Order-Optimal Permutation Codes in the Generalized Cayley Metric

Siyi Yang, Clayton Schoeny, Lara Dolecek

LORIS, Electrical and Computer Engineering, UCLA

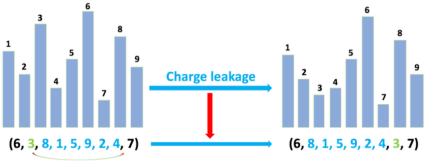
March 12th, 2018

Outline

Outline

Applications

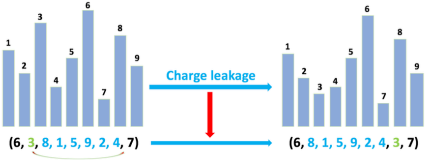
- Flash memories: charge leakage between cells [1]



[1] A. Jiang et al. "Rank Modulation for Flash Memories". In: *IEEE Trans. Inf. Theory* 55.6 (2009), pp. 2659–2673.

Applications

- Flash memories: charge leakage between cells [1]



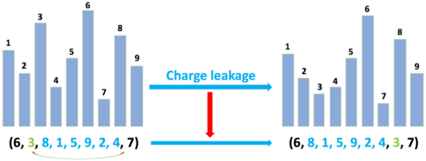
- Genome resequencing: gene rearrangement in a chromosome [2]

[1] A. Jiang et al. "Rank Modulation for Flash Memories". In: *IEEE Trans. Inf. Theory* 55.6 (2009), pp. 2659–2673.

[2] R. Zeira and R. Shamir. "Sorting by cuts, joins and whole chromosome duplications". In: *Journal of Computational Biology* 24 (2017), pp. 127–137.

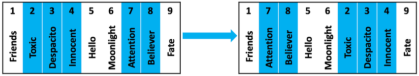
Applications

- Flash memories: charge leakage between cells [1]



- Genome resequencing: gene rearrangement in a chromosome [2]

- Cloud storage system: rearrangements of items in multiple folders



[1] A. Jiang et al. "Rank Modulation for Flash Memories". In: *IEEE Trans. Inf. Theory* 55.6 (2009), pp. 2659–2673.

[2] R. Zeira and R. Shamir. "Sorting by cuts, joins and whole chromosome duplications". In: *Journal of Computational Biology* 24 (2017), pp. 127–137.

Measures in Permutation Codes

- Common measures

Measures in Permutation Codes

- Common measures
  - Kendall-τ metric: transpositions [3]

[3] Y. Zhang and G. Ge. "Snake-in-the-Box Codes for Rank Modulation Under Kendall's τ-Metric". In: *IEEE Trans. Inf. Theory* 62 (Jan. 2016), pp. 151–158.

Measures in Permutation Codes

- Common measures
  - Kendall-τ metric: transpositions [3]

  - Ulam metric: translocation [4]

[3] Y. Zhang and G. Ge. "Snake-in-the-Box Codes for Rank Modulation Under Kendall's τ-Metric". In: *IEEE Trans. Inf. Theory* 62 (Jan. 2016), pp. 151–158.

[4] F. Farnoud, V. Skachek, and O. Milenkovic. "Error-correction in Flash Memories via Codes in the Ulam Metric". In: *IEEE Trans. Inf. Theory* 59 (May 2013), pp. 3003–3020.

Measures in Permutation Codes

- Common measures
  - Kendall-τ metric: transpositions [3]

  - Ulam metric: translocation [4]

- Measure under discussion

[3] Y. Zhang and G. Ge. "Snake-in-the-Box Codes for Rank Modulation Under Kendall's τ-Metric". In: *IEEE Trans. Inf. Theory* 62 (Jan. 2016), pp. 151–158.

[4] F. Farnoud, V. Skachek, and O. Milenkovic. "Error-correction in Flash Memories via Codes in the Ulam Metric". In: *IEEE Trans. Inf. Theory* 59 (May 2013), pp. 3003–3020.

Measures in Permutation Codes

- Common measures
  - Kendall-τ metric: transpositions [3]

  - Ulam metric: translocation [4]

- Measure under discussion
  - Generalized Cayley metric: generalized transposition [5]

  - No restrictions on the lengths and positions of the translocated segments

[3] Y. Zhang and G. Ge. "Snake-in-the-Box Codes for Rank Modulation Under Kendall's τ-Metric". In: *IEEE Trans. Inf. Theory* 62 (Jan. 2016), pp. 151–158.

[4] F. Farnoud, V. Skachek, and O. Milenkovic. "Error-correction in Flash Memories via Codes in the Ulam Metric". In: *IEEE Trans. Inf. Theory* 59 (May 2013), pp. 3003–3020.

[5] Y. M. Chee and V. K. Vu. "Breakpoint analysis and permutation codes in generalized Kendall tau and Cayley metrics". In: *Proc. IEEE Int. Symp. Inf. Theory*. Hawaii, USA, June 2014, pp. 2959–2963.

Ultimate Goal

- Objective
  - Construction of order-optimal codes in the generalized Cayley metric

Ultimate Goal

- Objective
  - Construction of order-optimal codes in the generalized Cayley metric
- Prior work [6]

[6] Y. M. Chee and V. K. Vu. "Breakpoint analysis and permutation codes in generalized Kendall tau and Cayley metrics". In: *Proc. IEEE Int. Symp. Inf. Theory*. Hawaii, USA, June 2014, pp. 2959–2963.

Ultimate Goal

- Objective
  - Construction of order-optimal codes in the generalized Cayley metric
- Prior work [6]
  - Based on the error-correcting codes in the Ulam metric [7]

[6] Y. M. Chee and V. K. Vu. "Breakpoint analysis and permutation codes in generalized Kendall tau and Cayley metrics". In: *Proc. IEEE Int. Symp. Inf. Theory*. Hawaii, USA, June 2014, pp. 2959–2963.

[7] F. Farnoud, V. Skachek, and O. Milenkovic. "Error-correction in Flash Memories via Codes in the Ulam Metric". In: *IEEE Trans. Inf. Theory* 59 (May 2013), pp. 3003–3020.

Ultimate Goal

- Objective
  - Construction of order-optimal codes in the generalized Cayley metric
- Prior work [6]
  - Based on the error-correcting codes in the Ulam metric [7]
  - Interleaving based: induce a redundancy of $\mathcal{O}(N)$ bits, where N is the codelength

[6] Y. M. Chee and V. K. Vu. "Breakpoint analysis and permutation codes in generalized Kendall tau and Cayley metrics". In: *Proc. IEEE Int. Symp. Inf. Theory*. Hawaii, USA, June 2014, pp. 2959–2963.

[7] F. Farnoud, V. Skachek, and O. Milenkovic. "Error-correction in Flash Memories via Codes in the Ulam Metric". In: *IEEE Trans. Inf. Theory* 59 (May 2013), pp. 3003–3020.

Ultimate Goal

- Objective
  - Construction of order-optimal codes in the generalized Cayley metric
- Prior work [6]
  - Based on the error-correcting codes in the Ulam metric [7]
  - Interleaving based: induce a redundancy of $\mathcal{O}(N)$ bits, where N is the codelength
- Ultimate goal
  - Redundancy for an order-optimal code that corrects t generalized transposition errors: $\mathcal{O}(t \log N)$ bits

[6] Y. M. Chee and V. K. Vu. "Breakpoint analysis and permutation codes in generalized Kendall tau and Cayley metrics". In: *Proc. IEEE Int. Symp. Inf. Theory*. Hawaii, USA, June 2014, pp. 2959–2963.

[7] F. Farnoud, V. Skachek, and O. Milenkovic. "Error-correction in Flash Memories via Codes in the Ulam Metric". In: *IEEE Trans. Inf. Theory* 59 (May 2013), pp. 3003–3020.

Outline

Generalized Cayley Distance

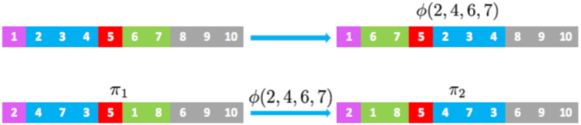
- **Generalized transposition** $\phi(i_1, j_1, i_2, j_2)$:
    - $\phi(i_1, j_1, i_2, j_2) \in \mathbb{S}_N$, $i_1 \leq j_1 < i_2 \leq j_2 \in [N]$, $\mathbb{S}_N$ is the symmetric group of permutations with length N
    - A permutation obtained from swapping the segments $e[i_1, j_1]$ and $e[i_2, j_2]$ in the identity permutation

Generalized Cayley Distance

- **Generalized transposition** $\phi(i_1, j_1, i_2, j_2)$:
  - $\phi(i_1, j_1, i_2, j_2) \in \mathbb{S}_N$, $i_1 \le j_1 < i_2 \le j_2 \in [N]$, $\mathbb{S}_N$ is the symmetric group of permutations with length N
  - A permutation obtained from swapping the segments $e[i_1, j_1]$ and $e[i_2, j_2]$ in the identity permutation

Generalized Cayley Distance

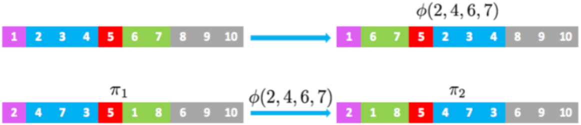
- **Generalized transposition** $\phi(i_1, j_1, i_2, j_2)$:
  - $\phi(i_1, j_1, i_2, j_2) \in \mathbb{S}_N$, $i_1 \le j_1 < i_2 \le j_2 \in [N]$, $\mathbb{S}_N$ is the symmetric group of permutations with length N
  - A permutation obtained from swapping the segments $e[i_1, j_1]$ and $e[i_2, j_2]$ in the identity permutation



  - $\pi_2 = \pi_1 \circ \phi$

Generalized Cayley Distance

- **Generalized transposition** $\phi(i_1, j_1, i_2, j_2)$:
  - $\phi(i_1, j_1, i_2, j_2) \in \mathbb{S}_N$, $i_1 \leq j_1 < i_2 \leq j_2 \in [N]$, $\mathbb{S}_N$ is the symmetric group of permutations with length N
  - A permutation obtained from swapping the segments $e[i_1, j_1]$ and $e[i_2, j_2]$ in the identity permutation



  - $\pi_2 = \pi_1 \circ \phi$
- **Generalized Cayley distance** $d_G(\pi_1, \pi_2)$:
  - The minimum number of generalized transpositions that is needed to obtain the permutation π_2 from π_1,

$$d_G(\pi_1, \pi_2) \triangleq \min_d \{\exists\ \phi_1, \phi_2, \cdots, \phi_d \in \mathbb{T}_N, \text{ s.t., } \pi_2 = \pi_1 \circ \phi_1 \circ \phi_2 \cdots \circ \phi_d\}.$$

Theoretical Foundation

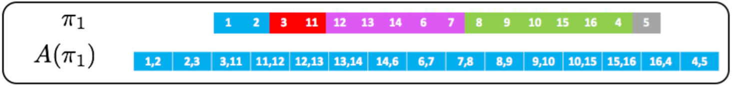
- Exact value of $d_G(\pi_1, \pi_2)$ is hard to compute
    - Objective: find another distance that $d_G(\pi_1, \pi_2)$ can be embedded in - block permutation distance

Theoretical Foundation

- Exact value of $d_G(\pi_1, \pi_2)$ is hard to compute
  - Objective: find another distance that $d_G(\pi_1, \pi_2)$ can be embedded in - block permutation distance
- **Characteristic set** $A(\pi) \triangleq \{(\pi(i), \pi(i+1)) | 1 \leq i \leq N\}$

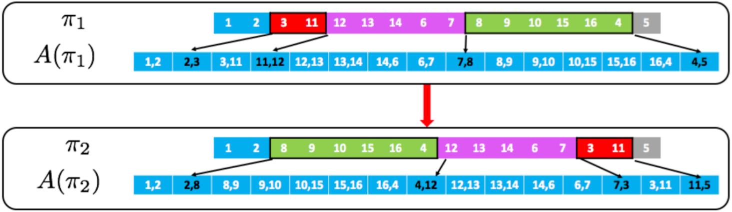
Theoretical Foundation

- Exact value of $d_G(\pi_1, \pi_2)$ is hard to compute
  - Objective: find another distance that $d_G(\pi_1, \pi_2)$ can be embedded in - block permutation distance
- **Characteristic set** $A(\pi) \triangleq \{(\pi(i), \pi(i+1)) | 1 \leq i \leq N\}$
- Observation
  - Each generalized transposition changes at most 4 elements in the characteristic set (boundaries of the unaltered blocks)



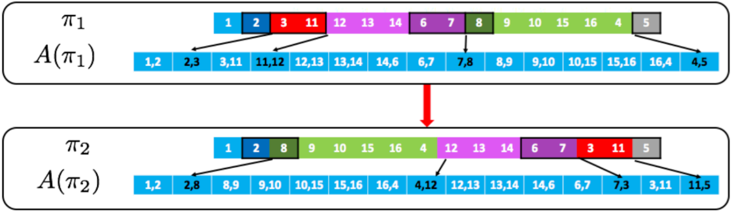
Theoretical Foundation

- Exact value of $d_G(\pi_1, \pi_2)$ is hard to compute
  - Objective: find another distance that $d_G(\pi_1, \pi_2)$ can be embedded in - block permutation distance
- **Characteristic set** $A(\pi) \triangleq \{(\pi(i), \pi(i+1)) | 1 \leq i \leq N\}$
- Observation
  - Each generalized transposition changes at most 4 elements in the characteristic set (boundaries of the unaltered blocks)



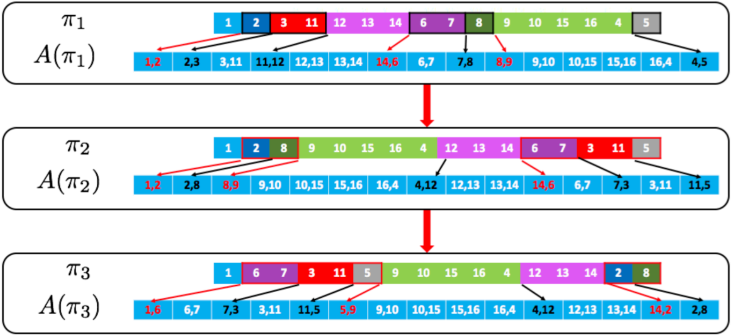
Theoretical Foundation

- Exact value of $d_G(\pi_1, \pi_2)$ is hard to compute
  - Objective: find another distance that $d_G(\pi_1, \pi_2)$ can be embedded in - block permutation distance
- **Characteristic set** $A(\pi) \triangleq \{(\pi(i), \pi(i+1)) | 1 \leq i \leq N\}$
- Observation
  - Each generalized transposition changes at most 4 elements in the characteristic set (boundaries of the unaltered blocks)



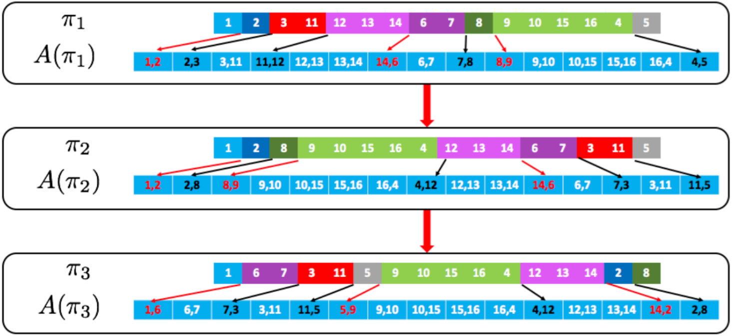
Theoretical Foundation

- Exact value of $d_G(\pi_1, \pi_2)$ is hard to compute
  - Objective: find another distance that $d_G(\pi_1, \pi_2)$ can be embedded in - block permutation distance
- **Characteristic set** $A(\pi) \triangleq \{(\pi(i), \pi(i+1)) | 1 \leq i \leq N\}$
- Observation
  - Each generalized transposition changes at most 4 elements in the characteristic set (boundaries of the unaltered blocks)



Theoretical Foundation

- Exact value of $d_G(\pi_1, \pi_2)$ is hard to compute
  - Objective: find another distance that $d_G(\pi_1, \pi_2)$ can be embedded in - block permutation distance
- **Characteristic set** $A(\pi) \triangleq \{(\pi(i), \pi(i+1)) | 1 \leq i \leq N\}$
- Observation
  - Each generalized transposition changes at most 4 elements in the characteristic set (boundaries of the unaltered blocks)



Block Permutation Distance

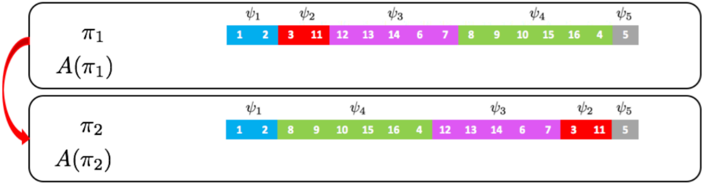
- **Block permutation distance** $d_B(\pi_1, \pi_2)$:
  - $d_B(\pi_1, \pi_2) = d$ iff $\exists \sigma \in \mathbb{D}_{d+1}$ such that $\forall\ 1 \leq i \leq d$, $\sigma(i+1) \neq \sigma(i) + 1$, $\psi_k = \pi_1 \left[i_{k-1} + 1 : i_k \right]$ for some $0 = i_0 < i_1 \cdots < i_d < i_{d+1} = N$, and $1 \leq k \leq d+1$, such that

$$\pi_1 = \left(\psi_1, \psi_2, \cdots, \psi_{d+1} \right),$$
$$\pi_2 = \left(\psi_{\sigma(1)}, \psi_{\sigma(2)}, \cdots, \psi_{\sigma(d+1)} \right).$$

Block Permutation Distance

- **Block permutation distance** $d_B(\pi_1, \pi_2)$:
  - $d_B(\pi_1, \pi_2) = d$ iff $\exists \sigma \in \mathbb{D}_{d+1}$ such that $\forall\ 1 \leq i \leq d$, $\sigma(i+1) \neq \sigma(i) + 1$, $\psi_k = \pi_1 \left[i_{k-1} + 1 : i_k\right]$ for some $0 = i_0 < i_1 \cdots < i_d < i_{d+1} = N$, and $1 \leq k \leq d+1$, such that

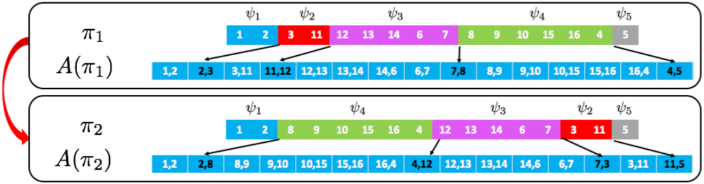
$$\pi_1 = \left(\psi_1, \psi_2, \cdots, \psi_{d+1}\right),$$
$$\pi_2 = \left(\psi_{\sigma(1)}, \psi_{\sigma(2)}, \cdots, \psi_{\sigma(d+1)}\right).$$



Block Permutation Distance

- **Block permutation distance** $d_B(\pi_1, \pi_2)$:
  - $d_B(\pi_1, \pi_2) = d$ iff $\exists \sigma \in \mathbb{D}_{d+1}$ such that $\forall\ 1 \leq i \leq d$, $\sigma(i+1) \neq \sigma(i) + 1$, $\psi_k = \pi_1\left[i_{k-1} + 1 : i_k\right]$ for some $0 = i_0 < i_1 \cdots < i_d < i_{d+1} = N$, and $1 \leq k \leq d+1$, such that

$$\pi_1 = \left(\psi_1, \psi_2, \cdots, \psi_{d+1}\right),$$
$$\pi_2 = \left(\psi_{\sigma(1)}, \psi_{\sigma(2)}, \cdots, \psi_{\sigma(d+1)}\right).$$

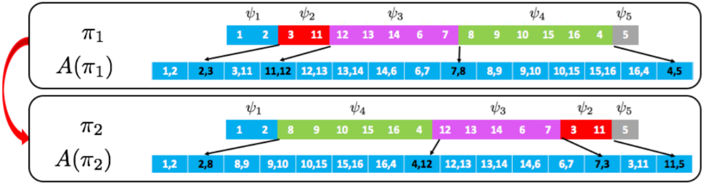


  - $d_B(\pi_1, \pi_2) = \frac{1}{2}|A(\pi_1) \Delta A(\pi_2)|$

Block Permutation Distance

- **Block permutation distance** $d_B(\pi_1, \pi_2)$:
  - $d_B(\pi_1, \pi_2) = d$ iff $\exists \sigma \in \mathbb{D}_{d+1}$ such that $\forall\ 1 \le i \le d$, $\sigma(i+1) \neq \sigma(i) + 1$, $\psi_k = \pi_1\left[i_{k-1} + 1 : i_k\right]$ for some $0 = i_0 < i_1 \cdots < i_d < i_{d+1} = N$, and $1 \le k \le d+1$, such that

$$\pi_1 = (\psi_1, \psi_2, \cdots, \psi_{d+1}),$$
$$\pi_2 = \left(\psi_{\sigma(1)}, \psi_{\sigma(2)}, \cdots, \psi_{\sigma(d+1)}\right).$$



  - $d_B(\pi_1, \pi_2) = \frac{1}{2}|A(\pi_1)\Delta A(\pi_2)|$
- Metric embedding:

$$d_G(\pi_1, \pi_2) \le d_B(\pi_1, \pi_2) \le 4d_G(\pi_1, \pi_2)$$

Definitions and Rates of Order-Optimal Codes

- *t*-**Generalized Cayley code** $\mathcal{C}_G(N, t)$
  - Corrects t generalized transposition errors, $d_{G,min} \geq 2t + 1$

Definitions and Rates of Order-Optimal Codes

- t-**Generalized Cayley code** $\mathcal{C}_G(N, t)$
  - Corrects t generalized transposition errors, $d_{G,min} \geq 2t + 1$
- t-**Block permutation code** $\mathcal{C}_B(N, t)$
  - Minimum block permutation distance $d_{B,min} \geq 2t + 1$

Definitions and Rates of Order-Optimal Codes

- t-**Generalized Cayley code** $\mathcal{C}_G(N, t)$
  - Corrects t generalized transposition errors, $d_{G,min} \geq 2t + 1$
- t-**Block permutation code** $\mathcal{C}_B(N, t)$
  - Minimum block permutation distance $d_{B,min} \geq 2t + 1$
- Optimal code rates: $R_{G,opt}(N, t)$, $R_{B,opt}(N, t)$

Definitions and Rates of Order-Optimal Codes

- t-**Generalized Cayley code** $\mathcal{C}_G(N,t)$
  - Corrects t generalized transposition errors, $d_{G,min} \geq 2t+1$
- t-**Block permutation code** $\mathcal{C}_B(N,t)$
  - Minimum block permutation distance $d_{B,min} \geq 2t+1$
- Optimal code rates: $R_{G,opt}(N,t)$, $R_{B,opt}(N,t)$
- Order-optimal $4t$-block permutation codes are order-optimal t-generalized Cayley codes

Theorem

The optimal rates satisfy the following inequalites,

$$1 - c_1 \cdot \frac{2t+1}{N} \leq R_{B,opt}(N,t) \leq 1 - \frac{t}{N},$$
$$1 - c_1 \cdot \frac{8t+1}{N} \leq R_{G,opt}(N,t) \leq 1 - c_2 \cdot \frac{4t}{N},$$

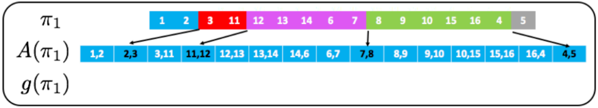
for fixed t and sufficiently large N, where $c_1 = 1 + \frac{2\log e}{\log N}$, $c_2 = 1 - \frac{3(\log t+1)}{4(\log N-1)}$.

Outline

Key Idea in Encoding Scheme

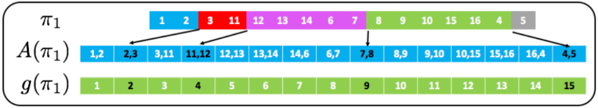
π_1	1	2	3	11	12	13	14	6	7	8	9	10	15	16	4	5
$A(\pi_1)$																
$g(\pi_1)$																

Key Idea in Encoding Scheme



Step 1: Compute the characteristic set $A(\pi)$ for every π

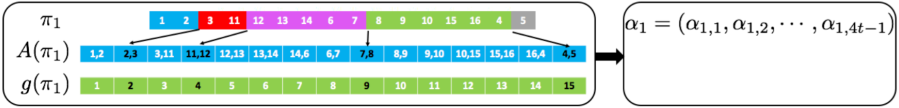
Key Idea in Encoding Scheme



Step 1: Compute the characteristic set $A(\pi)$ for every π

Step 2: Map $A(\pi)$ onto $\mathbb{F}_q$ as $g(\pi)$, where q is a prime number such that $N^2 - N \leq q \leq 2N^2 - 2N$ (*Bertrand's Postulate*)

Key Idea in Encoding Scheme

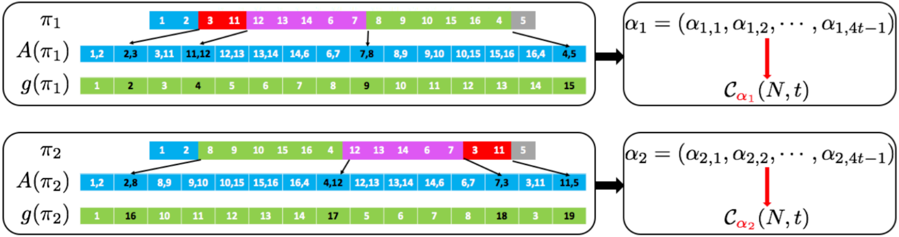


Step 1: Compute the characteristic set $A(\pi)$ for every π

Step 2: Map $A(\pi)$ onto $\mathbb{F}_q$ as $g(\pi)$, where q is a prime number such that $N^2 - N \leq q \leq 2N^2 - 2N$ (*Bertrand's Postulate*)

Step 3: Compute the parity check sum $h_t(\pi)$. Here $h_t(\pi) \triangleq (\alpha_1, \alpha_2, \cdots, \alpha_{4t-1})$, $\alpha_i = \sum_{b \in g(\pi)} b^i$, $1 \leq i \leq 4t-1$

Key Idea in Encoding Scheme



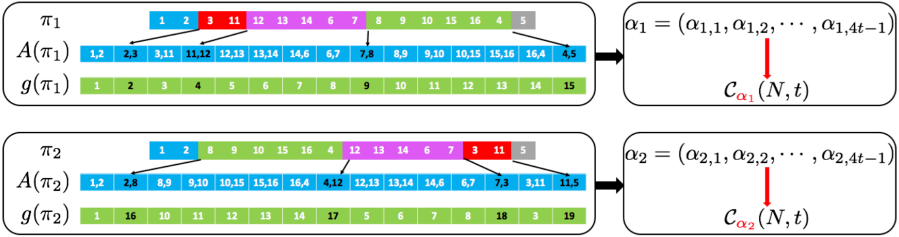
Step 1: Compute the characteristic set $A(\pi)$ for every π

Step 2: Map $A(\pi)$ onto $\mathbb{F}_q$ as $g(\pi)$, where q is a prime number such that $N^2 - N \leq q \leq 2N^2 - 2N$ (*Bertrand's Postulate*)

Step 3: Compute the parity check sum $h_t(\pi)$. Here $h_t(\pi) \triangleq (\alpha_1, \alpha_2, \cdots, \alpha_{4t-1})$, $\alpha_i = \sum_{b \in g(\pi)} b^i$, $1 \leq i \leq 4t-1$

Step 4: Permutations with the same α constitute a t-block permutation code $\mathcal{C}_\alpha(N,t)$

Key Idea in Encoding Scheme



Step 1: Compute the characteristic set $A(\pi)$ for every π

Step 2: Map $A(\pi)$ onto $\mathbb{F}_q$ as $g(\pi)$, where q is a prime number such that $N^2 - N \leq q \leq 2N^2 - 2N$ (*Bertrand's Postulate*)

Step 3: Compute the parity check sum $h_t(\pi)$. Here $h_t(\pi) \triangleq (\alpha_1, \alpha_2, \cdots, \alpha_{4t-1})$, $\alpha_i = \sum_{b \in g(\pi)} b^i$, $1 \leq i \leq 4t-1$

Step 4: Permutations with the same α constitute a t-block permutation code $\mathcal{C}_\alpha(N, t)$

Note: $\mathcal{C}_\alpha(N, t)$ with the maximum cardinality is order-optimal

Auxiliary Bound Results

Theorem

For all $B_1, B_2 \subset \mathbb{F}_q$, if $h_t(B_1) = h_t(B_2)$, then $|B_1 \Delta B_2| > 4t$.

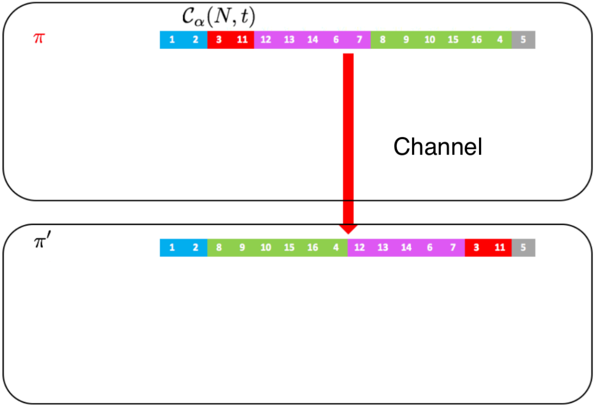
Proof.

If $|B_1 \Delta B_2| \leq 4t$, then $B_1 \setminus B_2 = \{x_1, x_2, \cdots, x_k\}$, $B_2 \setminus B_1 = \{x_{k+1}, x_{k+2}, \cdots, x_{2k}\}$, $k \leq 2t$.

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_{2k} \\ x_1^2 & x_2^2 & \cdots & x_{2k}^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{2d-1} & x_2^{2d-1} & \cdots & x_{2k}^{2d-1} \end{pmatrix} \mathbf{y} = \mathbf{0},$$

where $\mathbf{y} = [y_1, y_2, \cdots, y_{2k}]^T$, $y_i = 1(i \leq k)$, $y_i = -1(i > k)$.
The Vandermonde matrix has determinant $0 \implies \exists i, j$ such that $x_i = x_j$, contradiction! □

Key Steps in Decoding Algorithm



Channel: Receiver receives π' when sender sends π, $d_B(\pi, \pi') \leq t$

Key Steps in Decoding Algorithm

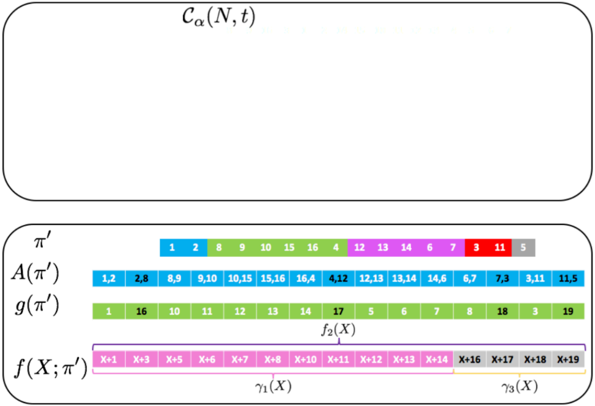
$\mathcal{C}_\alpha(N,t)$

π'		1	2	8	9	10	15	16	4	12	13	14	6	7	3	11	5
$A(\pi')$	1,2	2,8	8,9	9,10	10,15	15,16	16,4	4,12	12,13	13,14	14,6	6,7	7,3	3,11	11,5	
$g(\pi')$	1	16	10	11	12	13	14	17	5	6	7	8	18	3	19	

Channel: Receiver receives π' when sender sends π, $d_B(\pi, \pi') \leq t$

Step 1: Compute $A(\pi')$, $g(\pi')$ and $f_2 = (X; \pi')$ from π'

Key Steps in Decoding Algorithm

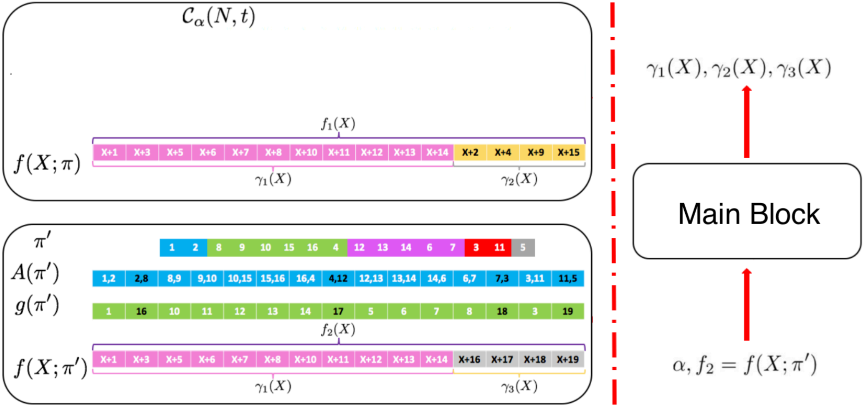


Channel: Receiver receives π' when sender sends π, $d_B(\pi,\pi') \le t$

Step 1: Compute $A(\pi')$, $g(\pi')$ and $f_2 = (X;\pi')$ from π'

Note: **Characteristic function** $f(X;\pi) = \prod_{b \in g(\pi)} (X+b)$

Key Steps in Decoding Algorithm



Channel: Receiver receives π' when sender sends π, $d_B(\pi, \pi') \leq t$

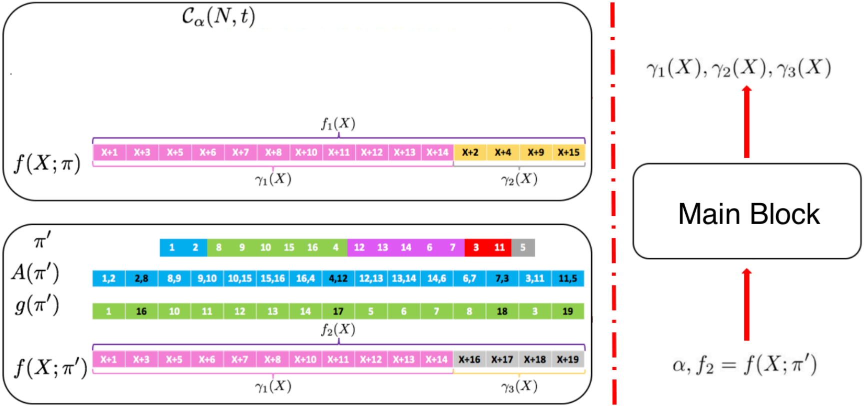
Step 1: Compute $A(\pi')$, $g(\pi')$ and $f_2 = (X; \pi')$ from π'

Note: **Characteristic function** $f(X;\pi) = \prod_{b \in g(\pi)} (X + b)$

f_2 provides incomplete information about the roots of f_1

α provides complete information about the $4t - 1$ coefficients of f_1

Key Steps in Decoding Algorithm



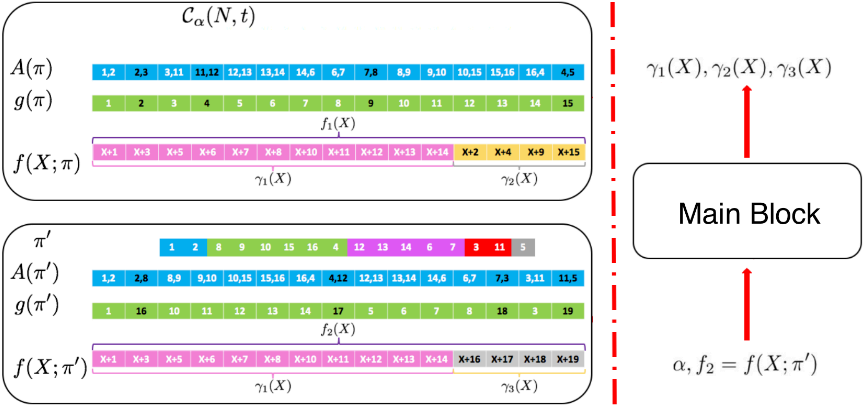
Channel: Receiver receives π' when sender sends π, $d_B(\pi,\pi') \leq t$

Step 1: Compute $A(\pi')$, $g(\pi')$ and $f_2 = (X;\pi')$ from π'

Note: **Characteristic function** $f(X;\pi) = \prod_{b\in g(\pi)}(X+b)$

Step 2: Compute $f_1(X) = f(X;\pi)$ from α and f_2

Key Steps in Decoding Algorithm



Channel: Receiver receives π' when sender sends π, $d_B(\pi, \pi') \leq t$

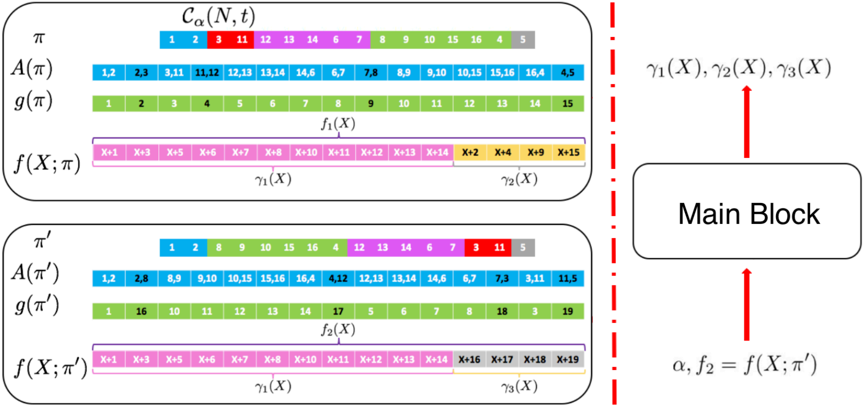
Step 1: Compute $A(\pi')$, $g(\pi')$ and $f_2 = (X; \pi')$ from π'

Note: **Characteristic function** $f(X;\pi) = \prod_{b \in g(\pi)} (X + b)$

Step 2: Compute $f_1(X) = f(X;\pi)$ from α and f_2

Step 3: Compute $g(\pi)$, $A(\pi)$ and π

Key Steps in Decoding Algorithm



Channel: Receiver receives π' when sender sends π, $d_B(\pi,\pi') \leq t$

Step 1: Compute $A(\pi')$, $g(\pi')$ and $f_2 = (X;\pi')$ from π'

Note: **Characteristic function** $f(X;\pi) = \prod_{b \in g(\pi)} (X+b)$

Step 2: Compute $f_1(X) = f(X;\pi)$ from α and f_2

Step 3: Compute $g(\pi)$, $A(\pi)$ and π

Main Block

- $(X^{t-k}\gamma_3, X^{t-k}\gamma_2)$ is a solution to $h_1 \circ f_1 = h_2 \circ f_2$, $\deg h_1 = \deg h_2 = t$
  - Any solution (h_1, h_2) is sufficient for computing γ_2, γ_3: $\gamma_1 = gcd(h_1, h_2)$, $\gamma_3 = \frac{h_1}{\gamma_1}$, $\gamma_2 = \frac{h_2}{\gamma_1}$;
- The first $4t$ constraints of the coefficients for h_1 cot $f_1 = h_2 \cdot f_2$ is $\mathbf{Ac} = \mathbf{b}$
  - The coefficient of $X^{N+t-k-1}$ in f: a_k, $(a_1, \cdots, a_{4t-1})$ is known from Newton's Identities
  - The coefficient of X^{t-k} in h: c_k
  - We can compute the coefficients of h_1, h_2 from the solution of $\mathbf{Ac} = \mathbf{b}$

$$\underbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ a_1 & 1 & \ddots & \vdots & a'_1 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots & \vdots & \ddots & 0 \\ a_{t-1} & a_{t-2} & \cdots & 1 & a'_{t-1} & a'_{t-2} & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{4t-2} & a_{4t-3} & \cdots & a_{3t-1} & a'_{4t-2} & a'_{4t-3} & \cdots & a'_{3t-1} \end{pmatrix}}_{\mathbf{A}} \underbrace{\begin{pmatrix} c_1 \\ \vdots \\ c_t \\ -c'_1 \\ \vdots \\ -c'_t \end{pmatrix}}_{\mathbf{c}} = \underbrace{\begin{pmatrix} a'_1 - a_1 \\ \vdots \\ a'_{4t-1} - a_{4t-1} \end{pmatrix}}_{\mathbf{b}}$$

Rate Comparison with Interleaving Based Codes

Lemma

Let $R_G(N,t)$, $R_{\rho_g C}(N,t)$ be the rate of our proposed code and the existing interleaving-based code, respectively. Then $R_G(N,t) > R_{\rho_g C}(N,t)$ when $t < \frac{N}{(16\log N+8)}$ for sufficiently large N.

Proof.

We know from previous discussion and [a] that

$$\begin{aligned} R_{\rho_g C}(N,t) &< 1 - \frac{2N + \mathcal{O}\left((\log N)^2\right)}{N\log N - (\log e)N + \frac{1}{2}\log N} \sim 1 - \frac{2}{\log N}, \\ R_G(N,t) &> 1 - \frac{32t\log N + 16t}{N\log N - (\log e)N + \frac{1}{2}\log N} \sim 1 - \frac{32t}{N}, \end{aligned} \quad (1)$$

$R_G(N,t) - R_{\rho_g C}(N,t) > 0$ when $t < \frac{N}{(16\log N+8)}$ for sufficiently large N. □

[a] R. Gabrys et al. "Codes Correcting Erasures and Deletions for Rank Modulation". In: *IEEE Trans. Inf. Theory* 62 (Jan. 2016), pp. 136–150.

Outline

Extension

- Problems in the previous construction

Extension

- Problems in the previous construction
  - Not explicitly constructive

Extension

- Problems in the previous construction
  - Not explicitly constructive
  - Non-systematic

Extension

- Problems in the previous construction
  - Not explicitly constructive
  - Non-systematic
    - Difficult to identify a bijection between the transmitted messages and the codewords

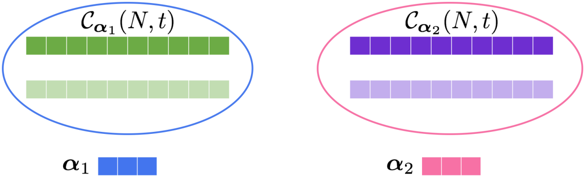
Extension

- Problems in the previous construction
  - Not explicitly constructive
  - Non-systematic
    - Difficult to identify a bijection between the transmitted messages and the codewords
- Solution
  - Constructing systematic codes in the generalized Cayley metric

Extension

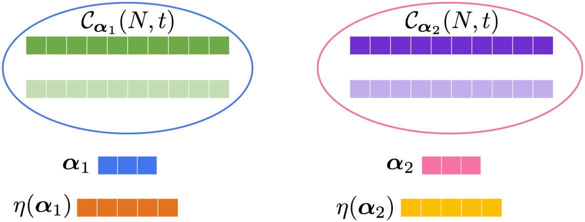
- Problems in the previous construction
  - Not explicitly constructive
  - Non-systematic
    - Difficult to identify a bijection between the transmitted messages and the codewords
- Solution
  - Constructing systematic codes in the generalized Cayley metric
  - Extended work submitted to IEEE Trans. Information Theory, also available at arxiv: https://arxiv.org/abs/1803.04314

Systematic Codes in the Generalized Cayley Metric



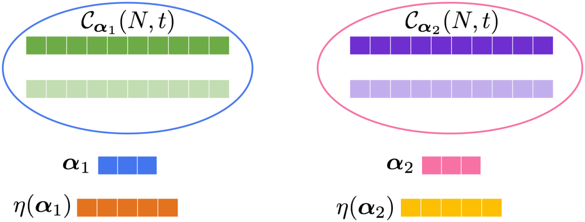
- Main idea: insert k elements $[N+1:N+k]$ into the length N permutations at positions decided by their parity check sums

Systematic Codes in the Generalized Cayley Metric



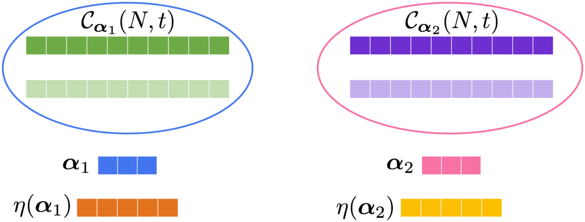
- Main idea: insert k elements $[N+1:N+k]$ into the length N permutations at positions decided by their parity check sums
  - Find an injection $\eta: \mathbb{F}_q^{4t-1} \to [N]^k$ for some $k \sim \mathcal{O}(t)$

Systematic Codes in the Generalized Cayley Metric



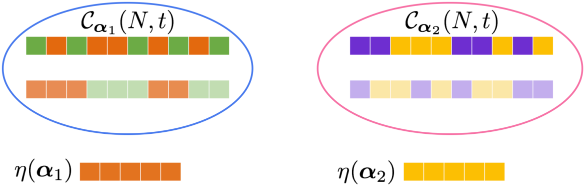
- Main idea: insert k elements $[N+1:N+k]$ into the length N permutations at positions decided by their parity check sums
  - Find an injection $\eta:\ \mathbb{F}_q^{4t-1} \to [N]^k$ for some $k \sim \mathcal{O}(t)$
- Permutations with the same parity check sum keep a distance greater than $2t$

Systematic Codes in the Generalized Cayley Metric



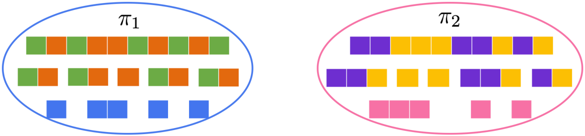
- Main idea: insert k elements $[N+1 : N+k]$ into the length N permutations at positions decided by their parity check sums
  - Find an injection $\eta : \mathbb{F}_q^{4t-1} \to [N]^k$ for some $k \sim \mathcal{O}(t)$
- Permutations with the same parity check sum keep a distance greater than $2t$
- Permutations with different parity check sums

Systematic Codes in the Generalized Cayley Metric



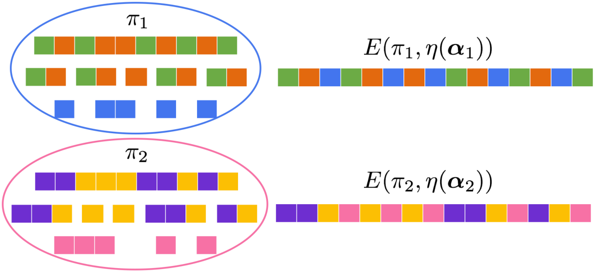
- Main idea: insert k elements $[N+1:N+k]$ into the length N permutations at positions decided by their parity check sums
  - Find an injection $\eta: \mathbb{F}_q^{4t-1} \rightarrow [N]^k$ for some $k \sim \mathcal{O}(t)$
- Permutations with the same parity check sum keep a distance greater than $2t$
- Permutations with different parity check sums
  - Each element in $\eta(\boldsymbol{\alpha})$ is identical to an element in π

Systematic Codes in the Generalized Cayley Metric



- Main idea: insert k elements $[N+1 : N+k]$ into the length N permutations at positions decided by their parity check sums
  - Find an injection $\eta : \mathbb{F}_q^{4t-1} \rightarrow [N]^k$ for some $k \sim \mathcal{O}(t)$
- Permutations with the same parity check sum keep a distance greater than $2t$
- Permutations with different parity check sums
  - Each element in $\eta(\boldsymbol{\alpha})$ is identical to an element in π
  - Insert $N+i$, $1 \leq i \leq k$ sequentially after the element in π identical to the i-th element in $\eta(\boldsymbol{\alpha})$

Systematic Codes in the Generalized Cayley Metric



- Main idea: insert k elements $[N+1 : N+k]$ into the length N permutations at positions decided by their parity check sums
  - Find an injection $\eta : \mathbb{F}_q^{4t-1} \to [N]^k$ for some $k \sim \mathcal{O}(t)$
- Permutations with the same parity check sum keep a distance greater than $2t$
- Permutations with different parity check sums
  - Each element in $\eta(\boldsymbol{\alpha})$ is identical to an element in π
  - Insert $N+i$, $1 \le i \le k$ sequentially after the element in π identical to the i-th element in $\eta(\boldsymbol{\alpha})$
  - New permutations also have distance at least $2t+1$

Extension of Permutations (Definition 5)

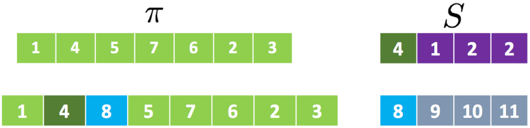
- **Extension** of π at the **extension point** s, $\pi \in \mathbb{S}_N$, $s \in [N]$:
  $E(\pi, s) \triangleq (\pi_1, \pi_2, \cdots, \pi_k = s, N+1, \pi_{k+1}, \cdots, \pi_N)$
- **Extension** of π at the **extension sequence** $S = (s_1, s_2, \cdots, s_k)$, $\pi \in \mathbb{S}_N$, $S \in [N]^k$:
  $E(\pi, S) \triangleq E(E(\cdots, E(E(\pi, s_1), s_2), \cdots, s_{k-1}), s_k)$

Extension of Permutations (Definition 5)

- **Extension** of π at the **extension point** s, $\pi \in \mathbb{S}_N$, $s \in [N]$:
  $E(\pi, s) \triangleq (\pi_1, \pi_2, \cdots, \pi_k = s, N+1, \pi_{k+1}, \cdots, \pi_N)$
- **Extension** of π at the **extension sequence** $S = (s_1, s_2, \cdots, s_k)$, $\pi \in \mathbb{S}_N$, $S \in [N]^k$:
  $E(\pi, S) \triangleq E(E(\cdots, E(E(\pi, s_1), s_2), \cdots, s_{k-1}), s_k)$

Extension of Permutations (Definition 5)

- **Extension** of π at the **extension point** s, $\pi \in \mathbb{S}_N$, $s \in [N]$:
  $E(\pi, s) \triangleq (\pi_1, \pi_2, \cdots, \pi_k = s, N+1, \pi_{k+1}, \cdots, \pi_N)$
- **Extension** of π at the **extension sequence** $S = (s_1, s_2, \cdots, s_k)$, $\pi \in \mathbb{S}_N$, $S \in [N]^k$:
  $E(\pi, S) \triangleq E(E(\cdots, E(E(\pi, s_1), s_2), \cdots, s_{k-1}), s_k)$

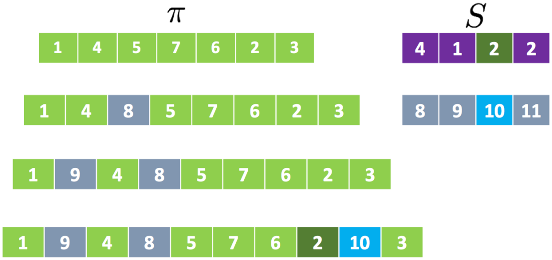


Extension of Permutations (Definition 5)

- **Extension** of π at the **extension point** s, $\pi \in \mathbb{S}_N$, $s \in [N]$:
  $E(\pi, s) \triangleq (\pi_1, \pi_2, \cdots, \pi_k = s, N+1, \pi_{k+1}, \cdots, \pi_N)$
- **Extension** of π at the **extension sequence** $S = (s_1, s_2, \cdots, s_k)$, $\pi \in \mathbb{S}_N$, $S \in [N]^k$:
  $E(\pi, S) \triangleq E(E(\cdots, E(E(\pi, s_1), s_2), \cdots, s_{k-1}), s_k)$

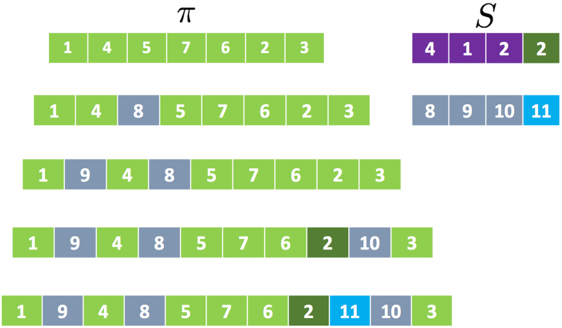
Extension of Permutations (Definition 5)

- **Extension** of π at the **extension point** s, $\pi \in \mathbb{S}_N$, $s \in [N]$:
  $E(\pi, s) \triangleq (\pi_1, \pi_2, \cdots, \pi_k = s, N+1, \pi_{k+1}, \cdots, \pi_N)$
- **Extension** of π at the **extension sequence** $S = (s_1, s_2, \cdots, s_k)$, $\pi \in \mathbb{S}_N$, $S \in [N]^k$:
  $E(\pi, S) \triangleq E(E(\cdots, E(E(\pi, s_1), s_2), \cdots, s_{k-1}), s_k)$



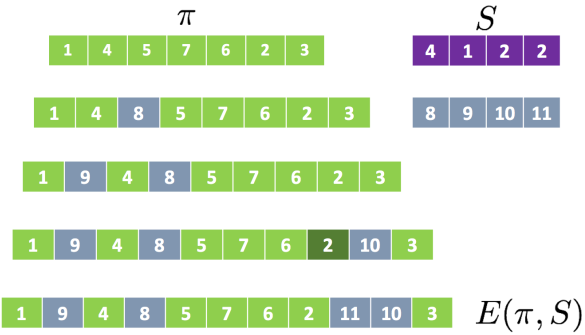
Extension of Permutations (Definition 5)

- **Extension** of π at the **extension point** s, $\pi \in \mathbb{S}_N$, $s \in [N]$:
  $E(\pi, s) \triangleq (\pi_1, \pi_2, \cdots, \pi_k = s, N+1, \pi_{k+1}, \cdots, \pi_N)$
- **Extension** of π at the **extension sequence** $S = (s_1, s_2, \cdots, s_k)$, $\pi \in \mathbb{S}_N$, $S \in [N]^k$:
  $E(\pi, S) \triangleq E(E(\cdots, E(E(\pi, s_1), s_2), \cdots, s_{k-1}), s_k)$



Extension of Permutations (Definition 5)

- **Extension** of π at the **extension point** s, $\pi \in \mathbb{S}_N$, $s \in [N]$:
  $E(\pi, s) \triangleq (\pi_1, \pi_2, \cdots, \pi_k = s, N+1, \pi_{k+1}, \cdots, \pi_N)$
- **Extension** of π at the **extension sequence** $S = (s_1, s_2, \cdots, s_k)$, $\pi \in \mathbb{S}_N$, $S \in [N]^k$:
  $E(\pi, S) \triangleq E(E(\cdots, E(E(\pi, s_1), s_2), \cdots, s_{k-1}), s_k)$



Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)

  Case 1 $k_1 = N$ or $k_2 = N$;

  Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)

  Case 1 $k_1 = N$ or $k_2 = N$;

  Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.

- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)

  Case 1 $k_1 = N$ or $k_2 = N$;

  Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.

- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
  - $d_B(\pi_1, \pi_2) = |A(\pi_1) \setminus A(\pi_2)|$, $d_B(\sigma_1, \sigma_2) = |A(\sigma_1) \setminus A(\sigma_2)|$

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)
  - Case 1 $k_1 = N$ or $k_2 = N$;
  - Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.
- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
  - $d_B(\pi_1, \pi_2) = |A(\pi_1) \setminus A(\pi_2)|$, $d_B(\sigma_1, \sigma_2) = |A(\sigma_1) \setminus A(\sigma_2)|$
  - If s_1 is a jump point

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)
  - Case 1 $k_1 = N$ or $k_2 = N$;
  - Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.
- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
  - $d_B(\pi_1, \pi_2) = |A(\pi_1) \setminus A(\pi_2)|$, $d_B(\sigma_1, \sigma_2) = |A(\sigma_1) \setminus A(\sigma_2)|$
  - If s_1 is a jump point
    - Case 1 $A(\sigma_1) \setminus A(\sigma_2) = A(\pi_1) \setminus A(\pi_2) \cup \{(s_1, N)\}$;

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)
  - Case 1 $k_1 = N$ or $k_2 = N$;
  - Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.
- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
  - $d_B(\pi_1, \pi_2) = |A(\pi_1) \setminus A(\pi_2)|$, $d_B(\sigma_1, \sigma_2) = |A(\sigma_1) \setminus A(\sigma_2)|$
  - If s_1 is a jump point
    - Case 1 $A(\sigma_1) \setminus A(\sigma_2) = A(\pi_1) \setminus A(\pi_2) \cup \{(s_1, N)\}$;
    - Case 2 $((A(\pi_1) \setminus A(\pi_2)) \setminus \{(s_1, \pi_{1,k_1+1})\}) \cup \{(s_1, N+1), (N+1, \pi_{1,k_1+1})\} \subset A(\sigma_1) \setminus A(\sigma_2)$

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)

  Case 1 $k_1 = N$ or $k_2 = N$;

  Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.

- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
  - $d_B(\pi_1, \pi_2) = |A(\pi_1) \setminus A(\pi_2)|$, $d_B(\sigma_1, \sigma_2) = |A(\sigma_1) \setminus A(\sigma_2)|$
  - If s_1 is a jump point

    Case 1 $A(\sigma_1) \setminus A(\sigma_2) = A(\pi_1) \setminus A(\pi_2) \cup \{(s_1, N)\}$;

    Case 2 $((A(\pi_1) \setminus A(\pi_2)) \setminus \{(s_1, \pi_{1,k_1+1})\}) \cup \{(s_1, N+1), (N+1, \pi_{1,k_1+1})\} \subset A(\sigma_1) \setminus A(\sigma_2)$

    $\Longrightarrow |A(\sigma_1) \setminus A(\sigma_2)| \geq |A(\pi_1) \setminus A(\pi_2)| + 1$

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)

  Case 1 $k_1 = N$ or $k_2 = N$;

  Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.

- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
  - $d_B(\pi_1, \pi_2) = |A(\pi_1) \setminus A(\pi_2)|$, $d_B(\sigma_1, \sigma_2) = |A(\sigma_1) \setminus A(\sigma_2)|$
  - If s_1 is a jump point

    Case 1 $A(\sigma_1) \setminus A(\sigma_2) = A(\pi_1) \setminus A(\pi_2) \cup \{(s_1, N)\}$;

    Case 2 $((A(\pi_1) \setminus A(\pi_2)) \setminus \{(s_1, \pi_{1,k_1+1})\}) \cup \{(s_1, N+1), (N+1, \pi_{1,k_1+1})\} \subset A(\sigma_1) \setminus A(\sigma_2)$

    $\Longrightarrow |A(\sigma_1) \setminus A(\sigma_2)| \geq |A(\pi_1) \setminus A(\pi_2)| + 1$
  - If s_1 is not a jump point

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)
  - Case 1 $k_1 = N$ or $k_2 = N$;
  - Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.
- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
  - $d_B(\pi_1, \pi_2) = |A(\pi_1) \setminus A(\pi_2)|$, $d_B(\sigma_1, \sigma_2) = |A(\sigma_1) \setminus A(\sigma_2)|$
  - If s_1 is a jump point
    - Case 1 $A(\sigma_1) \setminus A(\sigma_2) = A(\pi_1) \setminus A(\pi_2) \cup \{(s_1, N)\}$;
    - Case 2 $((A(\pi_1) \setminus A(\pi_2)) \setminus \{(s_1, \pi_{1,k_1+1})\}) \cup \{(s_1, N+1), (N+1, \pi_{1,k_1+1})\} \subset A(\sigma_1) \setminus A(\sigma_2)$

      $\Longrightarrow |A(\sigma_1) \setminus A(\sigma_2)| \geq |A(\pi_1) \setminus A(\pi_2)| + 1$
  - If s_1 is not a jump point

    $$A(\sigma_1)\setminus A(\sigma_2) = ((A(\pi_1)\setminus A(\pi_2))\setminus\{(s_1, \pi_{1,k_1+1})\})\cup\{(s_1, N+1)\}$$

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)

  Case 1 $k_1 = N$ or $k_2 = N$;

  Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.

- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
  - $d_B(\pi_1, \pi_2) = |A(\pi_1) \setminus A(\pi_2)|$, $d_B(\sigma_1, \sigma_2) = |A(\sigma_1) \setminus A(\sigma_2)|$
  - If s_1 is a jump point

    Case 1 $A(\sigma_1) \setminus A(\sigma_2) = A(\pi_1) \setminus A(\pi_2) \cup \{(s_1, N)\}$;

    Case 2 $((A(\pi_1) \setminus A(\pi_2)) \setminus \{(s_1, \pi_{1,k_1+1})\}) \cup \{(s_1, N+1), (N+1, \pi_{1,k_1+1})\} \subset A(\sigma_1) \setminus A(\sigma_2)$

    $\Longrightarrow |A(\sigma_1) \setminus A(\sigma_2)| \geq |A(\pi_1) \setminus A(\pi_2)| + 1$
  - If s_1 is not a jump point

    $A(\sigma_1) \setminus A(\sigma_2) = ((A(\pi_1) \setminus A(\pi_2)) \setminus \{(s_1, \pi_{1,k_1+1})\}) \cup \{(s_1, N+1)\}$

    $\Longrightarrow |A(\sigma_1) \setminus A(\sigma_2)| = |A(\pi_1) \setminus A(\pi_2)|$

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)
  - Case 1 $k_1 = N$ or $k_2 = N$;
  - Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.
- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
- m is a **Jump index** of $E(\pi_1, S_1)$ and $E(\pi_2, S_2)$ if s_1 is a jump point of $E(E(\pi_1, (s_{1,1}, s_{1,2}, \cdots, s_{1,m-1})), s_{1,m})$ with respect to $E(E(\pi_2, (s_{2,1}, s_{2,2}, \cdots, s_{2,m-1})), s_{2,m})$

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)

  Case 1 $k_1 = N$ or $k_2 = N$;

  Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.

- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
- m is a **Jump index** of $E(\pi_1, S_1)$ and $E(\pi_2, S_2)$ if s_1 is a jump point of $E(E(\pi_1, (s_{1,1}, s_{1,2}, \cdots, s_{1,m-1})), s_{1,m})$ with respect to $E(E(\pi_2, (s_{2,1}, s_{2,2}, \cdots, s_{2,m-1})), s_{2,m})$

  Note: d_B strictly increases when inserting $N + m$ for those jump points m

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)
  - Case 1 $k_1 = N$ or $k_2 = N$;
  - Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.
- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
- m is a **Jump index** of $E(\pi_1, S_1)$ and $E(\pi_2, S_2)$ if s_1 is a jump point of $E(E(\pi_1, (s_{1,1}, s_{1,2}, \cdots, s_{1,m-1})), s_{1,m})$ with respect to $E(E(\pi_2, (s_{2,1}, s_{2,2}, \cdots, s_{2,m-1})), s_{2,m})$
  - Note: d_B strictly increases when inserting $N + m$ for those jump points m
- **Jump set** $F(\pi_1, \pi_2, S_1, S_2)$: the set of all jump indices of $E(\pi_1, S_1)$ and $E(\pi_2, S_2)$

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)

  Case 1 $k_1 = N$ or $k_2 = N$;

  Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.

- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
- m is a **Jump index** of $E(\pi_1, S_1)$ and $E(\pi_2, S_2)$ if s_1 is a jump point of $E(E(\pi_1, (s_{1,1}, s_{1,2}, \cdots, s_{1,m-1})), s_{1,m})$ with respect to $E(E(\pi_2, (s_{2,1}, s_{2,2}, \cdots, s_{2,m-1})), s_{2,m})$

  Note: d_B strictly increases when inserting $N + m$ for those jump points m

- **Jump set** $F(\pi_1, \pi_2, S_1, S_2)$: the set of all jump indices of $E(\pi_1, S_1)$ and $E(\pi_2, S_2)$

  Note: d_B strictly increases when inserting $N + m$ for all $m \in F(\pi_1, \pi_2, S_1, S_2)$

Jump Points of Extensions

- s_1 is **Jump point** of $\sigma_1 = E(\pi_1, s_1)$ with respsect to $\sigma_2 = E(\pi_2, s_2)$ if (suppose $\pi_{1,k_1} = s_1$ and $\pi_{2,k_2} = s_2$)
  - Case 1 $k_1 = N$ or $k_2 = N$;
  - Case 2 $k_1, k_2 < N$, and $\pi_{1,k_1+1} \neq \pi_{2,k_2+1}$.
- $d_B(E(\pi_1, s_1), E(\pi_2, s_2)) > d_B(\pi_1, \pi_2)$ iff s_1 is a jump point (**Lemma 9**)
- m is a **Jump index** of $E(\pi_1, S_1)$ and $E(\pi_2, S_2)$ if s_1 is a jump point of $E(E(\pi_1, (s_{1,1}, s_{1,2}, \cdots, s_{1,m-1})), s_{1,m})$ with respect to $E(E(\pi_2, (s_{2,1}, s_{2,2}, \cdots, s_{2,m-1})), s_{2,m})$

  Note: d_B strictly increases when inserting $N + m$ for those jump points m
- **Jump set** $F(\pi_1, \pi_2, S_1, S_2)$: the set of all jump indices of $E(\pi_1, S_1)$ and $E(\pi_2, S_2)$

  Note: d_B strictly increases when inserting $N + m$ for all $m \in F(\pi_1, \pi_2, S_1, S_2)$

  $\Longrightarrow$ $d_B(\sigma_1, \sigma_2) \geq d_B(\pi_1, \pi_2) + |F(\pi_1, \pi_2, S_1, S_2)|$ (**Remark 5**)

Hamming Set and t-Auxiliary Set

- **Hamming set** of $\mathbf{v}_1$ with respect to $\mathbf{v}_2$, $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{N}^k$, $k \in \mathbb{N}$:
  $H(\mathbf{v}_1, \mathbf{v}_2) \triangleq \{v_{1,m} | v_{1,m} \neq v_{2,m}, m \in [k]\}$

Hamming Set and t-Auxiliary Set

- **Hamming set** of $\mathbf{v}_1$ with respect to $\mathbf{v}_2$, $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{N}^k$, $k \in \mathbb{N}$: $H(\mathbf{v}_1, \mathbf{v}_2) \triangleq \{v_{1,m} | v_{1,m} \neq v_{2,m}, m \in [k]\}$

  Note: Cardinality of Hamming sets induces a metric, i.e., $|H(\mathbf{v}_1, \mathbf{v}_3)| \leq |H(\mathbf{v}_1, \mathbf{v}_2)| + |H(\mathbf{v}_2, \mathbf{v}_3)|$

Hamming Set and t-Auxiliary Set

- **Hamming set** of $\mathbf{v}_1$ with respect to $\mathbf{v}_2$, $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{N}^k$, $k \in \mathbb{N}$:
  $H(\mathbf{v}_1, \mathbf{v}_2) \triangleq \{v_{1,m} | v_{1,m} \neq v_{2,m}, m \in [k]\}$

  Note: Cardinality of Hamming sets induces a metric, i.e.,
  $|H(\mathbf{v}_1, \mathbf{v}_3)| \leq |H(\mathbf{v}_1, \mathbf{v}_2)| + |H(\mathbf{v}_2, \mathbf{v}_3)|$
- $d_B(E(\pi_1, S_1), E(\pi_2, S_2)) \geq |H(S_1, S_2)|$ **(Lemma 10)**

Hamming Set and t-Auxiliary Set

- **Hamming set** of $\mathbf{v}_1$ with respect to $\mathbf{v}_2$, $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{N}^k$, $k \in \mathbb{N}$: $H(\mathbf{v}_1, \mathbf{v}_2) \triangleq \{v_{1,m} | v_{1,m} \neq v_{2,m}, m \in [k]\}$

  Note: Cardinality of Hamming sets induces a metric, i.e.,
  $|H(\mathbf{v}_1, \mathbf{v}_3)| \leq |H(\mathbf{v}_1, \mathbf{v}_2)| + |H(\mathbf{v}_2, \mathbf{v}_3)|$

- $d_B(E(\pi_1, S_1), E(\pi_2, S_2)) \geq |H(S_1, S_2)|$ **(Lemma 10)**

  Proof $\forall v \in H(S_1, S_2)$

Hamming Set and t-Auxiliary Set

- **Hamming set** of $\mathbf{v}_1$ with respect to $\mathbf{v}_2$, $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{N}^k$, $k \in \mathbb{N}$:
  $H(\mathbf{v}_1, \mathbf{v}_2) \triangleq \{v_{1,m} | v_{1,m} \neq v_{2,m}, m \in [k]\}$

  Note: Cardinality of Hamming sets induces a metric, i.e.,
  $|H(\mathbf{v}_1, \mathbf{v}_3)| \leq |H(\mathbf{v}_1, \mathbf{v}_2)| + |H(\mathbf{v}_2, \mathbf{v}_3)|$

- $d_B(E(\pi_1, S_1), E(\pi_2, S_2)) \geq |H(S_1, S_2)|$ **(Lemma 10)**

  Proof $\forall v \in H(S_1, S_2)$

  Case 1 $v \in F(\pi_1, \pi_2, S_1, S_2)$
  $|H(S_1, S_2) \cap F(\pi_1, \pi_2, S_1, S_2)| \leq |F(\pi_1, \pi_2, S_1, S_2)|$

Hamming Set and t-Auxiliary Set

- **Hamming set** of $\mathbf{v}_1$ with respect to $\mathbf{v}_2$, $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{N}^k$, $k \in \mathbb{N}$: $H(\mathbf{v}_1, \mathbf{v}_2) \triangleq \{v_{1,m} | v_{1,m} \neq v_{2,m}, m \in [k]\}$

  Note: Cardinality of Hamming sets induces a metric, i.e., $|H(\mathbf{v}_1, \mathbf{v}_3)| \leq |H(\mathbf{v}_1, \mathbf{v}_2)| + |H(\mathbf{v}_2, \mathbf{v}_3)|$

- $d_B(E(\pi_1, S_1), E(\pi_2, S_2)) \geq |H(S_1, S_2)|$ **(Lemma 10)**

  Proof $\forall v \in H(S_1, S_2)$

  Case 1 $v \in F(\pi_1, \pi_2, S_1, S_2)$
  $|H(S_1, S_2) \cap F(\pi_1, \pi_2, S_1, S_2)| \leq |F(\pi_1, \pi_2, S_1, S_2)|$

  Case 2 $v \notin F(\pi_1, \pi_2, S_1, S_2)$
  $\Longrightarrow \exists j \in [N]$ s.t. $(v, j) \in A(\pi_1) \setminus A(\pi_2)$
  $\Longrightarrow |H(S_1, S_2) \setminus F(\pi_1, \pi_2, S_1, S_2)| \leq A(\pi_1) \setminus A(\pi_2) = d_B(\pi_1, \pi_2)$

Hamming Set and t-Auxiliary Set

- **Hamming set** of $\mathbf{v}_1$ with respect to $\mathbf{v}_2$, $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{N}^k$, $k \in \mathbb{N}$:
  $H(\mathbf{v}_1, \mathbf{v}_2) \triangleq \{v_{1,m} | v_{1,m} \neq v_{2,m}, m \in [k]\}$

  Note: Cardinality of Hamming sets induces a metric, i.e.,
  $|H(\mathbf{v}_1, \mathbf{v}_3)| \leq |H(\mathbf{v}_1, \mathbf{v}_2)| + |H(\mathbf{v}_2, \mathbf{v}_3)|$

- $d_B(E(\pi_1, S_1), E(\pi_2, S_2)) \geq |H(S_1, S_2)|$ **(Lemma 10)**

  Proof $\forall v \in H(S_1, S_2)$

  Case 1 $v \in F(\pi_1, \pi_2, S_1, S_2)$
  $|H(S_1, S_2) \cap F(\pi_1, \pi_2, S_1, S_2)| \leq |F(\pi_1, \pi_2, S_1, S_2)|$

  Case 2 $v \notin F(\pi_1, \pi_2, S_1, S_2)$
  $\implies \exists j \in [N] \text{ s.t. } (v, j) \in A(\pi_1) \setminus A(\pi_2)$
  $\implies |H(S_1, S_2) \setminus F(\pi_1, \pi_2, S_1, S_2)| \leq A(\pi_1) \setminus A(\pi_2) = d_B(\pi_1, \pi_2)$

  $\implies$ $d_B(\sigma_1, \sigma_2) \geq d_B(\pi_1, \pi_2) + |F(\pi_1, \pi_2, S_1, S_2)| \geq |H(S_1, S_2)|$

Hamming Set and t-Auxiliary Set

- **Hamming set** of $\mathbf{v}_1$ with respect to $\mathbf{v}_2$, $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{N}^k$, $k \in \mathbb{N}$:
  $H(\mathbf{v}_1, \mathbf{v}_2) \triangleq \{v_{1,m} | v_{1,m} \neq v_{2,m}, m \in [k]\}$

  Note: Cardinality of Hamming sets induces a metric, i.e.,
  $|H(\mathbf{v}_1, \mathbf{v}_3)| \leq |H(\mathbf{v}_1, \mathbf{v}_2)| + |H(\mathbf{v}_2, \mathbf{v}_3)|$

- $d_B(E(\pi_1, S_1), E(\pi_2, S_2)) \geq |H(S_1, S_2)|$ **(Lemma 10)**

  Proof $\forall v \in H(S_1, S_2)$

  Case 1 $v \in F(\pi_1, \pi_2, S_1, S_2)$
  $|H(S_1, S_2) \cap F(\pi_1, \pi_2, S_1, S_2)| \leq |F(\pi_1, \pi_2, S_1, S_2)|$

  Case 2 $v \notin F(\pi_1, \pi_2, S_1, S_2)$
  $\Longrightarrow \exists j \in [N]$ s.t. $(v, j) \in A(\pi_1) \setminus A(\pi_2)$
  $\Longrightarrow |H(S_1, S_2) \setminus F(\pi_1, \pi_2, S_1, S_2)| \leq A(\pi_1) \setminus A(\pi_2) = d_B(\pi_1, \pi_2)$

  $\Longrightarrow$ $d_B(\sigma_1, \sigma_2) \geq d_B(\pi_1, \pi_2) + |F(\pi_1, \pi_2, S_1, S_2)| \geq |H(S_1, S_2)|$

- $\mathcal{A}(N, K, t) \subset [N]^K$ is called an t-**Auxiliary Set** if:
  $\forall \mathbf{c}_1 \neq \mathbf{c}_2 \in \mathcal{A}(N, K, t)$, $|H(\mathbf{c}_1, \mathbf{c}_2)| \geq 2t + 1$

Construction: Encoding

Step 1 Given a t-auxiliary set $\mathcal{A}(N, K, t)$ with cardinality that is no less than q^{4t-1}

Construction: Encoding

Step 1 Given a t-auxiliary set $\mathcal{A}(N, K, t)$ with cardinality that is no less than q^{4t-1}

Step 2 Find an injection $\varphi: \ q^{4t-1} \rightarrow \mathcal{A}(N, K, t)$, where q is a prime number such that $N^2 - N < q < 2(N^2 - N)$

Construction: Encoding

Step 1 Given a t-auxiliary set $\mathcal{A}(N, K, t)$ with cardinality that is no less than q^{4t-1}

Step 2 Find an injection $\varphi: \ q^{4t-1} \rightarrow \mathcal{A}(N, K, t)$, where q is a prime number such that $N^2 - N < q < 2(N^2 - N)$

Step 3 Compute the set $\mathcal{C}_B^{\mathrm{sys}}(N, K, t) = \{E(\pi, \varphi \circ \alpha(\pi)) | \pi \in \mathbb{S}_N\}$

Construction: Encoding

Step 1 Given a t-auxiliary set $\mathcal{A}(N, K, t)$ with cardinality that is no less than q^{4t-1}

Step 2 Find an injection $\varphi: \; q^{4t-1} \to \mathcal{A}(N, K, t)$, where q is a prime number such that $N^2 - N < q < 2(N^2 - N)$

Step 3 Compute the set $\mathcal{C}_B^{\text{sys}}(N, K, t) = \{E(\pi, \varphi \circ \alpha(\pi)) | \pi \in \mathbb{S}_N\}$

Theorem 4 $\mathcal{C}_B^{\text{sys}}(N, K, t)$ is a systematic t-block permutation code

Construction: Encoding

Step 1 Given a t-auxiliary set $\mathcal{A}(N, K, t)$ with cardinality that is no less than q^{4t-1}

Step 2 Find an injection $\varphi: \; q^{4t-1} \to \mathcal{A}(N, K, t)$, where q is a prime number such that $N^2 - N < q < 2(N^2 - N)$

Step 3 Compute the set $\mathcal{C}_B^{\mathrm{sys}}(N, K, t) = \{E(\pi, \varphi \circ \alpha(\pi)) | \pi \in \mathbb{S}_N\}$

Theorem 4 $\mathcal{C}_B^{\mathrm{sys}}(N, K, t)$ is a systematic t-block permutation code

For any $\pi_1 \neq \pi_2$, Let $\sigma_1 = E(\pi_1, \varphi(\alpha_1)), \sigma_2 = E(\pi_2, \varphi(\alpha_2))$

Construction: Encoding

Step 1 Given a t-auxiliary set $\mathcal{A}(N, K, t)$ with cardinality that is no less than q^{4t-1}

Step 2 Find an injection $\varphi: \ q^{4t-1} \rightarrow \mathcal{A}(N, K, t)$, where q is a prime number such that $N^2 - N < q < 2(N^2 - N)$

Step 3 Compute the set $\mathcal{C}_B^{\text{sys}}(N, K, t) = \{E(\pi, \varphi \circ \alpha(\pi)) | \pi \in \mathbb{S}_N\}$

Theorem 4 $\mathcal{C}_B^{\text{sys}}(N, K, t)$ is a systematic t-block permutation code

For any $\pi_1 \neq \pi_2$, Let $\sigma_1 = E(\pi_1, \varphi(\alpha_1)), \sigma_2 = E(\pi_2, \varphi(\alpha_2))$

Case 1 $\alpha(\pi_1) = \alpha(\pi_2) \Longrightarrow d_B(\sigma_1, \sigma_2) \geq d_B(\pi_1, \pi_2) \geq 2t+1$

Construction: Encoding

Step 1 Given a t-auxiliary set $\mathcal{A}(N,K,t)$ with cardinality that is no less than q^{4t-1}

Step 2 Find an injection $\varphi:\ q^{4t-1} \to \mathcal{A}(N,K,t)$, where q is a prime number such that $N^2 - N < q < 2(N^2 - N)$

Step 3 Compute the set $\mathcal{C}_B^{\mathrm{sys}}(N,K,t) = \{E(\pi, \varphi \circ \alpha(\pi)) | \pi \in \mathbb{S}_N\}$

Theorem 4 $\mathcal{C}_B^{\mathrm{sys}}(N,K,t)$ is a systematic t-block permutation code

For any $\pi_1 \neq \pi_2$, Let $\sigma_1 = E(\pi_1, \varphi(\alpha_1)), \sigma_2 = E(\pi_2, \varphi(\alpha_2))$

Case 1 $\alpha(\pi_1) = \alpha(\pi_2) \Longrightarrow d_B(\sigma_1, \sigma_2) \geq d_B(\pi_1, \pi_2) \geq 2t+1$

Case 2 $\alpha(\pi_1) \neq \alpha(\pi_2) \Longrightarrow S_1 = \varphi(\alpha_1) \neq S_2 = \varphi(\alpha_2)) \Longrightarrow$
$d_B(\sigma_1, \sigma_2) \geq H(S_1, S_2) \geq 2t+1$

Construction: Encoding

Step 1 Given a t-auxiliary set $\mathcal{A}(N, K, t)$ with cardinality that is no less than q^{4t-1}

Step 2 Find an injection $\varphi: \ q^{4t-1} \to \mathcal{A}(N, K, t)$, where q is a prime number such that $N^2 - N < q < 2(N^2 - N)$

Step 3 Compute the set $\mathcal{C}_B^{\mathrm{sys}}(N, K, t) = \{E(\pi, \varphi \circ \alpha(\pi)) | \pi \in \mathbb{S}_N\}$

Theorem 4 $\mathcal{C}_B^{\mathrm{sys}}(N, K, t)$ is a systematic t-block permutation code

For any $\pi_1 \neq \pi_2$, Let $\sigma_1 = E(\pi_1, \varphi(\alpha_1)), \sigma_2 = E(\pi_2, \varphi(\alpha_2))$

Case 1 $\alpha(\pi_1) = \alpha(\pi_2) \implies d_B(\sigma_1, \sigma_2) \geq d_B(\pi_1, \pi_2) \geq 2t+1$

Case 2 $\alpha(\pi_1) \neq \alpha(\pi_2) \implies S_1 = \varphi(\alpha_1) \neq S_2 = \varphi(\alpha_2)) \implies d_B(\sigma_1, \sigma_2) \geq H(S_1, S_2) \geq 2t+1$

$\implies d_B(\sigma_1, \sigma_2) \geq 2t+1$

Construction: Encoding

Step 1 Given a t-auxiliary set $\mathcal{A}(N, K, t)$ with cardinality that is no less than q^{4t-1}

Step 2 Find an injection $\varphi: \ q^{4t-1} \to \mathcal{A}(N, K, t)$, where q is a prime number such that $N^2 - N < q < 2(N^2 - N)$

Step 3 Compute the set $\mathcal{C}_B^{\text{sys}}(N, K, t) = \{E(\pi, \varphi \circ \alpha(\pi)) | \pi \in \mathbb{S}_N\}$

Theorem 4 $\mathcal{C}_B^{\text{sys}}(N, K, t)$ is a systematic t-block permutation code

For any $\pi_1 \neq \pi_2$, Let $\sigma_1 = E(\pi_1, \varphi(\alpha_1)), \sigma_2 = E(\pi_2, \varphi(\alpha_2))$

Case 1 $\alpha(\pi_1) = \alpha(\pi_2) \implies d_B(\sigma_1, \sigma_2) \geq d_B(\pi_1, \pi_2) \geq 2t+1$

Case 2 $\alpha(\pi_1) \neq \alpha(\pi_2) \implies S_1 = \varphi(\alpha_1) \neq S_2 = \varphi(\alpha_2)) \implies$
$d_B(\sigma_1, \sigma_2) \geq H(S_1, S_2) \geq 2t + 1$

$\implies d_B(\sigma_1, \sigma_2) \geq 2t + 1$

Note Only need to construct t-auxiliary set $\mathcal{A}(N, K, t)$ with cardinality that is no less than q^{4t-1} (will introduce later)

Construction: Decoding

Channel Send sents $\sigma = E(\pi, S = \varphi \circ \alpha(\pi))$ and the receiver receives σ', $d_B(\sigma, \sigma') \leq t$

Construction: Decoding

Channel Send sents $\sigma = E(\pi, S = \varphi \circ \alpha(\pi))$ and the receiver receives σ', $d_B(\sigma, \sigma') \leq t$

Step 1 Find $\pi' \in \mathbb{S}_N, S' \in [N]^K$ such that $\sigma' = E(\pi', S')$

Construction: Decoding

Channel Send sents $\sigma = E(\pi, S = \varphi \circ \alpha(\pi))$ and the receiver receives σ', $d_B(\sigma, \sigma') \leq t$

Step 1 Find $\pi' \in \mathbb{S}_N, S' \in [N]^K$ such that $\sigma' = E(\pi', S')$

Lemma 11 $H(S, S') \leq t$

Construction: Decoding

Channel Send sents $\sigma = E(\pi, S = \varphi \circ \alpha(\pi))$ and the receiver receives σ', $d_B(\sigma, \sigma') \leq t$

Step 1 Find $\pi' \in \mathbb{S}_N, S' \in [N]^K$ such that $\sigma' = E(\pi', S')$

Lemma 11 $H(S, S') \leq t$

$\implies$ S' can be decoded from S':

Construction: Decoding

Channel Send sents $\sigma = E(\pi, S = \varphi \circ \alpha(\pi))$ and the receiver receives σ', $d_B(\sigma, \sigma') \leq t$

Step 1 Find $\pi' \in \mathbb{S}_N, S' \in [N]^K$ such that $\sigma' = E(\pi', S')$

Lemma 11 $H(S, S') \leq t$

$\Longrightarrow$ S' can be decoded from S':

1 Cardinality of the Hamming set of elements from t-auxiliary set is at least $2t + 1$

Construction: Decoding

Channel Send sents $\sigma = E(\pi, S = \varphi \circ \alpha(\pi))$ and the receiver receives σ', $d_B(\sigma, \sigma') \leq t$

Step 1 Find $\pi' \in \mathbb{S}_N, S' \in [N]^K$ such that $\sigma' = E(\pi', S')$

Lemma 11 $H(S, S') \leq t$

$\Longrightarrow$ S' can be decoded from S':

1 Cardinality of the Hamming set of elements from t-auxiliary set is at least $2t + 1$

2 Cardinality of Hamming induces a metric

Construction: Decoding

Channel Send sents $\sigma = E(\pi, S = \varphi \circ \alpha(\pi))$ and the receiver receives σ', $d_B(\sigma, \sigma') \leq t$

Step 1 Find $\pi' \in \mathbb{S}_N, S' \in [N]^K$ such that $\sigma' = E(\pi', S')$

Lemma 11 $H(S, S') \leq t$

$\Longrightarrow$ S' can be decoded from S':

1 Cardinality of the Hamming set of elements from t-auxiliary set is at least $2t + 1$

2 Cardinality of Hamming induces a metric

Step 2 Decode S from S'

Construction: Decoding

Channel Send sents $\sigma = E(\pi, S = \varphi \circ \alpha(\pi))$ and the receiver receives σ', $d_B(\sigma, \sigma') \leq t$

Step 1 Find $\pi' \in \mathbb{S}_N, S' \in [N]^K$ such that $\sigma' = E(\pi', S')$

Lemma 11 $H(S, S') \leq t$

$\Longrightarrow$ S' can be decoded from S':

1. Cardinality of the Hamming set of elements from t-auxiliary set is at least $2t + 1$
2. Cardinality of Hamming induces a metric

Step 2 Decode S from S'

Step 3 Compute parity check sum $\alpha(\pi) = \varphi^{-1}(S)$ from S

Construction: Decoding

Channel Send sents $\sigma = E(\pi, S = \varphi \circ \alpha(\pi))$ and the receiver receives σ', $d_B(\sigma, \sigma') \leq t$

Step 1 Find $\pi' \in \mathbb{S}_N, S' \in [N]^K$ such that $\sigma' = E(\pi', S')$

Lemma 11 $H(S, S') \leq t$

$\Longrightarrow$ S' can be decoded from S':

1. Cardinality of the Hamming set of elements from t-auxiliary set is at least $2t + 1$
2. Cardinality of Hamming induces a metric

Step 2 Decode S from S'

Step 3 Compute parity check sum $\alpha(\pi) = \varphi^{-1}(S)$ from S

Step 4 $d_B(\pi, \pi') \leq d_B(\sigma, \sigma') \leq t$, decode π from π' and $\alpha(\pi)$ using **Theorem 3**

Construction: t-Auxiliary Set

Lemma 14 For all $k, N \in \mathbb{N}^*$, $k > 3$, $N > k^2$, consider an arbitrary subset $Y \subset [k]$, where $|Y| = M < k$, $Y = \{i_1, i_2, \cdots, i_M\}$, then $\mathrm{LCM}(N + i_1, N + i_2, \cdots, N + i_M) > N^{M - \frac{k}{2}}$

Construction: t-Auxiliary Set

Lemma 14 For all $k, N \in \mathbb{N}^*$, $k > 3$, $N > k^2$, consider an arbitrary subset $Y \subset [k]$, where $|Y| = M < k$, $Y = \{i_1, i_2, \cdots, i_M\}$, then $\mathrm{LCM}\left(N + i_1, N + i_2, \cdots, N + i_M\right) > N^{M - \frac{k}{2}}$

Construction For all $N, k, t \in \mathbb{N}^*$, $k \geq 28t$, $k < \lfloor \sqrt{N} - \frac{1}{2} \rfloor$, $\boldsymbol{x} = \left(x_1, x_2, \cdots, x_{4t-1}\right) \in [q]^{4t-1}$

Construction: t-Auxiliary Set

Lemma 14 For all $k, N \in \mathbb{N}^*$, $k > 3$, $N > k^2$, consider an arbitrary subset $Y \subset [k]$, where $|Y| = M < k$, $Y = \{i_1, i_2, \cdots, i_M\}$, then $\mathrm{LCM}\left(N + i_1, N + i_2, \cdots, N + i_M\right) > N^{M - \frac{k}{2}}$

Construction For all $N, k, t \in \mathbb{N}^*$, $k \geq 28t$, $k < \lfloor \sqrt{N} - \frac{1}{2} \rfloor$, $\boldsymbol{x} = (x_1, x_2, \cdots, x_{4t-1}) \in [q]^{4t-1}$

Step 1 Compute $\boldsymbol{\beta}(\boldsymbol{x}) = (\beta_1, \beta_2, \cdots, \beta_k)$, where $\beta_i = \sum_{i=1}^{4t-1} x_i q^{i-1} \mod (N + i)$

Construction: t-Auxiliary Set

Lemma 14 For all $k, N \in \mathbb{N}^*$, $k > 3$, $N > k^2$, consider an arbitrary subset $Y \subset [k]$, where $|Y| = M < k$, $Y = \{i_1, i_2, \cdots, i_M\}$, then $\mathrm{LCM}\left(N + i_1, N + i_2, \cdots, N + i_M\right) > N^{M - \frac{k}{2}}$

Construction For all $N, k, t \in \mathbb{N}^*$, $k \geq 28t$, $k < \lfloor \sqrt{N} - \frac{1}{2} \rfloor$, $\boldsymbol{x} = (x_1, x_2, \cdots, x_{4t-1}) \in [q]^{4t-1}$

Step 1 Compute $\boldsymbol{\beta}(\boldsymbol{x}) = (\beta_1, \beta_2, \cdots, \beta_k)$, where $\beta_i = \sum_{i=1}^{4t-1} x_i q^{i-1} \mod (N + i)$

Theorem 6 $\forall\ \boldsymbol{x}_1, \boldsymbol{x}_2 \in [q]^d$, $\boldsymbol{x}_1 \neq \boldsymbol{x}_2$, $d_H(\boldsymbol{\beta}(\boldsymbol{x}_1), \boldsymbol{\beta}(\boldsymbol{x}_2)) > 2t$

Construction: t-Auxiliary Set

Lemma 14 For all $k, N \in \mathbb{N}^*$, $k > 3$, $N > k^2$, consider an arbitrary subset $Y \subset [k]$, where $|Y| = M < k$, $Y = \{i_1, i_2, \cdots, i_M\}$, then $\mathrm{LCM}\,(N + i_1, N + i_2, \cdots, N + i_M) > N^{M - \frac{k}{2}}$

Construction For all $N, k, t \in \mathbb{N}^*$, $k \geq 28t$, $k < \lfloor \sqrt{N} - \frac{1}{2} \rfloor$, $\boldsymbol{x} = (x_1, x_2, \cdots, x_{4t-1}) \in [q]^{4t-1}$

Step 1 Compute $\boldsymbol{\beta}(\boldsymbol{x}) = (\beta_1, \beta_2, \cdots, \beta_k)$, where $\beta_i = \sum_{i=1}^{4t-1} x_i q^{i-1} \mod (N + i)$

Theorem 6 $\forall\ \boldsymbol{x}_1, \boldsymbol{x}_2 \in [q]^d$, $\boldsymbol{x}_1 \neq \boldsymbol{x}_2$, $d_H(\boldsymbol{\beta}(\boldsymbol{x}_1), \boldsymbol{\beta}(\boldsymbol{x}_2)) > 2t$

Step 2 Compute $\mathbf{c} = (c_1, c_2, \cdots, c_{2k})$, where $(c_{2i-1}, c_{2i}) = 1 + (i-1)\lfloor \frac{N}{k} \rfloor + (e_{2i-1}, e_{2i})$, (e_{2i-1}, e_{2i}) is the $\lfloor \frac{N}{k} \rfloor$-ary representation of β_i

Construction: t-Auxiliary Set

Lemma 14 For all $k, N \in \mathbb{N}^*$, $k > 3$, $N > k^2$, consider an arbitrary subset $Y \subset [k]$, where $|Y| = M < k$, $Y = \{i_1, i_2, \cdots, i_M\}$, then $\mathrm{LCM}\,(N + i_1, N + i_2, \cdots, N + i_M) > N^{M - \frac{k}{2}}$

Construction For all $N, k, t \in \mathbb{N}^*$, $k \geq 28t$, $k < \lfloor \sqrt{N} - \frac{1}{2} \rfloor$, $\boldsymbol{x} = (x_1, x_2, \cdots, x_{4t-1}) \in [q]^{4t-1}$

Step 1 Compute $\boldsymbol{\beta}(\boldsymbol{x}) = (\beta_1, \beta_2, \cdots, \beta_k)$, where $\beta_i = \sum_{i=1}^{4t-1} x_i q^{i-1} \mod (N + i)$

Theorem 6 $\forall\ \boldsymbol{x}_1, \boldsymbol{x}_2 \in [q]^d$, $\boldsymbol{x}_1 \neq \boldsymbol{x}_2$, $d_H(\boldsymbol{\beta}(\boldsymbol{x}_1), \boldsymbol{\beta}(\boldsymbol{x}_2)) > 2t$

Step 2 Compute $\mathbf{c} = (c_1, c_2, \cdots, c_{2k})$, where $(c_{2i-1}, c_{2i}) = 1 + (i-1)\lfloor \frac{N}{k} \rfloor + (e_{2i-1}, e_{2i})$, (e_{2i-1}, e_{2i}) is the $\lfloor \frac{N}{k} \rfloor$-ary representation of β_i

Theorem 7 $\mathcal{A}(N, 2k, t) = \{\mathbf{c}(\mathbf{x}) : \ \mathbf{x} \in [q]^{4t-1}\}$ is a t-auxiliary set with cardinality q^{4t-1}

Construction: t-Auxiliary Set

Lemma 14 For all $k, N \in \mathbb{N}^*$, $k > 3$, $N > k^2$, consider an arbitrary subset $Y \subset [k]$, where $|Y| = M < k$, $Y = \{i_1, i_2, \cdots, i_M\}$, then $\mathrm{LCM}\,(N + i_1, N + i_2, \cdots, N + i_M) > N^{M - \frac{k}{2}}$

Construction For all $N, k, t \in \mathbb{N}^*$, $k \geq 28t$, $k < \lfloor \sqrt{N} - \frac{1}{2} \rfloor$, $\boldsymbol{x} = (x_1, x_2, \cdots, x_{4t-1}) \in [q]^{4t-1}$

Step 1 Compute $\boldsymbol{\beta}(\boldsymbol{x}) = (\beta_1, \beta_2, \cdots, \beta_k)$, where $\beta_i = \sum_{i=1}^{4t-1} x_i q^{i-1} \mod (N + i)$

Theorem 6 $\forall\ \boldsymbol{x}_1, \boldsymbol{x}_2 \in [q]^d$, $\boldsymbol{x}_1 \neq \boldsymbol{x}_2$, $d_H(\boldsymbol{\beta}(\boldsymbol{x}_1), \boldsymbol{\beta}(\boldsymbol{x}_2)) > 2t$

Step 2 Compute $\mathbf{c} = (c_1, c_2, \cdots, c_{2k})$, where $(c_{2i-1}, c_{2i}) = 1 + (i-1)\lfloor \frac{N}{k} \rfloor + (e_{2i-1}, e_{2i})$, (e_{2i-1}, e_{2i}) is the $\lfloor \frac{N}{k} \rfloor$-ary representation of β_i

Theorem 7 $\mathcal{A}(N, 2k, t) = \{\mathbf{c}(\mathbf{x}) :\ \mathbf{x} \in [q]^{4t-1}\}$ is a t-auxiliary set with cardinality q^{4t-1}

Lemma 16 Code constructed by **Theorem 4** using $\mathcal{A}(N, 56t, t)$ is systematic and order-optimal

Outline

Conclusion and Future Work

- Conclusion

Conclusion and Future Work

- Conclusion
  - We derive the lower and the upper bounds of the optimal rate of the permutation codes in the generalized Cayley metric

Conclusion and Future Work

- Conclusion
  - We derive the lower and the upper bounds of the optimal rate of the permutation codes in the generalized Cayley metric
  - We provide a coding scheme of order-optimal codes

Conclusion and Future Work

- Conclusion
  - We derive the lower and the upper bounds of the optimal rate of the permutation codes in the generalized Cayley metric
  - We provide a coding scheme of order-optimal codes
  - We prove that our code is more rate efficient than the existing permutation codes based on interleaving

Conclusion and Future Work

- Conclusion
  - We derive the lower and the upper bounds of the optimal rate of the permutation codes in the generalized Cayley metric
  - We provide a coding scheme of order-optimal codes
  - We prove that our code is more rate efficient than the existing permutation codes based on interleaving
  - We extend our result by developing a construction of systematic permutation codes in this metric that is order-optimal

Conclusion and Future Work

- Conclusion
  - We derive the lower and the upper bounds of the optimal rate of the permutation codes in the generalized Cayley metric
  - We provide a coding scheme of order-optimal codes
  - We prove that our code is more rate efficient than the existing permutation codes based on interleaving
  - We extend our result by developing a construction of systematic permutation codes in this metric that is order-optimal
- Future work
  - Binary codes that corrects generalized transposition error (has potential in DNA storage)

Thank you!