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

1 Motivation
   • Background
   • Objective

2 Theoretical Analysis
   • Distances of Interest
   • Order-Optimal Codes

3 Construction
   • Encoding Schemes
   • Decoding Schemes
   • Rate Analysis
   • Systematic Codes

4 Conclusion
   • Conclusion and Future Work
Outline

1 Motivation
   - Background
   - Objective

2 Theoretical Analysis
   - Distances of Interest
   - Order-Optimal Codes

3 Construction
   - Encoding Schemes
   - Decoding Schemes
   - Rate Analysis
   - Systematic Codes

4 Conclusion
   - Conclusion and Future Work
Applications

- Flash memories: charge leakage between cells [1]

Applications

- Flash memories: charge leakage between cells [1]

![Diagram showing charge leakage between cells]

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

![Diagram showing genome rearrangements]

---


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

---


Measures in Permutation Codes

- Common measures
Measures in Permutation Codes

- Common measures
  - Kendall-$\tau$ metric: transpositions [3]

![Diagram showing transpositions]

Measures in Permutation Codes

- **Common measures**
  - Kendall-$\tau$ metric: transpositions [3]
  - Ulam metric: translocation [4]


Measures in Permutation Codes

- **Common measures**
  - Kendall-$\tau$ metric: transpositions [3]
    
    ![Kendall-$\tau$ Metric Example]
  - Ulam metric: translocation [4]
    
    ![Ulam Metric Example]

- **Measure under discussion**

---


Motivation

Objectives

Measures in Permutation Codes

- Common measures
  - **Kendall-τ metric**: transpositions [3]
    
    ![Kendall-τ metric example]

  - **Ulam metric**: translocation [4]
    
    ![Ulam metric example]

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

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

---


Ultimate Goal

Objective

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

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

Prior work [6]

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]

---


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 $O(N)$ bits, where $N$ is the codelength

---


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 $O(N)$ bits, where $N$ is the codelength

- **Ultimate goal**
  - Redundancy for an order-optimal code that corrects $t$ generalized transposition errors: $O(t \log N)$ bits

---


Outline

1 Motivation
   - Background
   - Objective

2 Theoretical Analysis
   - Distances of Interest
   - Order-Optimal Codes

3 Construction
   - Encoding Schemes
   - Decoding Schemes
   - Rate Analysis
   - Systematic Codes

4 Conclusion
   - Conclusion and Future Work
Generalized Cayley Distance

- **Generalized transposition** $\phi(i_1, j_1, i_2, j_2)$:
  - $\phi(i_1, j_1, i_2, j_2) \in S_N$, $i_1 \leq j_1 < i_2 \leq j_2 \in [N]$, $S_N$ 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** $\phi(i_1, j_1, i_2, j_2)$:
  - $\phi(i_1, j_1, i_2, j_2) \in S_N$, $i_1 \leq j_1 < i_2 \leq j_2 \in [N]$, $S_N$ 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

![Diagram showing a permutation transformation with generalized transposition $\phi(2, 4, 6, 7)$]
Generalized Cayley Distance

- **Generalized transposition** $\phi(i_1, j_1, i_2, j_2)$:
  - $\phi(i_1, j_1, i_2, j_2) \in S_N$, $i_1 \leq j_1 < i_2 \leq j_2 \in [N]$, $S_N$ 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

\[ \phi(2, 4, 6, 7) \]

- $\pi_2 = \pi_1 \circ \phi$
Generalized Cayley Distance

- **Generalized transposition** $\phi(i_1, j_1, i_2, j_2)$:
  - $\phi(i_1, j_1, i_2, j_2) \in S_N, \ i_1 \leq j_1 < i_2 \leq j_2 \in [N]$, $S_N$ 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 $\pi_2$ from $\pi_1$,
  $$d_G(\pi_1, \pi_2) \triangleq \min \{ \exists \ \phi_1, \phi_2, \ldots, \phi_d \in T_N, \ s.t., \ \pi_2 = \pi_1 \circ \phi_1 \circ \phi_2 \cdots \circ \phi_d \}. $$
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 Analysis

Distances of Interest

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)

![Diagram of characteristic set and transpositions]
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 Analysis

Distances of Interest

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 $\forall 1 \leq i \leq d$, $\sigma(i + 1) \neq \sigma(i) + 1$, $\psi_k = \pi_1[i_{k-1} + 1 : i_k]$ for some $0 = i_0 < i_1 \cdots < i_d < i_{d+1} = N$, and $1 \leq k \leq d + 1$, such that

\[
\pi_1 = (\psi_1, \psi_2, \cdots, \psi_{d+1}),
\]
\[
\pi_2 = (\psi_{\sigma(1)}, \psi_{\sigma(2)}, \cdots, \psi_{\sigma(d+1)}).
\]
## 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 $\forall 1 \leq i \leq d$, $\sigma(i + 1) \neq \sigma(i) + 1$, $\psi_k = \pi_1 [i_{k-1} + 1 : i_k]$ for some $0 = i_0 < i_1 \cdots < i_d < i_{d+1} = N$, and $1 \leq k \leq d + 1$, such that

  $$\pi_1 = (\psi_1, \psi_2, \cdots, \psi_{d+1}),$$

  $$\pi_2 = (\psi_{\sigma(1)}, \psi_{\sigma(2)}, \cdots, \psi_{\sigma(d+1)}).$$

### Example

<table>
<thead>
<tr>
<th>$\pi_1$</th>
<th>$\psi_1$</th>
<th>$\psi_2$</th>
<th>$\psi_3$</th>
<th>$\psi_4$</th>
<th>$\psi_5$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>$A(\pi_1)$</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\pi_2$</th>
<th>$\psi_1$</th>
<th>$\psi_4$</th>
<th>$\psi_3$</th>
<th>$\psi_2$</th>
<th>$\psi_5$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>$A(\pi_2)$</td>
<td>10</td>
<td>15</td>
<td>16</td>
<td>4</td>
<td>12</td>
</tr>
</tbody>
</table>
**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 $\forall 1 \leq i \leq d$, $\sigma(i + 1) \neq \sigma(i) + 1$, $\psi_k = \pi_1[i_{k-1} + 1 : i_k]$ for some $0 = i_0 < i_1 \cdots < i_d < i_{d+1} = N$, and $1 \leq k \leq d + 1$, such that
  
  $\pi_1 = (\psi_1, \psi_2, \cdots, \psi_{d+1})$,
  
  $\pi_2 = (\psi_{\sigma(1)}, \psi_{\sigma(2)}, \cdots, \psi_{\sigma(d+1)})$.

- $d_B(\pi_1, \pi_2) = \frac{1}{2}|A(\pi_1) \Delta A(\pi_2)|$
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 $\forall 1 \leq i \leq d$, $\sigma(i+1) \neq \sigma(i) + 1$, $\psi_k = \pi_1[i_{k-1} + 1 : i_k]$ for some $0 = i_0 < i_1 \cdots < i_d < i_{d+1} = N$, and $1 \leq k \leq d+1$, such that
    \[
    \pi_1 = (\psi_1, \psi_2, \cdots, \psi_{d+1}), \\
    \pi_2 = (\psi_{\sigma(1)}, \psi_{\sigma(2)}, \cdots, \psi_{\sigma(d+1)}).
    \]

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

- **Metric embedding**:
  \[
  d_G(\pi_1, \pi_2) \leq d_B(\pi_1, \pi_2) \leq 4d_G(\pi_1, \pi_2)
  \]
Definitions and Rates of Order-Optimal Codes

- **t-Generalized Cayley code** $C_G(N, t)$
  - Corrects $t$ generalized transposition errors, $d_{G,\text{min}} \geq 2t + 1$
Definitions and Rates of Order-Optimal Codes

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

- **t-Block permutation code** $C_B(N, t)$
  - Minimum block permutation distance $d_{B,\text{min}} \geq 2t + 1$
Definitions and Rates of Order-Optimal Codes

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

- **$t$-Block permutation code** $C_B(N, t)$
  - Minimum block permutation distance $d_{B,\text{min}} \geq 2t + 1$

- Optimal code rates: $R_{G,\text{opt}}(N, t), R_{B,\text{opt}}(N, t)$
Definitions and Rates of Order-Optimal Codes

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

- **t-Block permutation code** \( C_B(N, t) \)
  - Minimum block permutation distance \( d_{B,\min} \geq 2t + 1 \)

- Optimal code rates: \( R_{G,\text{opt}}(N, t) \), \( R_{B,\text{opt}}(N, t) \)

- Order-optimal \( 4t \)-block permutation codes are order-optimal \( t \)-generalized Cayley codes

**Theorem**

The optimal rates satisfy the following inequalities,

\[
1 - c_1 \cdot \frac{2t + 1}{N} \leq R_{B,\text{opt}}(N, t) \leq 1 - \frac{t}{N},
\]

\[
1 - c_1 \cdot \frac{8t + 1}{N} \leq R_{G,\text{opt}}(N, t) \leq 1 - c_2 \cdot \frac{4t}{N},
\]

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

1 Motivation
   - Background
   - Objective

2 Theoretical Analysis
   - Distances of Interest
   - Order-Optimal Codes

3 Construction
   - Encoding Schemes
   - Decoding Schemes
   - Rate Analysis
   - Systematic Codes

4 Conclusion
   - Conclusion and Future Work
Key Idea in Encoding Scheme

\[
p_1 \\
A(p_1) \\
g(p_1)
\]
**Key Idea in Encoding Scheme**

**Step 1:** Compute the characteristic set $A(\pi)$ for every $\pi$
### Key Idea in Encoding Scheme

<table>
<thead>
<tr>
<th>$\pi_1$</th>
<th>$A(\pi_1)$</th>
<th>$g(\pi_1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2, 3</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3, 11</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6, 7</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>8, 9, 10, 15</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>10, 15</td>
<td>10</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>12</td>
<td>12, 13</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>14</td>
<td>14, 6, 7</td>
<td>14</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>16</td>
<td>16, 4, 5</td>
<td>16</td>
</tr>
</tbody>
</table>

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

**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 $\pi$

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 $\pi$

**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 $\alpha$ constitute a $t$-block permutation code $C_\alpha(N, t)$
Key Idea in Encoding Scheme

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

**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 $\alpha$ constitute a $t$-block permutation code $C_{\alpha}(N, t)$

**Note:** $C_{\alpha}(N, t)$ with the maximum cardinality is order-optimal
**Key Steps in Decoding Algorithm**

Channel: Receiver receives $\pi'$ when sender sends $\pi$, $d_B(\pi, \pi') \leq t$
Key Steps in Decoding Algorithm

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

Step 1: Compute $A(\pi')$, $g(\pi')$ and $f_2 = (X; \pi')$ from $\pi'$
Key Steps in Decoding Algorithm

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

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

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

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

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

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

- $f_2$ provides incomplete information about the roots of $f_1$
- $\alpha$ provides complete information about the $4t - 1$ coefficients of $f_1$
Key Steps in Decoding Algorithm

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

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

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

Step 2: Compute $f_1(X) = f(X; \pi)$ from $\alpha$ and $f_2$
Key Steps in Decoding Algorithm

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

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

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

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

Step 3: Compute $g(\pi)$, $A(\pi)$ and $\pi$
Key Steps in Decoding Algorithm

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

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

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

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

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

$$R_{\rho_g}C(N, t) < 1 - \frac{2N + \mathcal{O}((\log N)^2)}{N \log N - (\log e)N + \frac{1}{2} \log N} \sim 1 - \frac{2}{\log N},$$

$$R_G(N, t) > 1 - \frac{32t \log N + 16t}{N \log N - (\log e)N + \frac{1}{2} \log N} \sim 1 - \frac{32t}{N},$$

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

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

Solution

Constructing systematic codes in the generalized Cayley metric

Extended work submitted to IEEE Transactions on Information Theory, also available at arxiv: https://arxiv.org/abs/1803.04314

Siyi Yang, Clayton Schoeny, Lara Dolecek

Order-Optimal Permutation 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 Transactions on Information Theory, also available at arxiv: https://arxiv.org/abs/1803.04314
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
Main idea: insert $k$ elements $[N + 1 : N + k]$ into the length $N$ permutations at positions decided by their parity check sums.
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 $k \sim \mathcal{O}(t)$.
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 $2t$
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 $k \sim O(t)$
- Permutations with the same parity check sum keep a distance greater than $2t$
- Permutations with different parity check sums
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 $k \sim O(t)$

- Permutations with the same parity check sum keep a distance greater than $2t$

- Permutations with different parity check sums
  - Each element in $\eta(\alpha)$ is identical to an element in $\pi$
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 $k \sim O(t)$

- Permutations with the same parity check sum keep a distance greater than $2t$

- Permutations with different parity check sums
  - Each element in $\eta(\alpha)$ is identical to an element in $\pi$
  - Insert $N + i$, $1 \leq i \leq k$ sequentially after the element in $\pi$ identical to the $i$-th element in $\eta(\alpha)$
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 $k \sim O(t)$
- Permutations with the same parity check sum keep a distance greater than $2t$
- Permutations with different parity check sums
  - Each element in $\eta(\alpha)$ is identical to an element in $\pi$
  - Insert $N+i$, $1 \leq i \leq k$ sequentially after the element in $\pi$ identical to the $i$-th element in $\eta(\alpha)$
  - New permutations also have distance at least $2t+1$
Outline

1 Motivation
   • Background
   • Objective

2 Theoretical Analysis
   • Distances of Interest
   • Order-Optimal Codes

3 Construction
   • Encoding Schemes
   • Decoding Schemes
   • Rate Analysis
   • Systematic Codes

4 Conclusion
   • Conclusion and Future Work
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.

**Future work**
- Binary 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
  - We prove that our code is more rate efficient than the existing permutation codes based on interleaving

Future work

- Binary 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
- 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 in the generalized Cayley metric.
Thank you!