Order-Optimal Permutation Codes in the Generalized Cayley Metric

Siyi Yang, Clayton Schoeny, and Lara Dolecek
Electrical and Computer Engineering, University of California, Los Angeles
siyiyang, cschoeny@g.ucla.edu and dolecek@ee.ucla.edu

***Abstract*—Permutation codes have recently garnered substantial research interest due to their potential in flash memories. We study the theoretical bounds and the constructions of permutation codes in the generalized Cayley metric. The generalized Cayley metric captures the number of generalized transposition errors in a permutation, and subsumes previously studied error types, including transpositions and translocations, without imposing restrictions on the lengths and positions of the translocated segments. Relying on the *breakpoint analysis* proposed by Chee and Vu, we propose a coding scheme that is order-optimal.**

I. Introduction

Permutation codes have recently garnered substantial interest due to their potential in flash memories [1]. In recent years, permutation codes in the Kendall-τ metric [2] and Ulam metric [3] have been intensely studied. Based on the frameworks in the Ulam metric, Chee and Vu introduce the so-called generalized Cayley metric that captures the number of generalized transpositions between two permutations [4]. Generalized transposition errors subsume transpositions and translocations that the Kendall-τ metric and Ulam metric describe, when no restrictions are imposed on the positions and lengths of the translocated segments.

Codes in the generalized Cayley metric were first studied by Chee and Vu in [4] using *breakpoint analysis*, and they proposed a coding scheme based on the construction of permutation codes in the Ulam metric in [3]. Let N be the codelength, the interleaving technique used in that scheme inevitably incurs a noticeable rate penalty of $\mathcal{O}\left(\frac{1}{\log N}\right)$. As we show later, the best possible rate of a length-N code that corrects t generalized transposition errors is $1-\mathcal{O}(\frac{t}{N})$. When t is small compared to $\mathcal{O}(\frac{N}{\log N})$, the gap between the rate of existing codes based on interleaving and the optimal rate increases with N, thus motivating the need to introduce other techniques that are not based on interleaving. All the details can be found in [5].

II. Measure of Distance

A. Generalized Cayley Metric

A **generalized transposition** $\phi(i_1, j_1, i_2, j_2) \in \mathbb{S}_N$, where $i_1 \leq j_1 < i_2 \leq j_2 \in [N]$, refers to a permutation on $[1:N]$ that is obtained from swapping two segments $e[i_1, j_1]$ and $e[i_2, j_2]$ in the identity permutation e, namely, $\phi(i_1, j_1, i_2, j_2) \triangleq \{1, \cdots, i_1-1, i_2, \cdots, j_2, j_1+1, \cdots, i_2-1, i_1, \cdots, j_1, j_2+1, \cdots, N\}$. Denote the set of all generalized transpositions on a permutation on $[1:N]$ as $\mathbb{T}_N$. For each $\pi \in \mathbb{S}_N$ and $\phi(i_1, j_1, i_2, j_2) \in \mathbb{T}_N$, the permutation obtained from swapping two segments $\pi[i_1; j_1]$ and $\pi[i_2; j_2]$ is exactly $\pi \circ \phi$.

Definition 1. (Generalized Cayley Distance, cf. [4]) *The* ***generalized Cayley distance*** $d_G(\pi_1, \pi_2)$ *is defined as the minimum number of generalized transpositions that is needed to obtain the permutation* π_2 *from* π_1*, i.e.,*

$$\begin{aligned} d_G(\pi_1, \pi_2) \triangleq \min_d \{ & \exists\ \phi_1, \phi_2, \cdots, \phi_d \in \mathbb{T}_N, \\ & \textit{s.t.},\ \pi_2 = \pi_1 \circ \phi_1 \circ \phi_2 \cdots \circ \phi_d\}. \end{aligned} \tag{1}$$

Notice that the generalized Cayley distance d_G between two permutations is hard to compute, which makes it difficult to construct codes in the generalized Cayley metric. The common method to solve this problem is metric embedding, where we find another metric that is computable and is of the same order as d_G. Then we are able to transform the construction of codes in d_G into that in the new metric. This new metric is the *block permutation distance* we introduce next.

Definition 2. *The* ***block permutation distance*** $d_B(\pi_1, \pi_2)$ *between two permutations* $\pi_1, \pi_2 \in \mathbb{S}_N$ *is equal to* d *if*

$$\begin{aligned} \pi_1 &= (\psi_1, \psi_2, \cdots, \psi_{d+1}), \\ \pi_2 &= \left(\psi_{\sigma(1)}, \psi_{\sigma(2)}, \cdots, \psi_{\sigma(d+1)}\right), \end{aligned} \tag{2}$$

where $\sigma \in \mathbb{D}_{d+1}$*,* $\psi_k = \pi_1[i_{k-1}+1 : i_k]$ *for some* $0 = i_0 < i_1 \cdots < i_d < i_{d+1} = N$*, and* $1 \leq k \leq d+1$.

Lemma 1. *For all* $\pi_1, \pi_2 \in \mathbb{S}_N$*, we have:*

$$d_G(\pi_1, \pi_2) \leq d_B(\pi_1, \pi_2) \leq 4 d_G(\pi_1, \pi_2). \tag{3}$$

III. Theoretical Bounds

A subset $\mathcal{C}_G(N, t)$ of $\mathbb{S}_N$ is called a ***t-generalized Cayley code*** if it can correct t generalized transposition errors. Any t-generalized Cayley code has minimum generalized Cayley distance $d_{G,min} \geq 2t+1$. Similarly, a subset $\mathcal{C}_B(N, t)$ of $\mathbb{S}_N$ is a ***t-block permutation code*** if its minimum block permutation distance $d_{B,min} \geq 2t+1$. Denote the optimal code rate of $\mathcal{C}_G(N, t)$ and $\mathcal{C}_B(N, t)$ as $R_{G,opt}(N, t)$ and $R_{B,opt}(N, t)$, respectively.

Theorem 1. *For fixed t and sufficiently large* N*, the optimal rates satisfy the following inequalities,*

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

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

Theorem 1 indicates that the rate $R = 1 - \mathcal{O}\left(\frac{t}{N}\right)$ is order-optimal for both the t-generalized Cayley codes and the t-block permutation codes. We know from *Lemma 1* that any $4t$-block permutation code is also a t-generalized Cayley code. In the sequel, we thus focus on the construction of order-optimal t-block permutation codes.

IV. Construction

A. Encoding Scheme

Definition 3. *The* **characteristic set** $A(\pi)$ *for any* $\pi \in \mathbb{S}_N$ *is defined as the set of all consecutive pairs in* π*, i.e.,*

$$A(\pi) \triangleq \{(\pi(i), \pi(i+1))\,|1 \le i < N\}. \tag{5}$$

Denote the set of all ordered pairs of non-identical elements from $[N]$ as P, then $|P| = N^2 - N$. From *Bertrand's postulate*, we can find a prime q such that $|P| \le q \le 2|P|$. Let $u: \; P \to \mathbb{F}_q$ be an injection from P to $\mathbb{F}_q$, where $\mathbb{F}_q$ is the Galois field of order q. For all $\pi \in \mathbb{S}_N$, let $g(\pi)$ be the image of $A(\pi)$ under u. We define a surjection $h: \; \mathbb{S}_N \to \mathbb{F}_q^{4t-1}$ as follows:

$$h(\pi) \triangleq (\alpha_1, \alpha_2, \cdots, \alpha_{4t-1}), \tag{6}$$

where $\alpha_k \equiv \sum_{b \in g(\pi)} b^k \mod q$ for all $1 \le k \le 4t-1$.

Construction 1. *For all* $\boldsymbol{\alpha} \in \mathbb{F}_q^{4t-1}$*, let the* t*-block permutation code with parity check sum* $\boldsymbol{\alpha}$ *be defined as follows*

$$\mathcal{C}_{\boldsymbol{\alpha}}(N,t) = \{\pi | \pi \in \mathbb{S}_N, \; h(\pi) = \boldsymbol{\alpha}\}, \tag{7}$$

where h *is defined in (6).*

Remark 1. *In* Construction 1*, suppose the codebook with maximal cardinality has parity check sum* $\boldsymbol{\alpha}_{\max}$*, then* $\mathcal{C}_{\boldsymbol{\alpha}_{\max}}(N,t)$ *is order-optimal.*

B. Decoding Scheme

In this subsection, all the polynomials as well as the polynomial operations are defined in $\mathbb{F}_q$. For an arbitrary $\pi \in \mathbb{S}_N$, define

$$f(X;\pi) \triangleq \prod_{b \in g(\pi)} (X+b) = X^{N-1} + \sum_{i=1}^{N-1} a_{i,\pi} X^{N-1-i}. \tag{8}$$

Suppose the transmitter sends a codeword $\pi \in \mathbb{S}_N$ from the codebook $\mathcal{C}_{\boldsymbol{\alpha}}(N,t)$ and the receiver receives π', where $d_B(\pi,\pi') \le t$. Denote $f_1 \triangleq f(X;\pi), f_2 \triangleq f(X;\pi')$. Let $a_i = a_{i,\pi}$ and $a_i' = a_{i,\pi'}$ for all $1 \le i < 4t$. Let $B' = g(\pi')$. The following *Algorithm 1* describes our coding schme, where $\mathbf{b} = \left(a_1', \cdots, a_{4t-1}'\right)^T - \left(a_1, \cdots, a_{4t-1}\right)^T$, and

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ a_1 & 1 & \ddots & \vdots & a_1' & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots & \vdots & \ddots & 0 \\ a_{t-1} & a_{t-2} & \cdots & 1 & a_{t-1}' & a_{t-2}' & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{4t-2} & a_{4t-3} & \cdots & a_{3t-1} & a_{4t-2}' & a_{4t-3}' & \cdots & a_{3t-1}' \end{pmatrix}.$$

Algorithm 1 Decoding Algorithm

Input:
Prior knowledge: α;
Received sequence: π';
Output:
Estimated codeword: $\hat{\pi}$;
Compute the coefficients of f_2: $\{a_i'\}_{i=1}^{4t-1}$ and B' from π';
Compute the coefficients of f_1: $\{a_i\}_{i=1}^{4t-1}$ from α by *Newton's Identities*;
Find a solution $\mathbf{c}$ of $\mathbf{A}\mathbf{c} = \mathbf{b}$;
Compute $h_1 = X^t + c_1 X^{t-1} + c_2 X^{t-2} + \cdots + c_t$, $h_2 = X^t + c_1' X^{t-1} + c_2' X^{t-2} + \cdots + c_t'$;
Compute $\gamma_1 = \gcd(h_1, h_2)$, $\gamma_3 = \frac{h_1}{h}$, $\gamma_2 = \frac{h_2}{h}$;
Find the set of negative roots of γ_2 and γ_3 to be D_1, D_2, respectively;
Compute $\hat{\pi} = g^{-1}\left(D_1 \cup (B' \setminus D_2)\right)$;
return $\hat{\pi}$;

C. Rate Comparison with Interleaving-based scheme

From *Lemma 1*, we can construct a t-generalized Cayley code $\mathcal{C}_G(N,t) = \mathcal{C}_{\boldsymbol{\alpha}}(N,4t)$ with rate $R_G(N,t)$ using *Construction 1*. In [4], a t-generalized Cayley code $A_{\rho_g C}(N,t)$ with rate $R_{\rho_g C}(N,t)$ was constructed. The following *Lemma 2* proves the efficiency of our scheme.

Lemma 2. $R_G(N,t) > R_{\rho_g C}(N,t)$ *when* $t < \frac{N}{(16\log N + 8)}$ *for sufficiently large* N.

V. Conclusion

Permutation codes have been shown to have potential in flash memories. In this work, we studied the permutation codes in the generalized Cayley metric. Interleaving was previously shown to be efficient in constructions of permutation codes in the generalized Cayley metric. However, interleaving incurs a noticeable rate penalty such that the constructed permutation codes cannot be order-optimal. We presented a construction of order-optimal permutation codes. Our proposed codes are more rate efficient than the existing coding schemes based on interleaving, in the regime of sufficiently large N and small t.

Acknowledgment

The authors would like to thank the funding from NSF CAREER grant No.1150212 and NSF CIF grant No.1527130.

References

[1] R. Gabrys, E. Yaakobi, F. Farnoud, and J. Bruck, "Codes correcting erasures and deletions for rank modulation," in *Proc. IEEE Int. Symp. Inf. Theory*, Hawaii, USA, Jun. 2014, pp. 2759–2763.

[2] S. Buzaglo, E. Yaakobi, T. Etzion, and J. Bruck, "Systematic error-correcting codes for permutations and multi-permutations," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3113–3124, Jun. 2016.

[3] F. Farnoud, V. Skachek, and O. Milenkovic, "Error-correction in flash memories via codes in the Ulam metric," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 3003–3020, May 2013.

[4] 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, Jun. 2014, pp. 2959–2963.

[5] S. Yang, C. Schoeny, and L. Dolecek, "Order-optimal permutation codes in the generalized Cayley metric," uclacodess.org/papers/PermutationCodesITW.pdf, 2017.