

An Achievable Scheme for the K-user Linear Computation Broadcast Channel



Yinbin Ma



Daniela Tuninetti

University of Illinois Chicago

June 23, 2025

Outline

Introduction

Problem Formulation

Subspace Decomposition

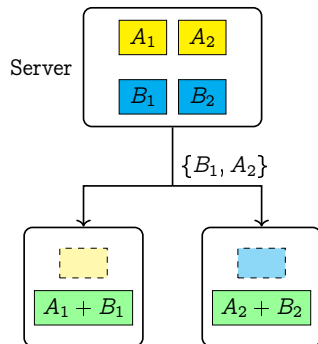
Achievability

Example

Conclusion

What is K-LCBC?

- ▶ A K-LCBC comprises data stored on a server and K users.
- ▶ Each user aims to retrieve a desired linear function of data.
- ▶ Users leverage their prior side information (also a linear function of data) to retrieve their desired information.
- ▶ The server broadcasts a message to the users so as to minimize the communication load.



Motivation & Contributions

- ▶ Motivated by distributed computing (e.g., federated learning), and related to other models in info. theory.
- ▶ Index coding was instrumental to determine the minimal load of the LCBC with uncoded placement.
- ▶ LCBC could potentially be leveraged to derive the ultimate performance limits of coded caching with linear coded placement.

Motivation & Contributions

- ▶ Motivated by distributed computing (e.g., federated learning), and related to other models in info. theory.
- ▶ Index coding was instrumental to determine the minimal load of the LCBC with uncoded placement.
- ▶ LCBC could potentially be leveraged to derive the ultimate performance limits of coded caching with linear coded placement.
- ▶ Prior LCBC works include optimality results for 2 and 3 users, and a ‘generic’ setting with any number of users.
- ▶ We introduce an LP-framework for K-LCBC achievability by multicast and interference elimination.

System Model

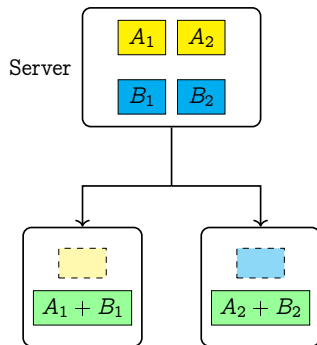
- ▶ Server stores data i.i.d. uniformly at random

$$\mathbf{f}(t) = [f_1(t), \dots, f_d(t)]^T \in \mathbb{F}_q^{d \times 1}.$$

- ▶ Side info. for user k : $\mathbf{w}'_k(t) = \mathbf{f}(t)^T \mathbf{V}'_k \in \mathbb{F}_q^{1 \times m'_k}$.
- ▶ Desired info. for user k : $\mathbf{w}_k(t) = \mathbf{f}(t)^T \mathbf{V}_k \in \mathbb{F}_q^{1 \times m_k}$.
- ▶ WLOG, $\mathbf{V}'_k$ and $\mathbf{V}_k$ are linearly independent.

System Model (Cont.)

$$\begin{aligned}d &= 4, m'_* = 1, m_* = 2, \\f(t) &= [A_1, A_2, B_1, B_2]^T, \\V'_1 &= [1, 0, 1, 0], \\V'_2 &= [0, 1, 0, 1], \\V_1 &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \\V_2 &= \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.\end{aligned}$$



Performance Metric

An achievable $(L, N, \phi, (\varphi_k)_{k \in [K]})$ coding scheme consists of:

- ▶ Server aggregates L instances: $F = [f(1), \dots, f(L)]$.
- ▶ Server sends $X = \phi(F)$ of size N .
- ▶ User k decodes $W_k = \varphi_k(W'_k, X)$.
- ▶ Rate: $R = N/L$.
- ▶ LCBC Capacity: The infimum of N/L over all achievable schemes.
- ▶ Capacity for 2 and 3 users is known. Capacity for $K \geq 4$ users is open.

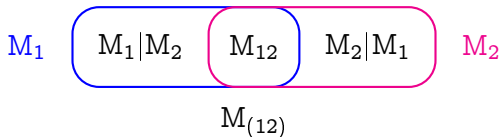
General Subspace Decomposition

- ▶ Our proposed scheme is based on a subspace decomposition derived from representable polymatroid spaces.
- ▶ This enables the server to design multicast messages that simultaneously benefit multiple users.
- ▶ Users can eliminate interference using their available side information.
- ▶ Notation:
 - ▶ Matrix: M . If columns are linear indept., they are a base.
 - ▶ Space spanned by columns of M : $\langle M \rangle$.
 - ▶ Intersection of subspaces: $M_S := \bigcap_{k \in S} \langle M_k \rangle$.
 - ▶ Union of subspaces: $M_{(S)} := \bigcup_{k \in S} \langle M_k \rangle$.

General Subspace Decomposition (Cont.)

- ▶ Notation:
 - ▶ Matrix: M . If columns are linear indept., they are a base.
 - ▶ Space spanned by columns of M : $\langle M \rangle$.
 - ▶ Intersection of subspaces: $M_S := \bigcap_{k \in S} \langle M_k \rangle$.
 - ▶ Union of subspaces: $M_{(S)} := \bigcup_{k \in S} \langle M_k \rangle$.
- ▶ Rank Notation:
 - ▶ Conditional Rank:

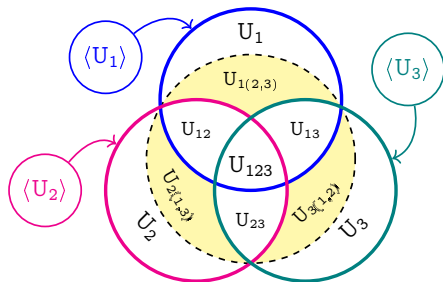
$$\text{rk}(M_1|M_2) := \text{rk}(M_{(12)}) - \text{rk}(M_2) = \text{rk}(M_1) - \text{rk}(M_{12}).$$



Subspace & Basis

Given $\{U_k : k \in [K]\}$, define $\mathcal{V} := \mathcal{V}_1 \cup \mathcal{V}_2 \cup \mathcal{V}_3$:

- ▶ $\mathcal{V}_1 = \{U_{\mathcal{S}} : \mathcal{S} \subseteq [K], |\mathcal{S}| \geq 2\}$.
- ▶ $\mathcal{V}_2 = \{U_{k(\mathcal{T} \setminus k)} : \mathcal{T} \subseteq [K], |\mathcal{T}| \geq 3, k \in \mathcal{T}\}$.
- ▶ $\mathcal{V}_3 = \{U_k, k \in [K]\}$.

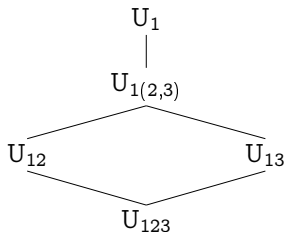
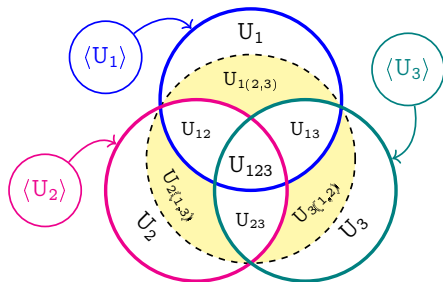


$$\begin{aligned}\mathcal{V}_1 &= \{U_{123}, U_{12}, U_{13}, U_{23}\}, \\ \mathcal{V}_2 &= \{U_{1(2,3)}, U_{2(1,3)}, U_{3(1,2)}\}, \\ \mathcal{V}_3 &= \{U_1, U_2, U_3\}.\end{aligned}$$

Subspace & Basis (Cont.)

Given $\{U_k : k \in [K]\}$, define $\mathcal{V} := \mathcal{V}_1 \cup \mathcal{V}_2 \cup \mathcal{V}_3$:

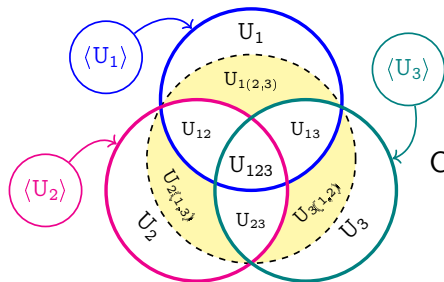
- ▶ For a subspace $V \in \mathcal{V}$, $LS(V)$ lists the "closest" subspaces contained in V .
- ▶ An ordered tree is possible by connecting node V and every node in $LS(V)$.



Subspace & Basis (Cont.)

Given $\{U_k : k \in [K]\}$, define $\mathcal{V} := \mathcal{V}_1 \cup \mathcal{V}_2 \cup \mathcal{V}_3$:

- Basis $B(V) := V \setminus \bigcup_{Q \in \text{LS}(V)} Q$. This spans V but not the subspaces in $\text{LS}(V)$.
- $C(V) = B(V) \cup \left(\bigcup_{U \in \text{LS}(V)} C(U) \right)$ is the set of bases covered by V .

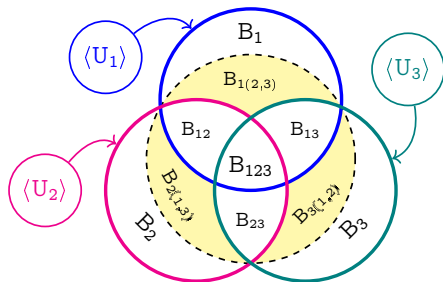


$$\begin{aligned}
 C(U_{12}) &= \{B_{12}, B_{123}\}, \\
 C(U_{1(2,3)}) &= \{B_{(123)}, B_{12}, B_{13}, B_{123}\}, \\
 C(U_1) &= \{B_1, B_{(123)}, B_{12}, B_{13}, B_{123}\}.
 \end{aligned}$$

Subspace & Basis (Cont.)

Lemma

Given any $\mathcal{T} \subseteq [K]$ and $t := |\mathcal{T}| \geq 3$, the subspaces $B_{k(\mathcal{T} \setminus \{k\})} : k \in \mathcal{T}$, have identical dimension, and any $t - 1$ of them are linearly independent.

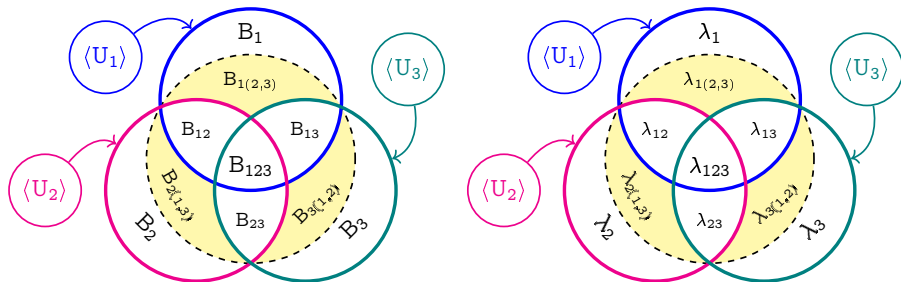


When $K = 3$, [YJ24a] shows $B_{1(2,3)}$, $B_{2(1,3)}$ and $B_{3(1,2)}$ are pairwise linearly independent, and have same dimension.

Theorem 1: Achievability via LP

Let $\lambda_\star \geq 0$ be the optimizing variables, essentially coding gain from linear coding.

- ▶ For every $U_S \in \mathcal{V}_1$, λ_S is assigned to its base B_S ;
- ▶ For every $U_{k(S)} \in \mathcal{V}_2$, $\lambda_{(\{k\} \cup S)}$ is assigned to $B_{k(S)}$;
- ▶ For every U_k , λ_k is assigned to B_k .



Theorem 1: Achievability via LP

For the K-LCBC, let $U_k = [V'_k; V_k]$. The following rate is achievable:

$$\min_{\lambda_* \geq 0} \sum_{S \subseteq [K]} \lambda_S + \sum_{t=3}^K \sum_{S \in \Omega_{[K]}^t} (t-1) \lambda_{(S)}$$

Where λ_* are variables associated with bases from $\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3$.

► For $U_S \in \mathcal{V}_1$ and $\mathcal{L}_S \subseteq \text{LC}(U_S)$,

$$\text{"Sum of } C_\lambda(U_S) \text{"} \leq \text{rk}(U_S \mid V'_k), \quad (1a)$$

$$\text{"Sum of } \bigcup_{V \in \mathcal{L}_S} C_\lambda(V) \text{"} \leq \text{rk}(\mathcal{L}_S \mid V'_k), \quad (1b)$$

Theorem 1: Achievability via LP

For the K-LCBC, let $U_k = [V'_k; V_k]$. The following rate is achievable:

$$\min_{\lambda_{\star} \geq 0} \sum_{S \subseteq [K]} \lambda_S + \sum_{t=3}^K \sum_{S \in \Omega_{[K]}^t} (t-1) \lambda_{(S)}$$

Where $\lambda_{\star}$ are variables associated with bases from $\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3$.

- For $U_S \in \mathcal{V}_1$ and $\mathcal{L}_S \subseteq \text{LC}(U_S)$,

$$\text{"Sum of } C_{\lambda}(U_S) \text{"} \leq \text{rk}(U_S \mid V'_k), \quad (1a)$$

$$\text{"Sum of } \bigcup_{V \in \mathcal{L}_S} C_{\lambda}(V) \text{"} \leq \text{rk}(\mathcal{L}_S \mid V'_k), \quad (1b)$$

- For $U_{k(S)} \in \mathcal{V}_2$ and $\mathcal{L}_{k(S)} \subseteq \text{LC}(U_{k(S)})$,

$$\text{"Sum of } C_{\lambda}(U_{k(S)}) \text{"} \leq \text{rk}(U_{k(S)} \mid V'_k), \quad (2a)$$

$$\text{"Sum of } \bigcup_{V \in \mathcal{L}_{k(S)}} C_{\lambda}(V) \text{"} \leq \text{rk}(\mathcal{L}_{k(S)} \mid V'_k), \quad (2b)$$

Theorem 1: Achievable Rate via LP

For the K-LCBC, let $U_k = [V'_k; V_k]$. The following rate is achievable:

$$\min_{\lambda_{\star} \geq 0} \sum_{\mathcal{S} \subseteq [K]} \lambda_{\mathcal{S}} + \sum_{t=3}^K \sum_{\mathcal{S} \in \Omega_{[K]}^t} (t-1) \lambda_{(\mathcal{S})}$$

Where $\lambda_{\star}$ are coefficients associated with bases from $\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3$.

► ...

► For $U_k \in \mathcal{V}_3$,

$$\text{"Sum of } C_{\lambda}(U_k) = \text{rk}(U_k \mid V'_k) = \text{rk}(V_k), \quad (3)$$

► Equality ensures all desired information is recovered.

► When $K = 2$ or $K = 3$, this LP is proved as optimal in [SJ19] and [YJ24a], respectively.

Interpreting λ Variables & Coding Gain

The objective function can be rewritten as:

$$\sum_{k=1}^K \text{rk}(U_k | V'_k) - \sum_{t=2}^K \sum_{\mathcal{S} \in \Omega_{[K]}^t} (t-1) \lambda_{\mathcal{S}} - \sum_{\mathcal{S} \subseteq [K], |\mathcal{S}| \geq 3} \lambda_{(\mathcal{S})}$$

- ▶ First term: Load of uncoded transmissions (serving users individually).
- ▶ Each $\lambda_{\star}$ represents the coding gain from a multicast message.

Interpreting λ Variables & Coding Gain

The objective function can be rewritten as:

$$\sum_{k=1}^K \text{rk}(U_k | V'_k) - \sum_{t=2}^K \sum_{\mathcal{S} \in \Omega_{[K]}^t} (t-1) \lambda_{\mathcal{S}} - \sum_{\mathcal{S} \subseteq [K], |\mathcal{S}| \geq 3} \lambda_{(\mathcal{S})}$$

- ▶ First term: Load of uncoded transmissions (serving users individually).
- ▶ Each $\lambda_{\star}$ represents the coding gain from a multicast message.
- ▶ $\lambda_{\mathcal{S}}$: Rank of (multicast or unicast when $|\mathcal{S}| = 1$) message serving $|\mathcal{S}|$ users, reducing load by $(|\mathcal{S}| - 1) \lambda_{\mathcal{S}}$.
- ▶ $\lambda_{(\mathcal{S})}$: Rank of messages where $t - 1$ are linearly independent, serving $t = |\mathcal{S}|$ users, reducing load by $\lambda_{(\mathcal{S})}$.

Example: K=4 Users

Toy Example (Index Coding):

- ▶ $\mathbf{f} = [A, B, C, D]$.
- ▶ User 1 wants B , knows A ; User 2 wants C , knows B ; User 3 wants D , knows C ; User 4 wants A , knows D .
- ▶ Subspace decomposition
 - ▶ $U_1 = [A, B], U_2 = [B, C], U_3 = [C, D], U_4 = [A, D]$.
 - ▶ $B_{12} = B, B_{23} = C, B_{34} = D, B_{14} = A$.
- ▶ Objective function

$$\sum_{S \subseteq [4]} \lambda_S + \sum_{t=3}^4 \sum_{S \in \Omega_{[4]}^t} (t-1) \lambda_{(S)}.$$

- ▶ Constraints on λ_*
 - ▶ $\lambda_{12} \leq \text{rk}(U_{12}|V'_1) = \text{rk}([A, B]) - \text{rk}([B]) = 1,$
 - ▶ $\lambda_{12} \leq \text{rk}(U_{12}|V'_2) = \text{rk}([B, B]) - \text{rk}([B]) = 0$
 - ▶ All $\lambda_S = 0$ where $S \subseteq [4], |S| \geq 2$.

Example: K=4 Users

Toy Example (Index Coding):

- ▶ $\mathbf{f} = [A, B, C, D]$.
- ▶ User 1 wants B , knows A ; User 2 wants C , knows B ; User 3 wants D , knows C ; User 4 wants A , knows D .
- ▶ Subspace decomposition
 - ▶ $U_1 = [A, B], U_2 = [B, C], U_3 = [C, D], U_4 = [A, D]$.
 - ▶ $B_{12} = B, \quad B_{23} = C, \quad B_{34} = D, \quad B_{14} = A$.
- ▶ Objective function

$$\sum_{S \subseteq [4]} \lambda_S + \sum_{t=3}^4 \sum_{S \in \Omega_{[4]}^t} (t-1) \lambda_{(S)}.$$

- ▶ Constraints on $\lambda_\star$
 - ▶ $\lambda_{(123)} \leq \text{rk}(U_{1(23)} | V'_1) = \text{rk}([A]) - \text{rk}([A]) = 0,$
 - ▶ $\lambda_{(123)} \leq \text{rk}(U_{2(13)} | V'_2) = \text{rk}([A, B]) - \text{rk}([B]) = 1,$
 - ▶ $\lambda_{(123)} \leq \text{rk}(U_{3(12)} | V'_3) = \text{rk}([C, C]) - \text{rk}([C]) = 0,$
 - ▶ $\lambda_{(123)} = \lambda_{(124)} = \lambda_{(134)} = \lambda_{(234)} = 0.$

Example: K=4 Users

Toy Example (Index Coding):

- ▶ $\mathbf{f} = [A, B, C, D]$.
- ▶ User 1 wants B , knows A ; User 2 wants C , knows B ; User 3 wants D , knows C ; User 4 wants A , knows D .
- ▶ Subspace decomposition
 - ▶ $U_1 = [A, B], U_2 = [B, C], U_3 = [C, D], U_4 = [A, D]$.
 - ▶ $B_{12} = B, \quad B_{23} = C, \quad B_{34} = D, \quad B_{14} = A$.
- ▶ Objective function

$$\sum_{S \subseteq [4]} \lambda_S + \sum_{t=3}^4 \sum_{S \in \Omega_{[4]}^t} (t-1) \lambda_{(S)}.$$

- ▶ Constraints on λ_*
 - ▶ $\lambda_{(1234)} \leq \text{rk}(U_{1(234)} | V'_1) = \text{rk}([A, B]) - \text{rk}([A]) = 1,$
 - ▶ $\lambda_{(1234)} \leq \text{rk}(U_{2(134)} | V'_2) = \text{rk}([B, C]) - \text{rk}([B]) = 1,$
 - ▶ $\lambda_{(1234)} \leq \text{rk}(U_{3(124)} | V'_3) = \text{rk}([C, D]) - \text{rk}([C]) = 1,$
 - ▶ $\lambda_{(1234)} \leq \text{rk}(U_{4(123)} | V'_4) = \text{rk}([A, D]) - \text{rk}([D]) = 1,$

Example: K=4 Users

Toy Example (Index Coding):

- ▶ $f = [A, B, C, D]$.
- ▶ User 1 wants B , knows A ; User 2 wants C , knows B ; User 3 wants D , knows C ; User 4 wants A , knows D .
- ▶ Subspace decomposition
 - ▶ $U_1 = [A, B], U_2 = [B, C], U_3 = [C, D], U_4 = [A, D]$.
 - ▶ $B_{12} = B, \quad B_{23} = C, \quad B_{34} = D, \quad B_{14} = A$.
- ▶ Objective function

$$\sum_{S \subseteq [4]} \lambda_S + \sum_{t=3}^4 \sum_{S \in \Omega_{[4]}^t} (t-1) \lambda_{(S)}.$$

- ▶ Constraints on λ_* : $\lambda_{(1234)} \leq 1, \lambda_k \leq 1$,
- ▶ “Four birds Three stones”, $X = (A + B, B + C, C + D)$.
- ▶ Optimal as proved by [AK⁺18, MAIS converse].

Generic LCBC Setting

- ▶ Consider a LCBC instance Λ_n where
 - ▶ uniform cache size and demand size;
 - ▶ V'_k and V_k are generated from $\mathbb{F}_{p^n}$ at i.i.d. uniformly random;
- ▶ Performance Metric
 - ▶ Find Δ s.t. $\Pr(|\Delta^*(\Lambda_n) - \Delta| < \epsilon) \rightarrow 1$ when $n \rightarrow \infty$.
 - ▶ Since $\Delta^*(\Lambda_n)$ is always bounded, it implies $\mathbb{E}\Delta^*(\Lambda_n) = \Delta$.
- ▶ [YJ24b] proves such exact Δ^* exists when certain conditions hold, if not, it is within a factor of 2.
 - ▶ The scheme invokes asymptotic IA scheme in K-user interference channel.

Example: K=4 Users

Example (Generic LCBC setting)

- ▶ $\mathbf{f} = [A, B, C, D]$, $d = 4$, $m'_k = m_k = 1$.
- ▶ $\mathbf{V}'_k = [v'_{k,i} : i \in [4]]$, $\mathbf{V}_k = [v_{k,i} : i \in [4]]$.
- ▶ $[\mathbf{V}'_1; \dots; \mathbf{V}'_4; \mathbf{V}_1; \dots; \mathbf{V}_4]$ is $(4, 8)$ MDS code.

Subspace decomposition ($ijr\ell$ is a permutation of 1234)

- ▶ $B_{i(jr)} = U_i$, other bases are 0.

Constraints on $\lambda_\star$

$$\lambda_{(ijr)} \leq \text{rk}(U_{i(jr)} | \mathbf{V}'_i) = 1, \quad (4a)$$

$$\lambda_{(1234)} \leq \text{rk}(U_{i(jr\ell)} | \mathbf{V}'_i) = 1 \quad (4b)$$

$$\lambda_{(ijr)} + \lambda_{(ij\ell)} \leq \text{rk}(U_{i(jr)}, U_{i(j\ell)} | \mathbf{V}'_i) = 1, \quad (4c)$$

$$\lambda_{(ijr)} + \lambda_{(ij\ell)} + \lambda_{(ir\ell)} \leq \text{rk}(U_{i(jr)}, U_{i(j\ell)}, U_{i(r\ell)} | \mathbf{V}'_i) = 1, \quad (4d)$$

Solving LP, $\lambda_{(ijr)} = \frac{1}{3}$, thus the load is $\frac{8}{3}$. However, [YJ24b] proves the exact load is 2.

Conclusion

- ▶ We propose a new achievable scheme for general K-LCBC (i.e., arbitrary number of users K).
- ▶ The scheme is based on a general subspace decomposition derived from representable polymatroid spaces.
- ▶ It leverages linear dependencies among subspaces to enable multicast opportunities and interference elimination, optimizing the communication load via a linear program.
- ▶ The scheme recovers known capacity results for $K = 2$ and $K = 3$ users.

Future Work

- ▶ Comparing the achievable rate with a converse bound to determine optimality or sub-optimality gaps.
- ▶ Further strengthening the scheme by accounting for more complex dependencies that may exist in the subspace decomposition, potentially lowering the rate.
- ▶ Exploring applications to related problems, such as:
 - ▶ Coded caching with linear coded placement.
 - ▶ Coded caching with scalar linear function retrieval.

Thank You!

References I



Fatemeh Arbabjolfaei, Young-Han Kim, et al.

Fundamentals of index coding.

Foundations and Trends® in Communications and Information Theory, 14(3-4):163–346, 2018.



Hua Sun and Syed Ali Jafar.

On the capacity of computation broadcast.

IEEE Transactions on Information Theory, 66(6):3417–3434, 2019.



Yuhang Yao and Syed A Jafar.

The capacity of 3 user linear computation broadcast.

IEEE Transactions on Information Theory, 2024.

References II



Yuhang Yao and Syed A Jafar.

On the generic capacity of k-user symmetric linear computation broadcast.

IEEE Transactions on Information Theory, 2024.