$I_{1,5}$
	$I_{2,1}$	$I_{2,2} + x_{1,2}^{(m)}$	$I_{2,3} + x_{1,3}^{(m)}$	$I_{2,4}$	$I_{2,5}$

- $\mathcal{S}_2' = \{1, 4, 5\} \Longrightarrow$ obtain $x_{1,2}^{(m)}, x_{1,3}^{(m)}$

Symmetric vs. Asymmetric PIR Protocols

- Consider the binary $[5,3,2]$ non-MDS-PIR capacity-achieving code $\mathscr{C}'$
- Define the interference symbols: $I_{h,l} \triangleq \boldsymbol{u}_h^{\mathsf{T}} \boldsymbol{c}_l$, $h \in \mathbb{N}$, $l \in [1:n]$
- $\boldsymbol{u}$ is a vector of length βM with i.i.d. uniformly distributed components
- **Symmetric Protocol:** $\mathsf{H}(A_1) = \cdots = \mathsf{H}(A_5) = 2$ $\qquad \mathsf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

Responses	Server 1	Server 2	Server 3	Server 4	Server 5
$\mathsf{H}(A_l)$	$I_{1,1} + x_{1,1}^{(m)}$	$I_{1,2}$	$I_{1,3}$	$I_{1,4}$	$I_{1,5}$
	$I_{2,1}$	$I_{2,2} + x_{1,2}^{(m)}$	$I_{2,3} + x_{1,3}^{(m)}$	$I_{2,4}$	$I_{2,5}$

- $\mathcal{S}_3' = \{1,2,3\} \Longrightarrow$ recover the m-th file: $\left[x_{1,1}^{(m)}, x_{1,2}^{(m)}, x_{1,3}^{(m)}\right]$ $(\beta = 1)$

Symmetric vs. Asymmetric PIR Protocols

- Theorem (Symmetric Protocol). The PIR rate

$$\mathrm{R}_{\mathrm{M},\,\mathrm{S}}(\mathscr{C}) = \frac{(\nu-\kappa)k}{\kappa n}\left[1-\left(\frac{\kappa}{\nu}\right)^{\mathrm{M}}\right]^{-1} \quad \text{is achievable}$$

Symmetric vs. Asymmetric PIR Protocols

- Theorem (Symmetric Protocol). The PIR rate

$$\mathsf{R}_{\mathsf{M},\mathsf{S}}(\mathscr{C}) = \frac{(\nu-\kappa)k}{\kappa n}\left[1-\left(\frac{\kappa}{\nu}\right)^{\mathsf{M}}\right]^{-1} \quad \text{is achievable}$$

- Asymmetric: $\mathsf{H}(A_1) = \cdots = \mathsf{H}(A_4) = 2$, but $\mathsf{H}(A_5) = 1$ $\qquad \mathsf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

Protocol A:

Responses	Server 1	Server 2	Server 3	Server 4	Server 5
$\mathsf{H}(A_l)$	$I_{1,1} + x_{1,1}^{(m)}$	$I_{1,2}$	$I_{1,3}$	$I_{1,4}$	$I_{1,5}$
	$I_{2,1}$	$I_{2,2} + x_{1,2}^{(m)}$	$I_{2,3} + x_{1,3}^{(m)}$	$I_{2,4}$	$I_{2,5}$

- $\mathcal{I}_1' = \{2,3,4\} \Longrightarrow$ obtain $x_{1,1}^{(m)}$

Symmetric vs. Asymmetric PIR Protocols

- Theorem (Symmetric Protocol). The PIR rate

$$\mathsf{R}_{\mathsf{M},\,\mathsf{S}}(\mathscr{C}) = \frac{(\nu-\kappa)k}{\kappa n}\left[1-\left(\frac{\kappa}{\nu}\right)^{\mathsf{M}}\right]^{-1} \quad \text{is achievable}$$

- Asymmetric: $\mathsf{H}(A_1) = \cdots = \mathsf{H}(A_4) = 2$, but $\mathsf{H}(A_5) = 1$ $\qquad \mathsf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

Protocol A:

Responses	Server 1	Server 2	Server 3	Server 4	Server 5
$\mathsf{H}(A_l)$	$I_{1,1} + x_{1,1}^{(m)}$	$I_{1,2}$	$I_{1,3}$	$I_{1,4}$	$I_{1,5}$
	$I_{2,1}$	$I_{2,2} + x_{1,2}^{(m)}$	$I_{2,3} + x_{1,3}^{(m)}$	$I_{2,4}$	$I_{2,5}$

- $\mathcal{I}_2' = \{1, 4, 5\} \Longrightarrow$ obtain $x_{1,2}^{(m)}, x_{1,3}^{(m)}$

Symmetric vs. Asymmetric PIR Protocols

- Theorem (Symmetric Protocol). The PIR rate

$$\mathsf{R}_{\mathsf{M},\mathsf{S}}(\mathscr{C}) = \frac{(\nu-\kappa)k}{\kappa n}\left[1-\left(\frac{\kappa}{\nu}\right)^{\mathsf{M}}\right]^{-1} \quad \text{is achievable}$$

- Asymmetric: $\mathsf{H}(A_1) = \cdots = \mathsf{H}(A_4) = 2$, but $\mathsf{H}(A_5) = 1$ $\quad \mathsf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

Protocol A:

Responses	Server 1	Server 2	Server 3	Server 4	Server 5
$\mathsf{H}(A_l)$	$I_{1,1} + x_{1,1}^{(m)}$	$I_{1,2}$	$I_{1,3}$	$I_{1,4}$	$I_{1,5}$
	$I_{2,1}$	$I_{2,2} + x_{1,2}^{(m)}$	$I_{2,3} + x_{1,3}^{(m)}$	$I_{2,4}$	$I_{2,5}$

- $\mathcal{I}_3' = \{1,2,3\} \Longrightarrow$ recover the m-th file: $\left[x_{1,1}^{(m)}, x_{1,2}^{(m)}, x_{1,3}^{(m)}\right]$ $(\beta = 1)$

Asymmetry Helps for Non-MDS-PIR Capacity-Achieving Codes

- **Theorem (Asymmetric Protocol A). The PIR rate**

$$\mathrm{R}_{\mathrm{M},\,\mathrm{A}}(\mathscr{C}) \triangleq \left(1-\frac{\kappa}{\nu}\right)\left[1-\left(\frac{\kappa}{\nu}\right)^{\mathrm{M}}\right]^{-1} \quad \text{is achievable}$$

Asymmetry Helps for Non-MDS-PIR Capacity-Achieving Codes

- **Theorem (Asymmetric Protocol A). The PIR rate**

$$\mathrm{R}_{\mathrm{M,\,A}}(\mathscr{C}) \triangleq \left(1 - \frac{\kappa}{\nu}\right)\left[1 - \left(\frac{\kappa}{\nu}\right)^{\mathrm{M}}\right]^{-1} \quad \text{is achievable}$$

- It can be shown that $\mathrm{R}_{\mathrm{M,\,S}}(\mathscr{C}) < \mathrm{R}_{\mathrm{M,\,A}}(\mathscr{C})$ for any given ν and κ

Asymmetric Protocol for a Special Class of Codes

- Consider the $[5, 3, 2]$ binary non-MDS code $\mathscr{C}'$ with generator matrix

$$\mathsf{G}' = \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Asymmetric Protocol for a Special Class of Codes

- Consider the $[5,3,2]$ binary non-MDS code $\mathscr{C}'$ with generator matrix

$$\mathsf{G}' = \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

- Decompose G' into $\mathsf{G}'_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ and $\mathsf{G}'_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}$:

Protocol A:

Responses	Server 1	Server 2	Server 3	Server 4	Server 5
$\mathsf{H}(A_l)$	$I_{1,1} + x_{1,1}^{(m)}$	$I_{1,2}$	$I_{1,3}$	$I_{1,4}$	$I_{1,5}$
	$I_{2,1}$	$I_{2,2} + x_{1,2}^{(m)}$	$I_{2,3} + x_{1,3}^{(m)}$	$I_{2,4}$	$I_{2,5}$

Asymmetric Protocol for a Special Class of Codes

- Consider the $[5,3,2]$ binary non-MDS code $\mathscr{C}'$ with generator matrix

$$\mathsf{G}' = \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

- Decompose G' into $\mathsf{G}'_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ and $\mathsf{G}'_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}$:

Protocol B:

Responses	Server 1	Server 2	Server 3	Server 4	Server 5
$\mathsf{H}(A_l)$	$I_{1,1} + x_{1,1}^{(m)}$	$I_{1,2}$	$I_{1,3}$	$I_{1,4}$	$I_{1,5}$
	$I_{2,1}$	$I_{2,2} + x_{1,2}^{(m)}$	$I_{2,3} + x_{1,3}^{(m)}$	$I_{2,4}$	$I_{2,5}$

Asymmetric Protocol for a Special Class of Codes

- Consider the $[5,3,2]$ binary non-MDS code $\mathscr{C}'$ with generator matrix

$$\begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \mathsf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

- Decompose G' into $\mathsf{G}'_1 = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ and $\mathsf{G}'_2 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 1 \end{smallmatrix}\right)$:

Protocol B:

Responses	Server 1	Server 2	Server 3	Server 4	Server 5
$\mathsf{H}(A_l)$	$I_{1,1} + x_{1,1}^{(m)}$	$I_{1,2}$	$I_{1,3}$	$I_{1,4}$	$I_{1,5}$
	$I_{2,1}$	$I_{2,2} + x_{1,2}^{(m)}$	$I_{2,3} + x_{1,3}^{(m)}$	$I_{2,4}$	$I_{2,5}$

Asymmetric Protocol for a Special Class of Codes

- If the generator matrix G of a non-MDS-PIR capacity-achieving code $\mathscr{C}_{\mathsf{DS}}$ has the structure $(n = \sum_{p=1}^{\mathsf{P}} n_p, k = \sum_{p=1}^{\mathsf{P}} k_p$, G_p: size $k_p \times n_p)$

$$\mathsf{G} = \begin{pmatrix} \mathsf{G}_1 & & & \\ & \mathsf{G}_2 & & \\ & & \ddots & \\ & & & \mathsf{G}_{\mathsf{P}} \end{pmatrix}, \quad \mathscr{C}^{\mathsf{G}_p} : [n_p, k_p] \text{ MDS-PIR capacity-achieving codes with } \mathsf{G}_p$$

(a direct sum of MDS-PIR capacity-achieving codes)

Asymmetric Protocol for a Special Class of Codes

- If the generator matrix G of a non-MDS-PIR capacity-achieving code $\mathscr{C}_{\mathsf{DS}}$ has the structure $(n = \sum_{p=1}^{\mathsf{P}} n_p, k = \sum_{p=1}^{\mathsf{P}} k_p$, G_p: size $k_p \times n_p)$

$$\mathsf{G} = \begin{pmatrix} \mathsf{G}_1 & & & \\ & \mathsf{G}_2 & & \\ & & \ddots & \\ & & & \mathsf{G}_{\mathsf{P}} \end{pmatrix}, \quad \mathscr{C}^{\mathsf{G}_p} : [n_p, k_p] \text{ MDS-PIR capacity-achieving codes with } \mathsf{G}_p$$

(a direct sum of MDS-PIR capacity-achieving codes)

- **Theorem (Asymmetric Protocol B). The PIR rate**

$$\mathsf{R}_{\mathsf{M},\,\mathsf{B}}(\mathscr{C}_{\mathsf{DS}}) \triangleq \left(\sum_{p=1}^{\mathsf{P}} \frac{k_p}{k} \left(\mathsf{C}_{\mathsf{M}}^{[n_p,k_p]} \right)^{-1} \right)^{-1} \quad \text{is achievable}$$

Asymmetric Protocol for a Special Class of Codes

- If the generator matrix G of a non-MDS-PIR capacity-achieving code $\mathscr{C}_{\mathsf{DS}}$ has the structure $\left(n = \sum_{p=1}^{\mathsf{P}} n_p, k = \sum_{p=1}^{\mathsf{P}} k_p,\ \mathsf{G}_p\text{: size } k_p \times n_p\right)$

$$\mathsf{G} = \begin{pmatrix} \mathsf{G}_1 & & & \\ & \mathsf{G}_2 & & \\ & & \ddots & \\ & & & \mathsf{G}_{\mathsf{P}} \end{pmatrix}, \quad \mathscr{C}^{\mathsf{G}_p} : [n_p, k_p] \text{ MDS-PIR capacity-achieving codes with } \mathsf{G}_p$$

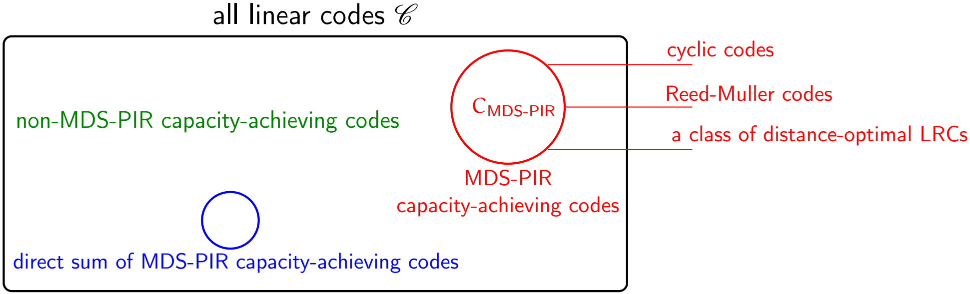
(a direct sum of MDS-PIR capacity-achieving codes)

- **Theorem (Asymmetric Protocol B). The PIR rate**

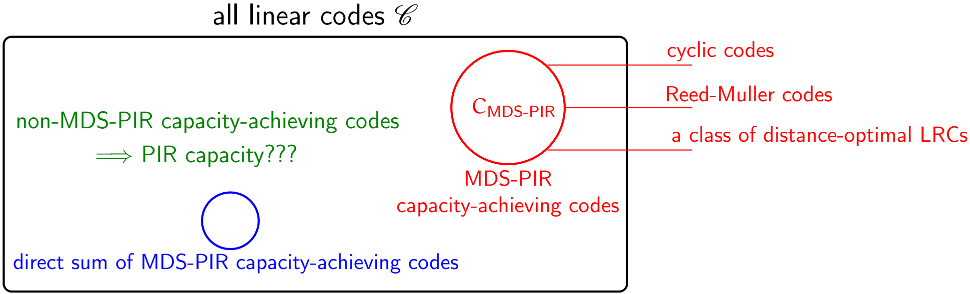
$$\mathsf{R}_{\mathsf{M},\,\mathsf{B}}(\mathscr{C}_{\mathsf{DS}}) \triangleq \left(\sum_{p=1}^{\mathsf{P}} \frac{k_p}{k} \left(\mathsf{C}_{\mathsf{M}}^{[n_p,k_p]}\right)^{-1}\right)^{-1} \quad \text{is achievable}$$

- If such code exists, then one can show that $\mathsf{R}_{\mathsf{M},\,\mathsf{A}}(\mathscr{C}_{\mathsf{DS}}) < \mathsf{R}_{\mathsf{M},\,\mathsf{B}}(\mathscr{C}_{\mathsf{DS}})$

Take Home Messages

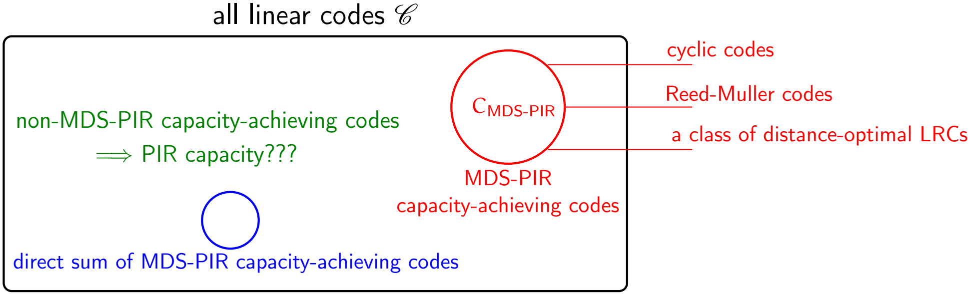


Take Home Messages



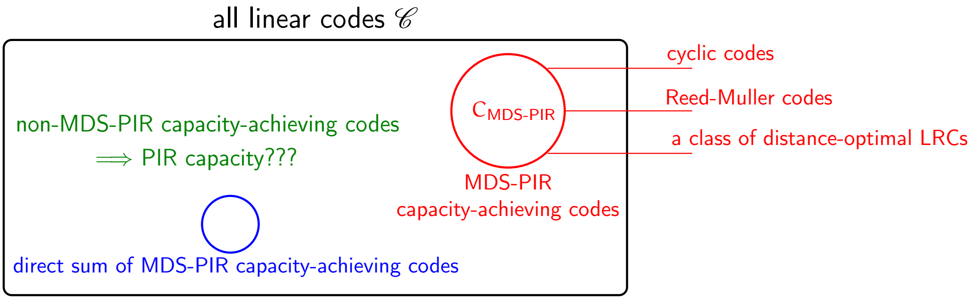
- For codes that cannot be decomposed into a direct sum of MDS-PIR capacity-achieving codes, the PIR capacity is still unknown...
  - a code-dependent, but file-independent asymmetric protocol is also proposed
  - Protocol A could still be improved

Take Home Messages



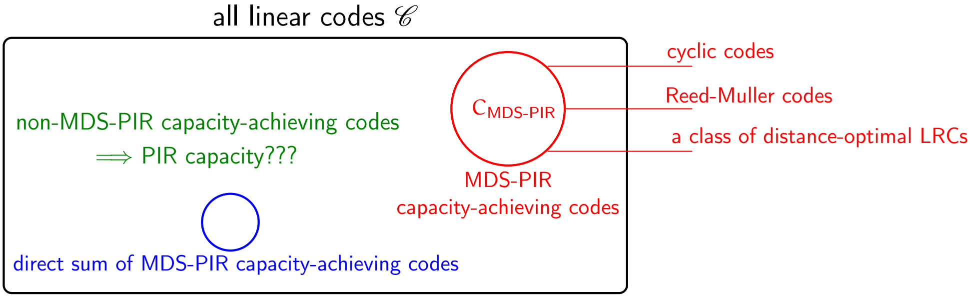
- **Open Problem 1: What is the PIR capacity for non-MDS encoded data?**

Take Home Messages



- **Open Problem 2: Is $\mathrm{C}_{\mathrm{M}}^{[n,k]}$ the limit for any $[n,k]$ linear-coded DSS?**
  - So far, no $[n,k]$ non-MDS-PIR capacity-achieving code gives a strictly larger PIR rate than $\mathrm{C}_{\mathrm{M}}^{[n,k]}$

Take Home Messages



- Asymmetric PIR protocols could be needed for a coded DSS using non-MDS-PIR capacity-achieving codes