On the Labeling Problem of Permutation Group Codes Under the Infinity Metric

Itzhak Tamo, *Student Member, IEEE*, and Moshe Schwartz, *Senior Member, IEEE*

***Abstract*—We consider codes over permutations under the infinity norm. Given such a code, we show that a simple relabeling operation, which produces an isomorphic code, may drastically change the minimal distance of the code. Thus, we may choose a code structure for efficient encoding procedures, and then optimize the code's minimal distance via relabeling. To establish that the relabeling problem is hard and is of interest, we formally define it and show that all codes may be relabeled to get a minimal distance at most 2. On the other hand, the decision problem of whether a code may be relabeled to distance 2 or more is shown to be NP-complete, and calculating the best achievable minimal distance after relabeling is proved to be hard to approximate up to a factor of 2. We then consider general bounds on the relabeling problem. We specifically construct the optimal relabeling for transitive cyclic groups. We conclude with the main result—a general probabilistic bound, which we then use to show both the $\mathrm{AGL}(p)$ group and the dihedral group on p elements may be relabeled to a minimal distance of $p - O(\sqrt{p \ln p})$.**

***Index Terms*—Error-correcting codes, group codes, permutations, rank modulation.**

I. Introduction

CODES over permutations have a long history, starting with the early papers of Slepian [38] (later extended in [2]), in which permutations were used to digitize vectors from a time-discrete memoryless Gaussian source, and Chadwick and Kurz [8], in which permutations were used in the context of signal detection over channels with non-Gaussian noise (especially impulse noise). Further early studies include works such as [2]–[4], [7], [9], and [12].

The use of codes over permutations has regained interest recently due to applications in power-line communications (for example, see, [40]), and rank modulation for flash memories [17] as well as for phase-change memories [31]. In the latter two applications, a group of n cells (either flash or phase-change memory cells) is used to store information by means of ranking the cells according to charge level in the former, or resistance in the latter. Thus, the stored information is a permutation of $\{1, 2, \ldots, n\}$.

To be able to define an error-correcting code over permutations, a metric needs to be selected. There exists a wide variety of metrics over permutations to choose from (see the survey [11]). In this study, we shall be interested in the ℓ_∞-metric, codes over which have already been studied before: Counting problems concerning sets of permutations with bounded pairwise distance properties under the ℓ_∞-metric were studied in [20], [21], [25], [32], and [37]. Error-correcting codes under this metric (sometimes also called permutation arrays) may be found in [5], [22], [26], [36], and [39]. The motivation behind some of these works is a limited-magnitude error model. Following the convention of [39], we shall call such codes limited-magnitude rank-modulation codes (LMRM codes).

A similar error model for flash memory was considered in [6] (though not over permutations), while a different error-model (charge-constrained errors for rank modulation) was studied in [1], [18], and [28]. Codes over permutations have been studied in the past under different metrics [3], [4], [8], [10], [13], [15], [40]. We also mention a generalization of the rank modulation scheme which uses partial permutations studied in [14] and [33].

A code over permutations, being a subset of the symmetric group S_n, may happen to be a subgroup, in which case we call it a *group code*. Group theory offers a rich structure to be exploited when constructing and analyzing group codes, in an analogy to the case of linear codes over vector spaces. Hence, throughout this paper, we focus on LMRM group codes.

If $\mathcal{C}$ and $\mathcal{C}'$ are conjugate subgroups of the symmetric group, then from a group-theoretic point of view, they are almost the same algebraic object, and they share many properties. However, from a coding point of view, these two codes can possess vastly different minimal distance, which is one of the most important properties of a code. For example, consider the following two subgroups of S_n, $\mathcal{C} = \{\iota, (1, n)\}$ and $\mathcal{C}' = \{\iota, (1, 2)\}$, where ι is the identity permutation and the rest of the permutations are given in a cycle notation. The subgroups $\mathcal{C}$ and $\mathcal{C}'$ are conjugate but the minimal distance of $\mathcal{C}$ and $\mathcal{C}'$ is $n - 1$ and 1, respectively, which are the highest and the lowest possible minimal distances in the ℓ_∞-metric.

Hence, we conclude that the minimal distance of a code $\mathcal{C}$ depends crucially on the specific conjugate subgroup. Thus, while a certain group code might be chosen due to its group-theoretic structure (perhaps allowing simple encoding or even simple decoding), we may choose to use an isomorphic conjugate of the group, having the same group-theoretic structure, but with a higher minimal distance. We refer to the problem of finding the optimal minimal distance among all conjugate groups (sets) of a certain group (set) as the *labeling problem*.

Apart from introducing and motivating the labeling problem, we show that this algorithmic problem is hard. However, we are able to show the existence of a labeling with high minimal

Manuscript received September 18, 2011; revised March 28, 2012; accepted May 25, 2012. Date of current version June 08, 2012; date of current version September 11, 2012. This paper was presented in part at the 2011 IEEE International Symposium on Information Theory.

The authors are with the Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer Sheva 84105, Israel (e-mail: tamo@ee.bgu.ac.il; schwartz@ee.bgu.ac.il).

Communicated by E. Arıkan, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2012.2204035

distance for a variety of codes, based on the size of the code and the number of cycles in certain permutations derived from the code itself.

The rest of this paper is organized as follows. In Section II, we define the notation, introduce the error model with the associated ℓ_∞-metric, as well as formally define the labeling problem. We proceed in Section III to introduce two algorithmic problems related to the labeling problem, and we show their hardness. In Section IV, we give some labeling results on ordinary groups and we present our main result of the paper, which gives general labeling results for arbitrary codes based on a probabilistic argument. In addition, we give a few corollaries by applying this result to some well-known groups. We conclude in Section V with a summary of the results and short concluding remarks.

II. Definitions and Notation

For any $m, n \in \mathbb{N}$, $m \leqslant n$, let $[m,n]$ denote the set $\{m, m+1, \ldots, n\}$, where we also denote by $[n]$ the set $[1,n]$. Given any $n \in \mathbb{N}$ we denote by S_n the set of all permutations over the set $[n]$.

We will mostly use the cycle notation for permutations $f \in S_n$, where $f = (f_0, f_1, \ldots, f_{k-1})$ denotes the permutation mapping $f_i \mapsto f_{(i+1) \bmod k}$ for $i \in [0, k-1]$. We shall occasionally use the vector notation whereby a permutation $f = [f_1, f_2, \ldots, f_n] \in S_n$ denotes the mapping $i \mapsto f_i$, for all $i \in [n]$. Given two permutations $f, g \in S_n$, the product fg is a permutation mapping $i \mapsto f(g(i))$ for all $i \in [n]$.

A *code*, $\mathcal{C}$ is a subset $\mathcal{C} \subseteq S_n$. Note that sometimes $\mathcal{C}$ will also be a subgroup of S_n, in which case we shall refer to $\mathcal{C}$ as a *group code*. For a code $\mathcal{C}$ and a permutation $f \in S_n$, we call the code $f\mathcal{C}f^{-1} = \{fcf^{-1} : c \in \mathcal{C}\}$ a *conjugate* of $\mathcal{C}$.

We shall describe the motivating error model using rank-modulation for flash (as in [39]), though it is the same as for phase-change memory [31], and for pulse-amplitude modulation with additive white Gaussian noise mentioned in [22]. Consider n flash memory cells which we name $1, 2, \ldots, n$. The charge level of each cell is denoted by $c_i \in \mathbb{R}$ for all $i \in [n]$. In the *rank-modulation scheme* defined in [17], the information is stored by the permutation induced by the cells' charge levels in the following way: The induced permutation (in vector notation) is $[f_1, f_2, \ldots, f_n]$ iff $c_{f_i} > c_{f_{i+1}}$ for all $i \in [n-1]$.

Having stored a permutation in n flash cells, a corrupted version of it may be read due to any of a variety of error sources (see [29] and [30]). To model a measure of the corruption in the stored permutations, one can use any of the well-known metrics over S_n (see [11]). Given a metric over S_n, defined by a distance function $d : S_n \times S_n \to \mathbb{N} \cup \{0\}$, an *error-correcting code* is a subset of S_n with lower bounded distance between distinct members.

In [18], the Kendall-τ metric was used, where the distance between two permutations is the number of adjacent transpositions required to transform one into the other. This metric is used when we can bound the total difference in charge levels.

In this study, we consider a different type of error—a limited-magnitude error. Suppose a permutation $f \in S_n$ was stored by setting the charge levels of n flash memory cells to $c_1, c_2, \ldots, c_n$. We say a single error of limited-magnitude L has occurred in the ith cell if the corrupted charge level, c'_i, obeys $|c_i - c'_i| \leqslant L$. The magnitude L depends on the voltage distribution when reading after programming a target charge level (see, for example, the distributions in flash memory in [30, Fig. 9.2, p. 200] and [29, Fig. 14.18, p. 420], as well as the phase-change memory equivalent in [31, Fig. 4]). The limited-magnitude error model has also been used for coding in the context of flash memory (not necessarily over permutations) in [6], [19], [22]–[24], [34], and [39].

In general, we say errors of limited-magnitude L have occurred if the corrupted charge levels of all the cells, $c'_1, c'_2, \ldots, c'_n$, obey

$$\max_{i \in [n]} |c_i - c'_i| \leqslant L.$$

Denote by f' the permutation induced by the cell charge levels $c'_1, c'_2, \ldots, c'_n$ under the rank-modulation scheme. Under the plausible assumption that distinct charge levels are not arbitrarily close (due to resolution constraints and quantization at the reading mechanism), i.e., $|c_i - c_j| \geqslant \ell$ for some positive constant $\ell \in \mathbb{R}$ for all $i \neq j$, an error of limited-magnitude L implies a constant $d \in \mathbb{N}$ such that

$$\max_{i \in [n]} \left| f^{-1}(i) - f'^{-1}(i) \right| < d.$$

Loosely speaking, an error of limited magnitude cannot change the *rank* of the cell i (which is simply $f^{-1}(i)$) by d or more positions.

We, therefore, find it suitable to use the ℓ_∞-metric over S_n defined by the distance function

$$d_\infty(f,g) = \max_{i \in [n]} |f(i) - g(i)|$$

for all $f, g \in S_n$. Since this will be the distance measure used throughout the paper, we will usually omit the ∞ subscript.

Definition 1: An LMRM-code with parameters (n, M, d) is a subset $\mathcal{C} \subseteq S_n$ of cardinality M, such that $d_\infty(f,g) \geqslant d$ for all $f, g \in \mathcal{C}$, $f \neq g$. (We will sometimes omit the parameter M.)

We note that unlike the charge-constrained rank-modulation codes of [18], in which the codeword is stored in the permutation induced by the charge levels of the cells, here the codeword is stored in the *inverse* of the permutation.

Permutation codes under the ℓ_∞-metric have been studied before in [22] and [39]. The size of spheres in this metric has been studied in [20] and [32], and the size of optimal anticodes in [35].

For a code $\mathcal{C}$, we define its minimal distance and denote it by $d(\mathcal{C})$ as

$$d(\mathcal{C}) = \min_{\substack{f,g \in \mathcal{C} \\ f \neq g}} d(f,g).$$

A *labeling* function is a permutation $l \in S_n$. A *relabeling* of a code C by a labeling $l \in S_n$ is defined as the set lCl^{-1}. We say that the code $\mathcal{C}$ has minimal distance d with a labeling function l when

$$d(lCl^{-1}) = d.$$

It is well known (see [11]) that the ℓ_∞-metric over S_n is only right invariant and not left invariant, i.e., for any $f, g, h \in S_n$, $d(f,g) = d(fh, gh)$, and usually $d(f,g) \neq d(hf, hg)$, thus we would expect that in many cases $d(\mathcal{C}) \neq d(l\mathcal{C}l^{-1})$. Therefore, the questions of which labeling permutation leads to the optimal minimal distance, and what is the optimal minimal distance, rise naturally in the context of error-correcting codes over permutations under the infinity metric. Note that l is called a labeling function because for a permutation in cycle notation $f = (a_1, \ldots, a_{k_1}) \cdots (a_{k_j+1}, \ldots, a_n)$, we get

$$lfl^{-1} = (l(a_1), \ldots, l(a_{k_1})) \cdots (l(a_{k_j+1}), \ldots, l(a_n)).$$

The labeled permutation lfl^{-1} has the same cycle structure as f but the elements within each cycle are relabeled by l.

By virtue of the right invariance of the ℓ_∞-metric, we shall assume throughout the paper that any code $\mathcal{C} \subseteq S_n$ contains the identity permutation, since right cosets of $\mathcal{C}$ preserve the distances between codewords, and one of the cosets contains the identity. Furthermore

$$d(\mathcal{C}) = \min_{g,h \in C, g \neq h} d(gh^{-1}, \iota)$$

where ι is the identity element of S_n, and where the distance from the identity shall be called the *weight* of the permutation. This makes it easier to calculate the minimal distance of a group code since gh^{-1} simply goes over all the codewords.

More specifically, we will explore the case where $\mathcal{C}$ is a subgroup of S_n and ask which conjugate group of $\mathcal{C}$ has the largest minimal distance. We denote by $\mathcal{L}_{\min}(\mathcal{C})$ $(\mathcal{L}_{\max}(\mathcal{C}))$ the minimal (maximal) achievable minimal distance among all the conjugates of a code $\mathcal{C}$.

III. Labeling Problem is Hard to Approximate

In this section, we define two algorithmic problems regarding the labeling of codes and show that they are hard to approximate. We shall begin by showing that for any code $\mathcal{C}$, $\mathcal{L}_{\min}(\mathcal{C}) \leqslant 2$, which means that the minimal distance of a code depends crucially on its labeling. We then continue by showing the decision problem of whether $\mathcal{L}_{\max}(\mathcal{C}) \geqslant 2$ is NP-complete, while finding out $\mathcal{L}_{\max}(\mathcal{C})$ is hard to approximate.

Recall the conjugacy relation over S_n: Two permutations $g, f \in S_n$ are said to be conjugate if there exists $h \in S_n$ such that $hgh^{-1} = f$. Conjugacy is an equivalence relation, and its equivalence classes are called conjugacy classes. Let $T = \{C_1, C_2, \ldots, C_k\}$ be the set of conjugacy classes of S_n. It is known that two permutations have the same cycle structure if and only if they share the same conjugacy class. Denote by $B(\iota, r)$ the ball of radius r centered at the identity

$$B(\iota, r) = \{f \in S_n : d(f, \iota) \leqslant r\}.$$

The following lemma will help us show that any code $\mathcal{C}$ has a "bad" labeling, i.e., a labeling with minimal distance 1 or 2.

Lemma 2: For any $n \in \mathbb{N}$, there is a permutation f composed of a single n-cycle, i.e., $f = (a_0, a_1, \ldots, a_{n-1}) \in S_n$, such that $|a_i - a_{(i+1) \bmod n}| \leqslant 2$ for all $i \in [0, n-1]$.

Proof: The proof is by induction. For $n = 1, 2, 3$, all n-cycles in S_n satisfy the claim. We assume the claim holds for n, and prove it also holds for $n+1$. By the induction hypothesis there is $f = (a_0, a_1, \ldots, a_{n-1}) \in S_n$ that satisfies the claim. Without loss of generality (w.l.o.g.), we can assume that $a_{n-1} = n-1$, $a_0 = n$, and $a_1 = n-2$; otherwise f^{-1} would satisfy these conditions. Set $a_n = n+1$ and the permutation $f' = (a_0, a_1, \ldots, a_{n-1}, a_n) \in S_{n+1}$ satisfies the claim. ■

Corollary 3: Let C be any conjugacy class of S_n, then

$$B(\iota, 2) \cap C \neq \emptyset.$$

Proof: Every conjugacy class of S_n is uniquely defined by the set of its cycles' lengths. Let $\{n_1, n_2, \ldots, n_k\}$ be the cycles' lengths of the permutations in C, where $\sum_{i=1}^{k} n_i = n$. By Lemma 2, we conclude that there exists some $f \in C$ such that

$$f = (a_1^1, a_2^1, \ldots, a_{n_1}^1)(a_1^2, a_2^2, \ldots, a_{n_2}^2) \cdots (a_1^k, a_2^k, \ldots, a_{n_k}^k)$$

where for each i, the set $\{a_j^i\}_{j=1}^{n_i} = [1 + \sum_{m=1}^{i-1} n_m, \sum_{m=1}^{i} n_m]$ and the cycle $(a_1^i, a_2^i, \ldots, a_{n_i}^i)$ satisfies Lemma 2. One can easily check that $d(f, \iota) \leqslant 2$, thus $f \in B(\iota, 2)$. ■

Now we are ready to prove that any code $\mathcal{C}$ has a "bad" labeling.

Theorem 4: For any code $\mathcal{C} \subseteq S_n$, $|\mathcal{C}| \geqslant 2$, there exists a labeling of the elements such that the minimum distance is at most 2, i.e., there exists $l \in S_n$ such that $d(l\mathcal{C}l^{-1}) \leqslant 2$. Moreover, $\mathcal{C}$ has a labeling with minimal distance 1 if and only if the set $\{ab^{-1} : a, b \in \mathcal{C}\}$ contains an involution (a permutation of order 2).

Proof: Let $f \in \mathcal{C}$, $f \neq \iota$, be a permutation whose cycles' lengths are $\{n_1, n_2 \ldots, n_k\}$ and where

$$f = (a_1^1, a_2^1, \ldots, a_{n_1}^1)(a_1^2, a_2^2, \ldots, a_{n_2}^2) \cdots (a_1^k, a_2^k, \ldots, a_{n_k}^k).$$

By Corollary 3, there exists $f' \in B(\iota, 2)$ with the same cycle structure as f. Let $l \in S_n$ be the permutation that conjugates f to f', i.e., $lfl^{-1} = f'$. Therefore

$$d(l\mathcal{C}l^{-1}) \leqslant d(l\iota l^{-1}, lfl^{-1}) = d(\iota, f') \leqslant 2.$$

We note that the only permutations of weight 1 are involutions in S_n, and that any involution in S_n may be easily relabeled to be of weight 1. Hence, $\mathcal{C}$ has a labeling with minimal distance 1 if and only if the set $\{ab^{-1} : a, b \in \mathcal{C}\}$ contains an involution. ■

After proving that the worst labeling satisfies $\mathcal{L}_{\min}(\mathcal{C}) \leqslant 2$ for all $\mathcal{C} \subseteq S_n$, we turn to consider the best labeling. We show that the algorithmic decision problem of determining whether a certain code $\mathcal{C}$ has $\mathcal{L}_{\max}(\mathcal{C}) = 1$ or $\mathcal{L}_{\max}(\mathcal{C}) \geqslant 2$ is NP-complete.

2-Distance Problem:

1) INPUT: A subset of permutations $\mathcal{C} \subseteq S_n$ given as a list of permutations, each given in vector notation.
2) OUTPUT: The correct Yes or No answer to the question "Does $\mathcal{C}$ have a labeling that leads to a minimal distance at least 2, i.e., is $\mathcal{L}_{\max}(\mathcal{C}) \geqslant 2$? "

We start with a few definitions. For a code $\mathcal{C} \subseteq S_n$, define its associated set of involutions as

$$I(\mathcal{C}) = \{g \in S_n : g^2 = \iota,\ g = ab^{-1} \neq \iota,\ a, b \in \mathcal{C}\}.$$

For any $g \in I(\mathcal{C})$, we define a subset of edges, $E(g)$, of the complete graph on n vertices, K_n, where the vertices are conveniently called $1, 2, \ldots, n$, as

$$E(g) = \{uv \in E(K_n) : g(u) = v, u \neq v\}.$$

Example 5: Let us consider the code

$$\mathcal{C} = \{\iota, (1,2,3,4), (4,3,2,1)\} \subseteq S_4.$$

We then have

$$\mathcal{C}\mathcal{C}^{-1} = \{\iota, (1,2,3,4), (4,3,2,1), (1,3)(2,4)\}.$$

Thus, by definition we get

$$I(\mathcal{C}) = \{(1,3)(2,4)\}$$

and if we take $g = (1,3)(2,4) \in I(\mathcal{C})$, then

$$E(g) = \{13, 24\}$$

i.e., the edge connecting 1 and 3, and the edge connecting 2 and 4, in K_4. □

Recall that a Hamiltonian path in an undirected graph G is a path which visits each vertex exactly once. The following theorem shows an equivalence between the property of a code having a labeling with minimal distance at least 2 and the existence of a certain Hamiltonian path in the complete graph K_n.

Theorem 6: Let $\mathcal{C} \subseteq S_n$ be a code, then $\mathcal{L}_{\max}(\mathcal{C}) \geqslant 2$ if and only if there exists a Hamiltonian path in K_n which does not include all the edges $E(g)$, for any $g \in I(\mathcal{C})$.

Proof: Recall that $d(\mathcal{C}) = \min_{f,h \in \mathcal{C}, f \neq h} d(fh^{-1}, \iota)$ and note that any permutation which contains a cycle of length 3 or more is at distance at least 2 from the identity. Hence, we only have to make sure the set of involutions, $I(\mathcal{C})$, has distance at least 2 from the identity.

If such a Hamiltonian path, $a_1, a_2, \ldots, a_n$, exists in K_n, then use this path as the labeling permutation and label the element a_i as i, i.e., the labeling permutation $l \in S_n$ satisfies $l(a_i) = i$ for all $i \in [n]$. For any $g \in I(\mathcal{C})$, we know that there exists some $uv \in E(g)$ which does not belong to the Hamiltonian path in K_n, and therefore, $|l(u) - l(v)| \geqslant 2$. From the definition of $E(g)$, we get that $g(u) = v$, and so $d(lgl^{-1}, \iota) \geqslant 2$.

For the other direction, let $l \in S_n$ be a labeling such that $d(l\mathcal{C}l^{-1}) \geqslant 2$. We now consider the Hamiltonian path $l^{-1}(1), l^{-1}(2), \ldots, l^{-1}(n)$ in K_n. By our choice of l, for any $g \in I(\mathcal{C})$, there exists $u, v \in [n]$ such that $g(u) = v$ and $|l(u) - l(v)| \geqslant 2$. Hence, the edge uv does not belong to the constructed Hamiltonian path in K_n. ■

By the last theorem, we conclude that any algorithm that finds a labeling of $\mathcal{C}$ with minimal distance at least 2 actually finds a Hamiltonian path in K_n which does not include all the edges $E(g)$, for any $g \in I(\mathcal{C})$. We are now able to show that the 2-DISTANCE problem is NP-complete.

Theorem 7: The 2-DISTANCE problem is NP-complete.

Proof: First, we show that 2-DISTANCE is in NP. For any given verifier, $l \in S_n$, which is a labeling function, we compute the distance between ι and all the elements of $I(\mathcal{C})$. Note that $|I(\mathcal{C})| \leqslant |\mathcal{C}|^2$ and constructing $I(\mathcal{C})$ may be easily done in polynomial time. Thus, the question can be verified in polynomial time.

In order to verify the completeness, we shall reduce the HAMILTONIAN-PATH problem (see [16]) to our problem. Let $G(V, E)$ be a graph on n vertices (given as an $n \times n$ adjacency matrix) in which we want to decide whether a Hamiltonian path exists. Define the code

$$\mathcal{C} = \{(u, v) : uv \notin E\} \cup \{\iota\} \subseteq S_n$$

where (u, v) is the permutation that fixes everything in place except commuting the elements u and v. Obviously, we can construct $\mathcal{C}$ from G in polynomial time. We then run the 2-DISTANCE algorithm on $\mathcal{C}$ and return its answer.

We observe that

$$I(\mathcal{C}) = \{(u,v)(k,l) : (u,v), (k,l) \in \mathcal{C}, \{u,v\} \cap \{k,l\} = \emptyset\} \cup \mathcal{C} \setminus \{\iota\}.$$

If $a_1, a_2, \ldots, a_n$ is a Hamiltonian path in G, then it is also a Hamiltonian path in K_n not containing all of $E(g)$, for any $g \in I(\mathcal{C})$. This is true because $E(g)$ only contains edges that are not in E.

For the other direction, if there is a Hamiltonian path in K_n which does not include all the edges of $E(g)$ for any $g \in I(\mathcal{C})$, then, in particular, this path does not include all of $E(g)$, $g \in \mathcal{C}$, $g \neq \iota$. Since for any such $g = (u, v) \in \mathcal{C}$, $E(g) = \{uv\}$, and $uv \notin E$, this path is also a Hamiltonian path in G. ■

We now define a harder algorithmic question and deduce by Theorem 7 that this problem is hard to approximate.

Optimal-Distance Problem:

1) INPUT: A subset of permutations $\mathcal{C} \subseteq S_n$ given in vector notation.
2) OUTPUT: The integer $\mathcal{L}_{\max}(\mathcal{C})$.

For a constant $\epsilon > 1$, we say the problem may be ϵ-approximated if there exists an efficient algorithm that for any input $\mathcal{C}$ computes $f(\mathcal{C})$ which satisfies

$$\frac{1}{\epsilon}\mathcal{L}_{\max}(\mathcal{C}) \leqslant f(\mathcal{C}) \leqslant \epsilon\mathcal{L}_{\max}(\mathcal{C}).$$

Corollary 8: For any constant $1 < \epsilon < 2$, the OPTIMAL-DISTANCE problem cannot be ϵ-approximated unless $P = \mathrm{NP}$.

Proof: Assume there exists an efficient algorithm computing $f(\mathcal{C}) \in \mathbb{N}$ which is an ϵ-approximation of $\mathcal{L}_{\max}(\mathcal{C})$. If $\mathcal{L}_{\max}(\mathcal{C}) = 1$, then $f(\mathcal{C}) < 2$ and so $f(\mathcal{C}) \leqslant 1$. If, however, $\mathcal{L}_{\max}(\mathcal{C}) \geqslant 2$, then $f(\mathcal{C}) > 1$. Thus, given such an efficient algorithm exists, we can decide whether $\mathcal{L}_{\max}(\mathcal{C}) \geqslant 2$, i.e., efficiently solve the 2-DISTANCE problem. By Theorem 7 we know that the 2-DISTANCE problem is NP-complete, and so $P = \mathrm{NP}$. ■

IV. Constructions and Bounds

In the previous section, we have shown that the 2-DISTANCE and OPTIMAL-DISTANCE problems are hard. We are, therefore, motivated to focus on solving and bounding the latter problem for specific families of codes, and in particular, codes that form a subgroup of the symmetric group S_n. The rich structure offered by such codes makes them easier to analyze, in much the same way as linear codes in vector space. Furthermore, knowing good labelings for certain groups is of great interest since one can use them as building blocks when constructing larger codes (see, for example, the direct and semi-direct product constructions in [39], or the first recursive construction of [22]).

A. Optimal Labeling for Transitive Cyclic Groups

The most simple basic groups one can think of are transitive cyclic groups. Recall that for a cyclic group G, there is an element $g \in G$ such that G is generated by the powers of g, i.e., $G = \{g^k : k \in \mathbb{N}\}$. We also recall that a group G acting on $[n]$ is said to be *transitive* if for every $a, b \in [n]$ there exists $g \in G$ such that $g(a) = b$. The following theorem gives an exact optimal labeling for transitive cyclic groups over the set $[n]$.

Theorem 9: Let $\mathcal{C} \subseteq S_n$ be a transitive cyclic group over the set $[n]$, then the optimal minimal distance for $\mathcal{C}$ is

$$\mathcal{L}_{\max}(\mathcal{C}) = n - \left\lceil \frac{\sqrt{4n-3}-1}{2} \right\rceil.$$

Proof: Let $f = (a_1, a_2, \ldots, a_n) \in \mathcal{C}$ be a generator[1] of $\mathcal{C}$, and let d be an achievable minimal distance, i.e., there is a labeling l such that $d(l\mathcal{C}l^{-1}) = d$. Denote $\mathcal{C}' = l\mathcal{C}l^{-1}$, then $f' = lfl^{-1} = (l(a_1), l(a_2), \ldots, l(a_n))$ is a generator of $\mathcal{C}'$. Define

$$B = \{(x, y) \in [n] \times [n] : |x - y| \geqslant d\}.$$

From the minimal distance of $\mathcal{C}'$, we know that for any $g \in \mathcal{C}'$, $g \neq \iota$, $d(g, \iota) \geqslant d$. Hence, there is at least one pair $(x, y) \in B$ such that $g(x) = y$. We note that

$$|B| = 2\sum_{i=1}^{n-d} i = (n-d)(n-d+1).$$

On the other hand, $\mathcal{C}$ is cyclic and transitive and so is $\mathcal{C}'$, so for any pair $(x, y) \in B$ there is exactly one $g \in \mathcal{C}'$ such that $g(x) = y$. It follows that

$$|\mathcal{C}' \setminus \{\iota\}| = n - 1 \leqslant |B| = (n-d)(n-d+1).$$

Solving the inequality and remembering that d is an integer, we get

$$d \leqslant n - \left\lceil \frac{\sqrt{4n-3}-1}{2} \right\rceil.$$

In order to show the upper bound is achievable, conveniently denote $k = \lceil (\sqrt{4n-3}-1)/2 \rceil$ and define the sets

$$A_1 = [1, k], \quad A_2 = [k+1, n-k], \quad A_3 = [n-k+1, n].$$

We define the following labeling $l \in S_n$:

1) First set $l(a_i) = i$ for all $i \in A_1$.
2) Then set $l(a_{(n+1-i)(2k-n+i)/2+1}) = i$ for all $i \in A_3$.
3) Finally set $l(a_j) = i$ for all $i \in A_2$, where j is chosen arbitrarily from the left-over indices.

We will show that for any $s \in [n-1]$, $d(f^s, \iota) \geqslant n - k$. Note that it is enough to show the claim for $s \leqslant \lceil n/2 \rceil$ since if $s > \lceil n/2 \rceil$ then by the right invariant property $d(f^s, \iota) = d(\iota, f^{-s}) = d(\iota, f^{n-s})$.

Let $s \in [\lceil n/2 \rceil]$, and note that

$$\begin{aligned}\sum_{i=1}^{k} i &= \frac{1}{2}\left\lceil \frac{\sqrt{4n-3}-1}{2} \right\rceil \left\lceil \frac{\sqrt{4n-3}+1}{2} \right\rceil \\ &\geqslant \frac{1}{2} \cdot \frac{\sqrt{4n-3}-1}{2} \cdot \frac{\sqrt{4n-3}+1}{2} \\ &= \frac{4n-4}{8} \\ &= \frac{n-1}{2}.\end{aligned}$$

However, since $\sum_{i=1}^{k} i$ is an integer, we get that

$$\sum_{i=1}^{k} i \geqslant \left\lceil \frac{n-1}{2} \right\rceil = \left\lfloor \frac{n}{2} \right\rfloor.$$

Thus, let $m \in [k]$ be the smallest integer such that

$$\sum_{j=0}^{m-1} (k-j) = \frac{m(2k-m+1)}{2} \geqslant s.$$

Hence

$$\frac{m(2k-m+1)}{2} - s + 1 \leqslant k - m + 1. \tag{1}$$

From labeling rule 2, we get that

$$a_{\frac{m(2k-m+1)}{2}+1} = n - m + 1$$

and from labeling rule 1

$$a_{\frac{m(2k-m+1)}{2}-s+1} = \frac{m(2k-m+1)}{2} - s + 1$$

and so

$$\begin{aligned}d(f^s, \iota) &= \max_{i \in [n]} |f^s(i) - i| \\ &\geqslant \left| f^s\left(\frac{m(2k-m+1)}{2} - s + 1\right) \right. \\ &\qquad \left. - \left(\frac{m(2k-m+1)}{2} - s + 1\right) \right| \\ &\geqslant \left| f^s\left(a_{\frac{m(2k-m+1)}{2}-s+1}\right) - (k-m+1) \right| \\ &= \left| a_{\frac{m(2k-m+1)}{2}+1} - (k-m+1) \right| \\ &= |n - m + 1 - (k-m+1)| \\ &= n - k, \end{aligned} \tag{2}$$

where (2) follows from (1). ∎

[1] A single-cycle generator must exist since $\mathcal{C}$ is transitive.

Since the labeling of indices in A_2 is arbitrary, we actually have $(n-2k)!$ different good labelings resulting from the theorem.

Example 10: Applying Theorem 9 for the case $n = 10$ we get that $k = 3$, and the optimal minimal distance is $\mathcal{L}_{\max}(\mathcal{C}) = n - k = 10 - 3 = 7$. Moreover, such a labeling is $a_1 = 1$, $a_2 = 2, a_3 = 3, a_4 = 10, a_6 = 9, a_7 = 8$, and one of the cycles that generates the cyclic group of minimal distance 7 is

$$(1, 2, 3, 10, 4, 9, 8, 5, 6, 7).$$

□

B. Neighboring-Sets Method

In this section, we present a general method that we call the neighboring-sets method. With this method, lower and upper bounds on $\mathcal{L}_{\max}(\mathcal{C})$ may be obtained provided certain neighboring sets of indices exist. We shall first describe the general method, and then apply it, using further probabilistic arguments, to show strong bounds on $\mathcal{L}_{\max}(\mathrm{AGL}(p))$ where $\mathrm{AGL}(p)$ is the affine general linear group of order p, as well as $\mathcal{L}_{\max}(D_n)$, where D_n is the dihedral group of order n.

We start by recalling the definitions of D_n and $\mathrm{AGL}(p)$ and dispensing with small parameters, for which we can give exact bounds.

Definition 11: For $n \in \mathbb{N}$, the dihedral group of order n, denoted D_n is the group generated by the two permutations

$$D_n = \langle (1, 2, \ldots, n), (1, n)(2, n-1) \cdots (\lfloor n/2 \rfloor, \lceil n/2 \rceil) \rangle .$$

The group D_n contains $2n$ permutations and is the group of symmetries of a regular polygon with n sides, containing both rotations and reflections.

Example 12: For $n = 4$

$$D_4 = \{\iota, (1, 2, 3, 4), (1, 3)(2, 4), (4, 3, 2, 1), (1, 4)(2, 3), (2, 4), (1, 2)(3, 4), (1, 3)\}.$$

□

We refer to the labeling of D_n described in the definition above as the *natural* labeling of D_n.

Definition 13: Let $p \in \mathbb{N}$ be a prime; then $\mathrm{AGL}(p)$ is defined by the subgroup of permutations that acts on the set $[0, p-1]$ and is generated by the permutations $f(x) = x + 1$ and $g(x) = ax$, where all calculations are over $\mathrm{GF}(p)$ and a is a primitive element in $\mathrm{GF}(p)$ (a generator of the multiplicative group of $\mathrm{GF}(p)$).

Throughout we shall consider only $\mathrm{AGL}(p)$ for $p \geqslant 3$. Like before, we refer to the natural labeling of $\mathrm{AGL}(p)$ as the labeling derived from the permutations f and g described previously. For example, the natural labeling of $\mathrm{AGL}(5)$ is the group generated by the permutations (in cycle notation) $f = (0, 1, 2, 3, 4)$ and $g = (1, 2, 4, 3)$. The following theorem gives us the minimal distance of the natural labeling of $\mathrm{AGL}(p)$.

Theorem 14: For any prime $p \geqslant 3$, $\mathrm{AGL}(p)$ with the natural labeling has minimal distance $(p-1)/2$.

Proof: Because $\mathrm{AGL}(p)$ is a group and the metric is right invariant it suffices to check only the distances from the identity permutation. Let σ_b be the permutation $\sigma_b : x \mapsto x + b$ for some $b \in [1, p-1]$. If $b \geqslant (p-1)/2$, then $|\sigma_b(0) - 0| \geqslant (p-1)/2$. Otherwise, $|\sigma_b(p-1) - (p-1)| \geqslant (p-1)/2$. Thus, in any case, $d(\sigma_b, \iota) \geqslant (p-1)/2$.

Let $\tau \in \mathrm{AGL}(p)$ be an arbitrary permutation of the kind $\tau(x) = ax + b$ where $a \neq 1$. Both of the permutations $\sigma_{(p-1)/2}$ and τ represent lines in the affine plane with different slopes, and so there exists $x_0 \in [0, p-1]$ such that $\tau(x_0) = \sigma_{(p-1)/2}(x_0)$. Hence, $|\tau(x_0) - x_0| \geqslant (p-1)/2$ and then $d(\tau, \iota) \geqslant (p-1)/2$, which concludes the proof. ■

The next theorem shows that the natural labeling is optimal for any prime $p < 8$.

Theorem 15: For any prime $3 \leqslant p < 8$

$$\mathcal{L}_{\max}(\mathrm{AGL}(p)) = \frac{p-1}{2}.$$

Proof: Let I be the set of involutions of $\mathrm{AGL}(p)$. It is easy to verify that any permutation $g \in I$ is of the form $g(x) = -x + b$ for some $b \in \mathrm{GF}(p)$, and so $|I| = p$. We note also that for any $x_1, x_2 \in \mathrm{GF}(p)$, there is exactly one involution $g \in I$ such that $g(x_1) = x_2$ (finding g is by solving the equation $x_2 = -x_1 + b$).

Assume that we have a labeling of $\mathrm{AGL}(p)$ with minimal distance more than the natural minimal distance. In particular, with this labeling, every involution has minimal distance at least $(p+1)/2$ from the identity permutation. Let

$$B = \left\{ \{x, y\} : x, y \in \mathrm{GF}(p), |x - y| \geqslant \frac{p+1}{2} \right\}.$$

Now, for any $g \in I$, there is at least one unordered pair $\{x, y\} \in B$ such that $g(x) = y$. It follows that

$$|B| = \frac{p^2 - 1}{8} \geqslant |I| = p.$$

Solving the inequality, we get $p \geqslant 4 + \sqrt{17} > 8$. ■

We can get a very similar result (which we omit) regarding the distance of the natural labeling of the dihedral group D_n, showing it to be approximately $n/2$.

It is tempting to assume that for large p and n we can get labelings for $\mathrm{AGL}(p)$ and D_n with normalized distance tending to 1, by virtue of their size alone: $|D_n| = 2n$ and $|\mathrm{AGL}(p)| = p(p-1)$, both vanishing in comparison to the size of S_n and S_p, respectively. However, a simple example of a code

$$\mathcal{C} = \{\iota\} \cup \left\{ l(1, 2)l^{-1} : l \in S_n \right\} \subseteq S_n$$

dispels this thought since $|\mathcal{C}| = n(n-1)/2 + 1$, $d(\mathcal{C}) = 1$, and for any $l \in S_n$ we have $l\mathcal{C}l^{-1} = \mathcal{C}$, so relabeling does not change the code's distance. Thus, we turn to describe the neighboring-sets method which will attain better results for $\mathrm{AGL}(p)$ and D_n.

Definition 16: Let $\mathcal{C} \subseteq S_n$ be any set of permutations acting on $[n]$. Two disjoint subsets $A, B \subseteq [n]$ are called $\mathcal{C}$-neighboring sets if for any $f \in \mathcal{C}$, $f \neq \iota$, the following holds:

$$(f(A) \cap B) \cup (f(B) \cap A) \neq \emptyset.$$

We define $O(\mathcal{C})$ to be the smallest integer $O(\mathcal{C}) = |A| + |B|$, where A and B are $\mathcal{C}$-neighboring sets. If there are no such sets then we define $O(\mathcal{C}) = \infty$.

First we show that if $\mathcal{C}$ is a group then, $O(\mathcal{C})$ is closely related to its optimal minimal distance.

Theorem 17: Let $\mathcal{C} \subseteq S_n$ be a group that acts on $[n]$ with $O(\mathcal{C}) < \infty$, then

$$n - O(\mathcal{C}) + 1 \leqslant \mathcal{L}_{\max}(\mathcal{C}).$$

Moreover, if $\mathcal{L}_{\max}(\mathcal{C}) \geqslant \frac{n}{2}$, then also

$$\mathcal{L}_{\max}(\mathcal{C}) \leqslant n - \frac{O(\mathcal{C})}{2}.$$

Proof: Since $O(\mathcal{C}) < \infty$, there exist $\mathcal{C}$-neighboring sets A, $B \subseteq [n]$ such that $|A| + |B| = O(\mathcal{C})$. Let the labeling function $l \in S_n$ be such that $l(A) = [1, |A|]$, and $l(B) = [n - |B| + 1, n]$. It is trivial to check that $l\mathcal{C}l^{-1}$ has minimal distance $n - O(\mathcal{C}) + 1 \leqslant d(\mathcal{C})$.

For the other inequality, assume that the labeling l of $\mathcal{C}$ gives the optimal minimal distance, $d(l\mathcal{C}l^{-1}) = \mathcal{L}_{\max}(\mathcal{C}) \geqslant \frac{n}{2}$. It follows that $n - \mathcal{L}_{\max}(\mathcal{C}) < \mathcal{L}_{\max}(\mathcal{C}) + 1$, so $A = [1, n - \mathcal{L}_{\max}(\mathcal{C})]$, and $B = [\mathcal{L}_{\max}(\mathcal{C}) + 1, n]$, are two disjoint sets. We will show that A and B are $\mathcal{C}$-neighboring sets.

For any $n - \mathcal{L}_{\max}(\mathcal{C}) < i < \mathcal{L}_{\max}(\mathcal{C}) + 1$, if such i exists at all, and for any $f \in l\mathcal{C}l^{-1}$, $f \neq \iota$, we have $|f(i) - i| < \mathcal{L}_{\max}(\mathcal{C})$. However, $d(f, \iota) \geqslant \mathcal{L}_{\max}(\mathcal{C})$ and so necessarily $(f(A) \cap B) \cup (f(B) \cap A) \neq \emptyset$. Thus, A and B are $\mathcal{C}$-neighboring sets. Hence, $O(\mathcal{C}) \leqslant 2(n - \mathcal{L}_{\max}(\mathcal{C}))$, and the result follows. ■

It is pointed out in the definition that some groups $\mathcal{C} \subseteq S_n$ might have $O(\mathcal{C}) = \infty$, e.g., $O(S_n) = \infty$. The following theorem shows that for any prime $p > 5$, $O(\mathrm{AGL}(p))$ is finite while also showing a lower bound.

Theorem 18: If $p = 3, 5$, then $O(\mathrm{AGL}(p)) = \infty$. For any prime $p \geqslant 7$

$$O(\mathrm{AGL}(p)) \geqslant \max\left\{\sqrt{2(p-1)}, 6\right\}.$$

For primes $p \geqslant 37$, we also have

$$O(\mathrm{AGL}(p)) \leqslant p.$$

Proof: We first start with the lower bounds. It is well known that $\mathrm{AGL}(p)$ is 2-transitive, i.e., for any (a, b), $(c, d) \in [0, p-1]^2$, $a \neq b$, $c \neq d$, there exists $f \in \mathrm{AGL}(p)$ such that $f((a, b)) = (c, d)$. If $O(\mathrm{AGL}(p)) \leqslant 5$ and A and B are $\mathrm{AGL}(p)$-neighboring sets then, w.l.o.g., we can assume that $|A| \leqslant 2$. Hence, there exists $f \in \mathrm{AGL}(p)$, $f \neq \iota$, such that $f(A) = A$ which contradicts the fact that A and B are $\mathrm{AGL}(p)$-neighboring sets. As a consequence, we also get that $O(\mathrm{AGL}(3)) = O(\mathrm{AGL}(5)) = \infty$.

The second lower bound is based on a counting argument. $\mathrm{AGL}(p)$ contains a permutation f composed of one cycle of length p. For any $i \in [p-1]$, there exists at least one $(k, m) \in (A \times B) \cup (B \times A)$ such that $f^i(k) = m$. On the other hand, for any $(k, m) \in (A \times B) \cup (B \times A)$, there exists only one $i \in [p-1]$ such that $f^i(k) = m$. Thus

$$p - 1 \leqslant |(A \times B) \cup (B \times A)| = 2|A| \cdot |B| \qquad (3)$$

and the result follows because the minimum of $O(\mathrm{AGL}(p)) = |A| + |B|$ given by (3) is $\sqrt{2(p-1)}$.

For the upper bound, we will show that there are $\mathrm{AGL}(p)$-neighboring sets A, $B \subseteq [0, p-1]$ of sizes $(p-1)/2$ and $(p+1)/2$, respectively, and thus $O(\mathrm{AGL}(p)) \leqslant p$. We note that A and B of the appropriate sizes are neighboring sets if and only if $f(A) \neq A$ for all $f \neq \iota$. We shall, therefore, try to bound the number of such "bad" subsets A. Assume $A \subseteq [0, p-1]$, $|A| = \frac{p-1}{2}$, and $f \in \mathrm{AGL}(p)$, $f \neq \iota$. Then, $f(A) = A$ iff A is a union of cycles of f. We define a polynomial which is related to the cycle-index polynomial of f as

$$Z_f(x) = \prod_i (1 + x^i)^{a_i(f)}$$

where $a_i(f)$ is the number of cycles of f of length i. It follows that the number of "bad" sets A for f is the coefficient of $x^{(p-1)/2}$ in $Z_f(x)$. Summing over all permutations $f \in \mathrm{AGL}(p)$ except the identity permutation will upper bound the number of such "bad" sets in $\mathrm{AGL}(p)$.

The group $\mathrm{AGL}(p)$ is a disjoint union (except for the identity) of p groups which are the cyclic group of order p generated by $(0, 1, \ldots, p-1)$, and $p-1$ cyclic groups generated by a permutation of the form $(a_0, a_1, \ldots, a_{p-2})(a_{p-1})$. Since, in a cyclic group of order ℓ, for each $i|\ell$ there are $\phi(i)$ elements of order i, where ϕ is Euler's totient function, we can define the polynomial $Z_{\mathrm{AGL}(p)}(x)$ and readily verify that

$$\begin{aligned} Z_{\mathrm{AGL}(p)}(x) &\triangleq \sum_{f \in \mathrm{AGL}(p), f \neq \iota} Z_f(x) = \\ &= (p-1)(1 + x^p) + \sum_{\substack{i | p-1 \\ i > 1}} p\phi(i)(1 + x)(1 + x^i)^{\frac{p-1}{i}}. \end{aligned}$$

We shall now upper bound the coefficient $a_{(p-1)/2}$ of $x^{(p-1)/2}$ in $Z_{\mathrm{AGL}(p)}$

$$a_{\frac{p-1}{2}} = \sum_{\substack{2i | p-1 \\ i > 1}} p\phi(i) \binom{\frac{p-1}{i}}{\frac{p-1}{2i}} \leqslant \frac{p^3}{\sqrt{\frac{\pi(p-1)}{4}}} \cdot 2^{\frac{p-1}{2}}$$

where the upper bound is derived by upper bounding $\phi(i) \leqslant p$, upper bounding the central binomial coefficient using [27], and taking at most p summands.

On the other hand, the number of subsets of $[0, p-1]$ of size $(p-1)/2$ is exactly $\binom{p}{(p-1)/2}$. One can easily verify that

$$\binom{p}{(p-1)/2} > \frac{p^3}{\sqrt{\frac{\pi(p-1)}{4}}} \cdot 2^{\frac{p-1}{2}}$$

for all primes $p \geqslant 37$. Thus, there are sets A such that $f(A) \neq A$, as required. ■

Example 19: Let $p = 7$. By Theorem 18, we have the lower bound $O(\mathrm{AGL}(7)) \geqslant 6$, and indeed the sets $A = \{0, 1, 2\}$, $B = \{4, 5, 6\}$ are $\mathrm{AGL}(7)$-neighboring sets. Furthermore, by Theorem 17, we get that $7 - O(\mathrm{AGL}(7)) + 1 = 2 \leqslant \mathcal{L}_{\max}(\mathrm{AGL}(7))$. However, by Theorem 15, we know that $\mathcal{L}_{\max}(\mathrm{AGL}(7)) = 3$. □

The following theorem is our main result of this section. It gives a generic labeling result for a code $\mathcal{C}$ over the set $[n]$ based

solely on the size of the code and the number of cycles in the set of permutations $\mathcal{C}\mathcal{C}^{-1} = \{gh^{-1} : g, h \in \mathcal{C}\}$.

Theorem 20: Let $\mathcal{C} \subseteq S_n$ be a code. If there exist $q, t \in \mathbb{R}$, $0 < q < \frac{1}{2}$, and $t > 0$, such that

$$e^{-\frac{2t^2}{n}} + e^{-nq^2/(1-q)} \sum_{\substack{f \in \mathcal{C}\mathcal{C}^{-1} \\ f \neq \iota}} e^{c(f)q^2/(1-q)} < 1 \tag{4}$$

where $c(f)$ is the number of cycles in the permutation f, then there exists a labeling $l \in S_n$ such that

$$\mathcal{L}_{\max}(\mathcal{C}) \geqslant d(lCl^{-1}) \geqslant n + 1 - \lfloor 2qn + t \rfloor .$$

Proof: We use a probabilistic argument to show such a labeling exists. We partition the set $[n]$ into three disjoint sets, A, B, and C, according the probabilities $P(i \in A) = q$, $P(i \in B) = q$, and $P(i \in C) = 1 - 2q$, where elements are placed independently.

Assume first that $f \in S_n$ is a single cycle, i.e., $f = (a_0, a_1, \ldots, a_{k-1})$. We define the events

$$D_i(f) = \{a_i \in A \text{ and } a_{i+1} \in B \text{ or } a_i \in B \text{ and } a_{i+1} \in A\}$$

for each $i \in [0, k-1]$, and where the indices are taken modulo k. Where it is clear from context, we shall write D_i for short. We also define the event D_f to be that A and B are $\{f\}$-neighboring sets.

We would like to evaluate the probability that A and B are not $\{f\}$-neighboring sets, i.e., the probability $P(\overline{D_f}) = P(\cap_{i=0}^{k-1} \overline{D_i})$. It is easy to calculate that

$$P(\overline{D_i}) = 1 - 2q^2.$$

Furthermore, for all $i \in [0, k-1]$, we denote

$$q_i = P(\overline{D_i} | \overline{D_0}, \ldots, \overline{D_{i-1}}).$$

We find the following recursion, for all $i \in [0, k-3]$:

$$\begin{aligned} q_{i+1} &= P(\overline{D_{i+1}} | \overline{D_0}, \ldots, \overline{D_i}) \\ &= P(a_{i+1} \in C | \overline{D_0}, \ldots, \overline{D_i}) \\ &\quad \cdot P(\overline{D_{i+1}} | \overline{D_0}, \ldots, \overline{D_i}, a_{i+1} \in C) \\ &\quad + P(a_{i+1} \notin C | \overline{D_0}, \ldots, \overline{D_i}) \\ &\quad \cdot P(\overline{D_{i+1}} | \overline{D_0}, \ldots, \overline{D_i}, a_{i+1} \notin C) \\ &= P(a_{i+1} \in C | \overline{D_0}, \ldots, \overline{D_i}) \\ &\quad + P(a_{i+1} \notin C | \overline{D_0}, \ldots, \overline{D_i}) \cdot (1 - q). \end{aligned}$$

In addition

$$\begin{aligned} P(a_{i+1} \in C | \overline{D_0}, \ldots, \overline{D_i}) &= \frac{P(a_{i+1} \in C | \overline{D_0}, \ldots, \overline{D_{i-1}})}{P(\overline{D_i} | \overline{D_0}, \ldots, \overline{D_{i-1}})} \\ &\quad \cdot P(\overline{D_i} | \overline{D_0}, \ldots, \overline{D_{i-1}}, a_{i+1} \in C) \\ &= \frac{1 - 2q}{q_i}. \end{aligned}$$

It follows that for all $i \in [0, k-3]$

$$\begin{aligned} q_0 &= 1 - 2q^2 \\ q_{i+1} &= 1 - q + q \cdot \frac{1 - 2q}{q_i}. \end{aligned}$$

It is easily seen that for all $i \in [0, k-2]$, $q_i \geqslant 1 - q$, and so for all $i \in [0, k-3]$

$$q_{i+1} = 1 - q + q \cdot \frac{1 - 2q}{q_i} \leqslant 1 - \frac{q^2}{1 - q}.$$

Furthermore, since $0 < q < \frac{1}{2}$

$$q_0 = 1 - 2q^2 \leqslant 1 - \frac{q^2}{1 - q}.$$

Combining the above, we get that

$$\begin{aligned} P(\overline{D_f}) &= P(\cap_{i=0}^{k-1} \overline{D_i}) \\ &= \prod_{i=0}^{k-1} P(\overline{D_i} | \cap_{j=0}^{i-1} \overline{D_j}) \\ &\leqslant \prod_{i=0}^{k-2} q_i \leqslant \left(1 - \frac{q^2}{1 - q}\right)^{k-1} \\ &\leqslant e^{-(k-1)q^2/(1-q)} \end{aligned}$$

since $1 - x \leqslant e^{-x}$ for all $x \in \mathbb{R}$.

Let $g \in S_n$ be a general permutation, with cycles' lengths $l_1, l_2, \ldots, l_k$, and $\sum_{i=1}^{k} l_i = n$; then the probability that A and B are not $\{g\}$-neighboring sets is

$$P(\overline{D_g}) \leqslant \prod_{i=1}^{k} e^{-(l_i - 1)q^2/(1-q)} = e^{-(n-k)q^2/(1-q)}.$$

Let $S = |A| + |B| = X_1 + X_2 + \cdots + X_n$, where X_i is the indicator random variable for the event $a_i \in A \cup B$. By the union bound

$$\begin{aligned} P &\left(\bigcup_{\substack{f \in \mathcal{C}\mathcal{C}^{-1} \\ f \neq \iota}} \overline{D_f} \cup \{S \geqslant E(S) + t\} \right) \leqslant \\ &\leqslant P\left(S \geqslant E(S) + t\right) + \sum_{\substack{f \in \mathcal{C}\mathcal{C}^{-1} \\ f \neq \iota}} P(\overline{D_f}) \\ &\leqslant e^{-\frac{2t^2}{n}} + e^{-nq^2/(1-q)} \sum_{\substack{f \in \mathcal{C}\mathcal{C}^{-1} \\ f \neq \iota}} e^{c(f)q^2/(1-q)} \\ &< 1, \end{aligned}$$

where $P(S \geqslant E(S) + t)$ was upper bounded using Hoeffding's inequality.

Therefore, with positive probability neither of these events occur, i.e., there is a labeling for $\mathcal{C}$ such that for any $f \in \mathcal{C}\mathcal{C}^{-1}$, $f \neq \iota$, A and B are $\{f\}$-neighboring sets and $S = |A| + |B| \leqslant E(S) + t = 2qn + t$, and the result follows. ∎

Note that when $\mathcal{C}$ forms a subgroup of S_n, the summation in (4) is done only over the elements of $\mathcal{C} \setminus \{\iota\}$. Theorem 20 easily gives us achievable-labeling results for any subgroup of S_n only by knowing the number of cycles in each of its elements.

We say that $a \in [n]$ is a fixed point of a permutation $f \in S_n$ if $f(a) = a$. The minimal degree of a subgroup $\mathcal{C} \subseteq S_n$ is the minimum number of nonfixed points among the nonidentity permutations in $\mathcal{C}$. The following corollary connects the minimal degree of a group and an achievable distance by applying Theorem 20.

Corollary 21: Let $\mathcal{C}$ be a subgroup of S_n with minimal degree d, such that there exist $t > 0$, $0 < q < \frac{1}{2}$, satisfying

$$e^{-\frac{2t^2}{n}} + |\mathcal{C}| e^{-\frac{dq^2}{2(1-q)}} < 1$$

then $\mathcal{C}$ has a labeling $l \in S_n$ with

$$d(l\mathcal{C}l^{-1}) \geqslant n + 1 - \lfloor 2qn + t \rfloor .$$

Proof: If $\mathcal{C}$ has minimal degree d, then the number of cycles of any $g \in \mathcal{C}$, $g \neq \iota$, is at most $n - \frac{d}{2}$ and the claim follows by Theorem 20. ∎

We now proceed to show strong bounds on $\mathcal{L}_{\max}(\mathrm{AGL}(p))$ and $\mathcal{L}_{\max}(D_n)$.

Theorem 22: For p, a large enough prime

$$p - O(\sqrt{p \ln p}) \leqslant \mathcal{L}_{\max}(\mathrm{AGL}(p)) \leqslant p - \left\lceil \frac{\sqrt{4p-3}-1}{2} \right\rceil .$$

Proof: For the upper bound, we simply note that a transitive cyclic group of order p is a subgroup of $\mathrm{AGL}(p)$, and then use Theorem 9. For the lower bound, we recall that $\mathrm{AGL}(p)$ is sharply 2-transitive; hence, its minimal degree is $p - 1$. By Corollary 21

$$e^{-\frac{2t^2}{p}} + |\mathrm{AGL}(p)| e^{-\frac{(p-1)q^2}{2(1-q)}} \leqslant e^{-\frac{2t^2}{p}} + p^2 e^{-\frac{(p-1)q^2}{2}}.$$

For $t = \sqrt{p \ln(p+1)}$ and $q = \sqrt{\frac{4\ln(p+1)}{p-1}}$, we get

$$e^{-\frac{2t^2}{p}} + p^2 e^{-\frac{(p-1)q^2}{2}} = \frac{1}{(p+1)^2} + \frac{p^2}{(p+1)^2} < 1.$$

We note that for p large enough, $q < \frac{1}{2}$. It follows that

$$\begin{aligned}\mathcal{L}_{\max}(\mathrm{AGL}(p)) &\geqslant p + 1 - \lfloor 2pq + t \rfloor \\ &\geqslant p - 2p\sqrt{\frac{4\ln(p+1)}{p-1}} - \sqrt{p\ln(p+1)} \\ &= p - O(\sqrt{p \ln p}).\end{aligned}$$

∎

Theorem 23: For the dihedral group, D_n, $n \geqslant 37$

$$n - O(\sqrt{n \ln n}) \leqslant \mathcal{L}_{\max}(D_n) \leqslant n - \left\lceil \frac{\sqrt{4n-3}-1}{2} \right\rceil .$$

Proof: For the upper bound, again we note that a transitive cyclic group of order n is a subgroup of D_n and then use Theorem 9. For the lower bound, we know that $|D_n| = 2n$, and that D_n has minimal degree $d \geqslant n - 2$ (it is $n - 2$ for even n, and $n - 1$ for odd n). We use Corollary 21 with

$$t = \sqrt{\frac{n\ln(2n+2)}{2}}, \qquad q = \sqrt{\frac{\ln(2n+2)}{n/2-1}}$$

and get

$$\begin{aligned}e^{-\frac{2t^2}{n}} + |D_n| e^{-\frac{dq^2}{2(1-q)}} &\leqslant e^{-\frac{2t^2}{n}} + 2ne^{-\frac{(n-2)q^2}{2}} \\ &= \frac{1}{2n+2} + \frac{2n}{2n+2} < 1.\end{aligned}$$

It is easy to verify that $q < \frac{1}{2}$ for all $n \geqslant 37$. Thus

$$\begin{aligned}\mathcal{L}_{\max}(D_n) &\geqslant n + 1 - \lfloor 2qn + t \rfloor \\ &\geqslant n - 2n\sqrt{\frac{\ln(2n+2)}{n/2-1}} - \sqrt{\frac{n\ln(2n+2)}{2}} \\ &= n - O(\sqrt{n \ln n}).\end{aligned}$$

∎

We would like to note that at first glance, all the codes $\mathcal{C} \subseteq S_n$ discussed so far have size polynomial in n. This is vanishingly small compared to $|S_n| = n!$. However, these codes may be used as building blocks in constructions such as the first recursive construction of [22], or Construction 2 of [39], to produce codes of size exponential in n, and improved minimal distance compared with a trivial use of the original constructions.

Example 24: Let $k \in \mathbb{N}$ be a constant, and consider a transitive cyclic group of order k, $\mathcal{C}_k \subseteq S_k$. For simplicity of presentation, assume k is even. Without relabeling, using the customary generator $(1, 2, \ldots, k)$, its minimal distance is $k/2$.

Let $n \in \mathbb{N}$ be some integer such that $k|n$. By using Construction 2 of [39] or the first recursive construction of [22], we can get a code of length n, size $k^{n/k}$, and minimal distance $\frac{n}{k} \cdot \frac{k}{2} = n/2$.

However, if we relabel the component cyclic codes according to Theorem 9, we can get the same code of length n, size $k^{n/k}$, but with minimal distance

$$n\left(1 - \frac{1}{k}\left\lceil \frac{\sqrt{4k-3}-1}{2} \right\rceil\right).$$

If we compare this with the best infinite family of codes from [39], then the codes of Construction 1 of [39] with the same minimum distance have size $2^{\left\lceil(\sqrt{4k-3}-1)/2\right\rceil n/k}$. Thus, the size of the codes of this example exceed that of [39] for all $k \leqslant 21$, k not a power of 2. □

V. Summary

In this paper, we examined the relabeling of permutation codes under the infinity metric. While relabeling preserves the code structure, producing an isomorphic code, it may drastically reduce or increase the relabeled code's minimal distance.

We formally defined the relabeling problem and showed that all codes may be relabeled to get a minimal distance of at most 2. Deciding whether one can relabel a given code to achieve minimal distance 2 or more was shown to be an NP-complete problem. In addition, calculating the best minimal distance achievable after relabeling was shown to be hard to approximate.

We then turned to bounding the best achievable minimal distance after relabeling for certain groups, and in particular, transitive cyclic groups, dihedral groups, and affine general linear groups. For transitive cyclic groups, an exact solution and relabeling was shown. For the other two families of groups, a probabilistic method was used to give a general bound which turned out to provide strong bounds on the relabeling distance.

Finding out how the best achievable minimal distance after relabeling depends on certain group properties, and finding

its exact value for other well-known groups, is still an open problem.

ACKNOWLEDGMENT

The authors wish to thank the anonymous reviewers, whose comments helped improve the presentation of this paper.

REFERENCES

[1] A. Barg and A. Mazumdar, "Codes in permutations and error correction for rank modulation," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3158–3165, Jul. 2010.
[2] T. Berger, F. Jelinek, and J. K. Wolf, "Permutation codes for sources," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 1, pp. 160–169, Jan. 1972.
[3] I. F. Blake, "Permutation codes for discrete channels," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 1, pp. 138–140, Jan. 1974.
[4] I. F. Blake, G. Cohen, and M. Deza, "Coding with permutations," *Inf. Control*, vol. 43, pp. 1–19, 1979.
[5] C. Buchheim, P. J. Cameron, and T. Wu, "On the subgroup distance problem," *Discrete Math.*, vol. 309, no. 4, pp. 962–968, Mar. 2009.
[6] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, "Codes for asymmetric limited-magnitude errors with applications to multi-level flash memories," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1582–1595, Apr. 2010.
[7] H. Chadwick and I. Reed, "The equivalence of rank permutation codes to a new class of binary codes," *IEEE Trans. Inf. Theory*, vol. IT-16, no. 5, pp. 640–641, Sep. 1970.
[8] H. D. Chadwick and L. Kurz, "Rank permutation group codes based on Kendall's correlation statistic," *IEEE Trans. Inf. Theory*, vol. IT-15, no. 2, pp. 306–315, Mar. 1969.
[9] G. Cohen and M. Deza, "Decoding of permutation codes," presented at the Int. CNRS Colloq., , France, 1977.
[10] C. J. Colbourn, T. Kløve, and A. C. H. Ling, "Permutation arrays for powerline communication and mutually orthogonal latin squares," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1289–1291, Jun. 2004.
[11] M. Deza and H. Huang, "Metrics on permutations, a survey," *J. Combin. Inf. Sys. Sci.*, vol. 23, pp. 173–185, 1998.
[12] M. Deza and P. Frankl, "On maximal numbers of permutations with given maximal or minimal distance," *J. Combin. Theory Ser. A*, vol. 22, 1977.
[13] C. Ding, F.-W. Fu, T. Kløve, and V. K. Wei, "Construction of permutation arrays," *IEEE Trans. Inf. Theory*, vol. 48, no. 4, pp. 977–980, Apr. 2002.
[14] E. E. Gad, M. Langberg, M. Schwartz, and J. Bruck, "Generalized Gray codes for local rank modulation," in *Proc. IEEE Int. Symp. Inf. Theory*, St. Petersburg, Russia, Aug. 2011, pp. 839–843.
[15] F.-W. Fu and T. Kløve, "Two constructions of permutation arrays," *IEEE Trans. Inf. Theory*, vol. 50, no. 5, pp. 881–883, May 2004.
[16] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. San Francisco, CA: Freeman, 1979.
[17] A. Jiang, R. Mateescu, M. Schwartz, and J. Bruck, "Rank modulation for flash memories," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2659–2673, Jun. 2009.
[18] A. Jiang, M. Schwartz, and J. Bruck, "Correcting charge-constrained errors in the rank-modulation scheme," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2112–2120, May 2010.
[19] T. Kløve, B. Bose, and N. Elarief, "Systematic, single limited magnitude error correcting codes for flash memories," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4477–4487, Jul. 2011.
[20] T. Kløve, "Generating functions for the number of permutations with limited displacement," *Electron. J. Combin.*, vol. 16, pp. 1–11, 2009.
[21] T. Kløve, "Lower bounds on the size of spheres of permutations under the Chebychev distance," *Designs, Codes Cryptography*, vol. 59, no. 1–3, pp. 183–191, 2011.
[22] T. Kløve, T.-T. Lin, S.-C. Tsai, and W.-G. Tzeng, "Permutation arrays under the Chebyshev distance," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2611–2617, Jun. 2010.
[23] T. Kløve, J. Luo, I. Naydenova, and S. Yari, "Some codes correcting asymmetric errors of limited magnitude," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7459–7472, Nov. 2011.
[24] T. Kløve, J. Luo, and S. Yari, "Codes correcting single errors of limited magnitude," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2206–2219, Apr. 2012.
[25] D. H. Lehmer, "Permutations with strongly restricted displacements," in *Combinatorial Theory and its Applications II*, P. Erdős, A. Rényi, and V. T. Sós, Eds. Amsterdam, The Netherlands: North Holland, 1970, pp. 273–291.
[26] T.-T. Lin, S.-C. Tsai, and W.-G. Tzeng, "Efficient encoding and decoding with permutation arrays," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, 2008, pp. 211–214.
[27] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1978.
[28] A. Mazumdar, A. Barg, and G. Zémor, "Constructions of rank modulation codes," in *Proc. IEEE Int. Symp. Inf. Theory*, St. Petersburg, Russia, Aug. 2011, pp. 834–838.
[29] R. Micheloni, L. Crippa, and A. Marelli, *Inside NAND Flash Memories*. New York: Springer, 2010.
[30] R. Micheloni, A. Marelli, and R. Ravasio, *Error Correction for Non-Volatile Memories*. New York: Springer, 2008.
[31] N. Papandreou, H. Pozidis, T. Mittelholzer, G. F. Close, M. Breitwisch, C. Lam, and E. Eleftheriou, "Drift-tolerant multilevel phase-change memory," in *Proc. 3rd IEEE Int. Memory Workshop*, Monterey, CA, May 2011, pp. 22–25.
[32] M. Schwartz, "Efficiently computing the permanent and hafnian of some banded toeplitz matrices," *Linear Algebra Appl.*, vol. 430, no. 4, pp. 1364–1374, Feb. 2009.
[33] M. Schwartz, "Constant-weight Gray codes for local rank modulation," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, Jun. 2010, pp. 869–873.
[34] M. Schwartz, "Quasi-cross lattice tilings with applications to flash memory," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2397–2405, Apr. 2012.
[35] M. Schwartz and I. Tamo, "Optimal permutation anticodes with the infinity norm via permanents of (0, 1)-matrices," *J. Combin. Theory Ser. A*, vol. 118, pp. 1761–1774, 2011.
[36] M.-Z. Shieh and S.-C. Tsai, "Decoding frequency permutation arrays under Chebyshev distance," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5730–5737, Nov. 2010.
[37] M.-Z. Shieh and S.-C. Tsai, "Computing the ball size of frequency permutations under Chebyshev distance," in *Proc. IEEE Int. Symp. Inf. Theory*, St. Petersburg, Russia, Aug. 2011, pp. 2100–2104.
[38] D. Slepian, "Permutation modulation," *Proc. IEEE*, vol. 53, no. 3, pp. 228–236, Mar. 1965.
[39] I. Tamo and M. Schwartz, "Correcting limited-magnitude errors in the rank-modulation scheme," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2551–2560, Jun. 2010.
[40] H. Vinck, J. Haering, and T. Wadayama, "Coded M-FSK for power line communications," in *Proc. IEEE Int. Symp. Inf. Theory*, Sorrento, Italy, 2000, pp. 137–137.

Itzhak Tamo (S'12) was born in Israel in 1981. He received his B.A. and B.Sc. degrees in 2008 from the Mathematics Department and the Electrical and Computer Engineering Department respectively at Ben-Gurion University, Israel.

He is now a doctoral student at the Department of Electrical and Computer Engineering, Ben-Gurion University, Israel. His research interests include algebraic coding, combinatorial structures, and finite group theory.

Moshe Schwartz (M'03–SM'10) was born in Israel in 1975. He received the B.A. (summa cum laude), M.Sc., and Ph.D. degrees from the Technion—Israel Institute of Technology, Haifa, Israel, in 1997, 1998, and 2004 respectively, all from the Computer Science Department.

He was a Fulbright post-doctoral researcher in the Department of Electrical and Computer Engineering, University of California San Diego, and a post-doctoral researcher in the Department of Electrical Engineering, California Institute of Technology. He now holds a position with the Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Israel.

He received the 2009 IEEE Communications Society Best Paper Award in Signal Processing and Coding for Data Storage, and the 2010 IEEE Communications Society Best Student Paper Award in Signal Processing and Coding for Data Storage. His research interests include algebraic coding, combinatorial structures, and digital sequences.