Infinity-Norm Permutation Covering Codes From Cyclic Groups

Ronen Karni and Moshe Schwartz, *Senior Member, IEEE*

***Abstract*— We study covering codes of permutations with the ℓ_∞-metric. We provide a general code construction, which combines short building-block codes into a single long code. We focus on cyclic transitive groups as building blocks, determining their exact covering radius, and showing a linear-time algorithm for finding a covering codeword. When used in the general construction, we show that the resulting covering code asymptotically out-performs the best known code while maintaining linear-time decoding. We also bound the covering radius of relabeled cyclic transitive groups under conjugation, showing that the covering radius is quite robust. While relabeling cannot reduce the covering radius by much, the downside is that we prove the covering radius cannot be increased by more than 1 when using relabeling.**

***Index Terms*— Covering codes, permutations, rank modulation, ℓ_∞-metric, relabeling, cyclic group.**

I. Introduction

Coding over permutations appears in the literature as early as the works [3], [22]. In a typical setting, the symmetric group of permutations on n elements, S_n, is endowed with a distance function, $d : S_n \times S_n \to \mathbb{N}_0$, to create a metric. An *error correcting code* of length n is then defined as a set $C \subseteq S_n$, the elements of which are called *codewords*, such that $d(f, g) \geq d_{\min}$, for all $f, g \in C$, $f \neq g$. The largest such $d_{\min}$ is called the minimum distance of the code. It is also well known that C induces a packing of the space, S_n, by disjoint balls of radius $\lfloor (d_{\min} - 1)/2 \rfloor$, the *packing radius*, centered at the codewords.

In this work, we are interested in the dual problem of covering. Instead of packing balls, we are interested in the smallest radius of balls, centered at the codewords, such that their union covers the entire space. This radius is called the *covering radius* of the code. Equivalently, we are looking for the smallest $r_{\min} \in \mathbb{N}_0$ such that every $f \in S_n$ has a codeword $g \in C$ with $d(f, g) \leq r_{\min}$.

In a typical application of covering codes, suppose we would like to describe any permutation from S_n. To do so, we may assign a unique integer in the range $1, \dots, n!$ to each of the permutations of S_n, calling this integer the *encoding* of the permutation. The reverse process of mapping the encoded integer back to a permutation is called *decoding*. Suppose now we would like to compress the description (i.e., reduce its rate) by using a smaller range of encoding integers, say, $1, \dots, M$, with $M < n!$. Then some permutations will be encoded to the same integer, and the decoding process may recover an incorrect permutation (i.e., a distorted version of the original permutation). Covering codes provide such a rate-distortion scheme: when given a permutation $f \in S_n$, by the properties of the covering code, C, we know f is contained in a ball or radius $r_{\min}$ centered around some codeword $g \in C$, i.e., $d(f, g) \leq r_{\min}$. We then encode g instead of f. The shorter description requires only $M = |C|$ integers, and the decoding back to g is guaranteed to have a distortion upper-bounded by $r_{\min}$. Thus, smaller $M = |C|$ and smaller $r_{\min}$ are better, and a trade-off exists between the two.

Covering codes over general spaces, mostly with the Hamming metric, have been extensively studied. These solve various combinatorial covering problems, are connected to applications in compression and rate-distortion theory, as well as indirectly providing bounds on the parameters of error-correcting codes. The reader is referred to [4] and the numerous constructions, bounds, applications, and references therein.

Covering codes over permutations have only recently been studied in depth, starting with the work of Cameron and Wanless [2], and following with [14], [20], all of which only use the Hamming distance over permutations. In [2], the exact size of covering codes over S_n and covering radius $n - 1$ is found, and bounds are given on the size of covering codes with smaller covering radius. Keevash and Ku [14] present a randomized construction for a code and use a certain frequency parameter to bound the covering radius of the code. A survey of error-correcting codes and covering codes over permutations is given in [20].

Motivated by applications to information storage in non-volatile memories, the rank-modulation scheme was recently suggested [11], in which information is stored in the form of permutations. The relevant permutation metrics for this scheme are mainly the ℓ_∞-metric and Kendall's-τ metric. Thus, we have works studying error-correcting codes [1], [7], [12], [18], [19], [23], [24], [28], [30], Gray codes and snake-in-the-box codes [9], [10], [26], [27], [29], and related combinatorial questions [16], [17], [21].

Covering codes over permutations with the ℓ_∞-metric have only been studied in [6] and [25]. In [25], various connections between different metrics over permutations were found, thus enabling code construction in the ℓ_∞-metric based on codes in

Manuscript received March 1, 2017; revised August 24, 2017; accepted October 13, 2017. Date of publication October 25, 2017; date of current version June 20, 2018. This work was supported by the Israel Science Foundation under Grant 130/14.

The authors are with the Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer-Sheva 8410501, Israel (e-mail: karniron@post.bgu.ac.il; schwartz@ee.bgu.ac.il).

Communicated by P. Sadeghi, Associate Editor for Coding Techniques.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2017.2766296

other metrics. Additionally, bounds on code parameters were given, which were later improved in [6], together with an explicit direct code construction.

The main contribution of this paper is a generalization of the code construction for the infinity norm from [6] and [25]. This generalization combines short building-block covering codes into a single long covering code. We study one such building-block code in detail – a cyclic transitive group of S_n. We derive the exact covering radius of this group. Additionally, we provide a linear-time covering-codeword algorithm for the constructed codes. Finally, it was shown in [24] that relabeling (i.e., conjugating) a group code in the ℓ_∞-metric can potentially change its minimum distance drastically, while preserving the group structure. We therefore study the effect of relabeling on the cyclic transitive group and bound its covering radius after relabeling.

The paper is organized as follows. In Section II we introduce formal definitions and notations used throughout the paper. Section III is devoted to the derivation of the covering radius of the naturally labeled cyclic transitive group. In Section IV we describe the generalized code construction, as well as a linear-time algorithm associated with it. We then turn in Section V to studying relabeling of the building-block code and finding bounds on its covering radius. We conclude in Section VI by discussing the results and suggesting open problems.

II. Notations and Definitions

For $m, m' \in \mathbb{N}$, we denote $[m, m'] \triangleq \{m, m+1, \dots, m'\}$, as well as $[m] \triangleq [1, m]$. For ease of notation, we write $m \bmod^+ n$ to denote the unique $r \in [n]$ such that n divides $m - r$. We emphasize that $m \bmod n$ returns an integer from $\{0, 1, \dots, n-1\}$, whereas $m \bmod^+ n$ return an integer from $[n] = \{1, 2, \dots, n\}$. We then define the *cyclic interval*

$$[m, m'] \bmod^+ n \triangleq \{m \bmod^+ n, (m+1) \bmod^+ n, \dots, m' \bmod^+ n\}.$$

The symmetric group of permutations is denoted by S_n. As will be evident later, it is important for us to fix the permuted elements. Thus, a permutation $f \in S_n$ is a bijection between $[n]$ and itself. We shall use either a one-line notation for permutations, where $f = [f_1, f_2, \dots, f_n]$ denotes a permutation mapping $i \mapsto f_i$ for all $i \in [n]$, or a cycle notation $f = (f_1, f_2, \dots, f_k)$ where f maps $f_i \mapsto f_{(i+1) \bmod^+ k}$ for all $i \in [k]$. If $f, g \in S_n$ are two permutations, their composition is denoted by fg, where $(fg)(i) = f(g(i))$ for all $i \in [n]$. The identity permutation is denoted by Id.

The metric of interest in this work is the ℓ_∞-metric, sometimes also called the Chebyshev metric. The distance function in this metric, denoted $d_\infty : S_n \times S_n \to \mathbb{N}_0$, is defined for all $f, g \in S_n$ by

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

Since this will be the only distance function of interest, we shall drop the ∞ subscript and use only d. We note that for all $f, g \in S_n$, we have $d(f, g) \leq n - 1$. It is well known (e.g., see [5]) that d is right invariant (but not left invariant), i.e., for all $f, g, h \in S_n$,

$$d(fh, gh) = d(f, g).$$

A *code* C is simply a subset $C \subseteq S_n$. Sometimes C will also be a subgroup of S_n, in which case we may refer to C as a *group code*. For such a code $C \subseteq S_n$, and $f \in S_n$, we define the distance between f and C by

$$d(f, C) \triangleq \min_{g \in C} d(f, g).$$

The main object of study in this work is now defined.

Definition 1: An (n, M, r) covering code *is a subset* $C \subseteq S_n$*, such that* $|C| = M$ *and* $d(f, C) \leq r$ *for all* $f \in S_n$*, and* r *is the minimal integer with this property.*

Given an (n, M, r) covering code C, we call $r(C) \triangleq r$ the *covering radius* of C. In an asymptotic setting it will be useful to define the *rate* of the code, $R(C)$, and its *normalized covering radius*, $\rho(C)$, by

$$R(C) \triangleq \frac{\log_2 M}{n}, \quad \rho(C) \triangleq \frac{r}{n-1}.$$

The main focus throughout this paper involves cyclic groups. Since the distance function crucially depends on the permuted elements, we need to define a "natural" description of these groups. Additionally, to avoid degenerate cases, we shall only examine transitive cyclic groups. We therefore give the following definition.

Definition 2: For all $n \in \mathbb{N}$*, the natural transitive cyclic group, denoted* $G_n \subseteq S_n$*, is the group generated by the permutation* $(1, 2, \dots, n)$*, i.e.,*

$$G_n \triangleq \langle (1, 2, \dots, n) \rangle = \{(1, 2, \dots, n)^k : k \in \mathbb{Z}\}. \quad (1)$$

It will additionally be helpful to have a notation for permutations that are close enough to the code. If $f, g \in S_n$ and $d(f, g) \leq \tilde{r}$, we say f is $\tilde{r}$*-covered by* g, and otherwise, we say f is $\tilde{r}$*-exposed by* g. If $C \subseteq S_n$ is a code, and $f \in S_n$ is $\tilde{r}$-covered by at least one $g \in C$, i.e., $d(f, C) \leq \tilde{r}$, we say f is $(\tilde{r}, C)$*-covered*. Otherwise, f is $\tilde{r}$-exposed by every $g \in C$, and we say f is $(\tilde{r}, C)$*-exposed*. In the latter case, for every $g \in C$, there exists $i \in [n]$ such that $|f(i) - g(i)| > \tilde{r}$, and we say that the mapping $i \mapsto f(i)$ is $\tilde{r}$*-exposed by* g.

III. The Covering Radius of the Cyclic Group

In this section we determine the covering radius of the natural transitive cyclic group. This will later be used as a component in a more general construction for covering codes. We first present two bounds on the covering radius, that nearly agree. We then close the small gap to obtain the exact covering radius.

Throughout this section, let $G_n \subseteq S_n$ denote the natural transitive cyclic group of (1). Since for $n = 1, 2$, we have $G_n = S_n$, we trivially have $r(G_1) = r(G_2) = 0$. Thus, in what follows we focus on $n \geq 3$.

If $f \in S_n$ is some permutation, $H \subseteq S_n$ a subgroup, and $\tilde{r} \in \mathbb{N}$, we define

$$A^H_{i \mapsto f(i)} \triangleq \{h^{-1}(1) \ : \ i \mapsto f(i) \text{ is } \tilde{r}\text{-exposed by } h \in H\}.$$

Since we will be mainly interested in the case of $H = G_n$, we define

$$A_{i\mapsto f(i)} \triangleq A^{G_n}_{i\mapsto f(i)}.$$

We also define the two sets

$$B \triangleq [n-\tilde{r}-1], \qquad T \triangleq [\tilde{r}+2, n],$$

for the bottom and top parts of the range $[n]$. In these definitions, to keep the notation simple, the dependence of B and T on n and $\tilde{r}$ is implicit. Some simple observations are formalized in the next two lemmas.

Lemma 3: Let $f \in S_n$ be any permutation, and $\tilde{r} \in \mathbb{N}$. If $H \subseteq S_n$ is a transitive group and $|H| = n$, then f is $(\tilde{r}, H)$-exposed if and only if

$$\bigcup_{i\in[n]} A^H_{i\mapsto f(i)} = [n]. \tag{2}$$

Proof: If (2) holds, since $|H| = n$, it follows that every $h \in H$ $\tilde{r}$-exposes f, hence f is $(\tilde{r}, H)$-exposed. In the other direction, if f is $(\tilde{r}, H)$-exposed, then every $h \in H$ $\tilde{r}$-exposes some mapping $i \mapsto f(i)$. Since $\bigcup_{h\in H}\left\{h^{-1}(1)\right\} = [n]$, the claim follows. ∎

Lemma 4: Let $\tilde{r}, n \in \mathbb{N}$, $\tilde{r} \geq \frac{n}{2}-1$, and let $H \subseteq S_n$ be a transitive subgroup with $|H| = n$. Then for all $i, j \in [n]$,

$$\left|A^H_{i\mapsto j}\right| = \begin{cases} n-\tilde{r}-j, & j \in B = [n-\tilde{r}-1], \\ j-\tilde{r}-1, & j \in T = [\tilde{r}+2, n], \\ 0 & \textit{otherwise.} \end{cases}$$

In particular, for $H = G_n$, for all $j_B \in B$, $j_T \in T$, and $i_B, i_T \in [n]$,

$$\begin{aligned} A_{i_B\to j_B} &= [i_B+1, i_B+n-\tilde{r}-j_B] \bmod^+ n, \\ A_{i_T\to j_T} &= [i_T-j_T+\tilde{r}+2, i_T] \bmod^+ n. \end{aligned}$$

Proof: Consider the first claim. If $i \mapsto j$, $j \in B$, is $\tilde{r}$-exposed by some $h \in H$, then $h(i) \in [j+\tilde{r}+1, n]$. Thus, since H is transitive and $|H| = n$, there are exactly $n-\tilde{r}-j$ such $h \in H$, proving the claim regarding the size of $A^H_{i\mapsto j}$.

Additionally, when considering $H = G_n \triangleq \langle(1, 2, \ldots, n)\rangle$, we know $h^{-1}(1) = (i_B - h(i_B) + 1) \bmod^+ n$. Combining this with the range of $h(i_B)$ we get

$$A_{i_B\to j_B} = [i_B+1, i_B+n-\tilde{r}-j_B] \bmod^+ n.$$

The rest of the claims, involving T, i_T, and j_T, are proven symmetrically. ∎

We can now prove an upper bound on the covering radius of G_n.

Lemma 5: For all $n \in \mathbb{N}$, $n \geq 3$,

$$r(G_n) \leq n - \left\lceil \frac{\sqrt{4n+1}-1}{2} \right\rceil.$$

Proof: Let $f \in S_n$ be any permutation, and consider any $\tilde{r} \in \mathbb{N}$ in the range $\frac{n}{2}-1 \leq \tilde{r} \leq n-1$. Using Lemma 4,

$$\begin{aligned} \left|\bigcup_{i\in[n]} A_{i\mapsto f(i)}\right| &\leq \sum_{i\in[n]} \left|A_{i\mapsto f(i)}\right| \\ &= \sum_{\substack{i\in[n] \\ f(i)\in B}} \left|A_{i\mapsto f(i)}\right| + \sum_{\substack{i\in[n] \\ f(i)\in T}} \left|A_{i\mapsto f(i)}\right| \\ &= \sum_{j\in B}(n-\tilde{r}-j) + \sum_{j\in T}(j-\tilde{r}-1) \\ &= 2\sum_{i=1}^{n-\tilde{r}-1} i = (n-\tilde{r}-1)(n-\tilde{r}). \end{aligned} \tag{3}$$

By Lemma 3, if

$$(n-\tilde{r}-1)(n-\tilde{r}) < n, \tag{4}$$

then f is $(\tilde{r}, G_n)$-covered. The smallest value of $\tilde{r}$ that satisfies (4) is

$$\tilde{r} = n - \left\lceil \frac{\sqrt{4n+1}-1}{2} \right\rceil,$$

and since for any $\tilde{r}$ that satisfies (4) we have $r(G_n) \leq \tilde{r}$, we obtain the desired bound. ∎

We now move on to a lower bound on the covering radius of G_n.

Lemma 6: For all $n \in \mathbb{N}$, $n \geq 3$,

$$r(G_n) \geq n - \left\lfloor \frac{\sqrt{4n+1}+1}{2} \right\rfloor.$$

Proof: By simple inspection, $r(G_3) = 1$, agreeing with the claim. We therefore focus on the remaining case of $n \geq 4$. For convenience we define

$$a \triangleq \left\lfloor \frac{\sqrt{4n+1}+1}{2} \right\rfloor, \qquad \tilde{r} \triangleq n-a-1.$$

The proof strategy is the following: we shall define a permutation $f_0 \in S_n$ and show that f_0 is $(\tilde{r}, G_n)$-exposed. It would then follow that $r(G_n) \geq \tilde{r}+1 = n-a$, which would complete the proof.

We construct a permutation $f_0 \in S_n$ as follows:

$$\begin{aligned} f_0(i) &\triangleq \begin{cases} n-a+k, & i = \binom{k+1}{2}, \quad k \in [a], \\ a-\ell+1, & i = 2\binom{a+1}{2} - 1 - \binom{\ell+1}{2}, \quad \ell \in [a], \\ \text{arbitrary}, & \text{otherwise}, \end{cases} \\ &= \begin{cases} j_T, & i = \binom{a-(n-j_T)+1}{2}, \quad j_T \in T, \\ j_B, & i = 2\binom{a+1}{2} - 1 - \binom{a-(j_B-1)+1}{2}, \quad j_B \in B, \\ \text{arbitrary}, & \text{otherwise}, \end{cases} \end{aligned} \tag{5}$$

for all $i \in [n]$, and where arbitrary entries are set in a way that completes f_0 to a permutation.

We first contend that f_0 is well defined. We note that since $n \geq 4$ we have $B \cap T = \emptyset$, so the values in the range of f_0

are distinct. As for the domain, the first two cases of (5) are disjoint, since otherwise we would have $k, \ell \in [a]$ such that

$$\binom{k+1}{2} + \binom{\ell+1}{2} = 2\binom{a+1}{2} - 1.$$

This obviously does not hold for $k = \ell = a$, as well as $k, \ell \in [a-1]$. The only remaining case is when $\{k, \ell\} = \{a, a-1\}$. However, it is easy to verify that

$$\binom{a+1}{2} + \binom{a}{2} = 2\binom{a+1}{2} - 1,$$

only when $a = 1$, which is never the case when $n \geq 4$. Hence, f_0 is indeed a well defined permutation.

We now proceed with showing that f_0 is $(\tilde{r}, G_n)$-exposed. By examining the first case of (5) and using Lemma 4, we obtain for all $j_T \in T$,

$$\begin{aligned}
&\bigcup_{j_T \in T} A_{f_0^{-1}(j_T) \mapsto j_T} \\
&= \bigcup_{k \in [a]} \left[\binom{k+1}{2} - k + 1, \binom{k+1}{2} \right] \bmod^+ n \\
&= \left[\binom{a+1}{2} \right] \bmod^+ n.
\end{aligned}$$

Symmetrically, let $\ell' \in [a]$ be the smallest integer such that

$$2\binom{a+1}{2} - 1 - \binom{\ell'+1}{2} \leq n.$$

Then by Lemma 4,

$$\begin{aligned}
&\bigcup_{j_B \in B} A_{f_0^{-1}(j_B) \mapsto j_B} \\
&= \bigcup_{\ell \in [\ell', a]} \left[2\binom{a+1}{2} - \binom{\ell+1}{2}, \right. \\
&\qquad \left. 2\binom{a+1}{2} - \binom{\ell+1}{2} + \ell - 1 \right] \bmod^+ n \\
&= \left[\binom{a+1}{2}, 2\binom{a+1}{2} - 1 - \binom{\ell'}{2} \right] \bmod^+ n.
\end{aligned}$$

We now note that

$$\begin{aligned}
&2\binom{a+1}{2} - 1 \\
&= \left\lfloor \frac{\sqrt{4n+1}+1}{2} \right\rfloor \left(\left\lfloor \frac{\sqrt{4n+1}+1}{2} \right\rfloor + 1 \right) - 1 \\
&> \frac{\sqrt{4n+1}-1}{2} \cdot \frac{\sqrt{4n+1}+1}{2} - 1 \\
&= n - 1,
\end{aligned}$$

and since the expression on the left-hand side is an integer, we get

$$2\binom{a+1}{2} - 1 \geq n.$$

Additionally, the choice of ℓ' ensures that also

$$2\binom{a+1}{2} - 1 - \binom{\ell'}{2} \geq n.$$

TABLE I

THE ENTRIES OF f_0 THAT ARE EXPLICIT IN THE PROOF OF LEMMA 5, THE PERMUTATIONS IN G_7 BY WHICH THEY ARE 3-EXPOSED, AND THE RELEVANT $A_{i \mapsto f_0(i)}$ SETS

f_0	3-exposed by	$A_{i \mapsto f_0(i)}$
$1 \mapsto 5$	g^0	$A_{1 \mapsto 5} = [1] = \{1\}$
$3 \mapsto 6$	g^5, g^6	$A_{3 \mapsto 6} = [2,3] = \{2,3\}$
$6 \mapsto 7$	g^2, g^3, g^4	$A_{6 \mapsto 7} = [4,6] = \{4,5,6\}$
$5 \mapsto 1$	g^0, g^1, g^2	$A_{5 \mapsto 1} = [6,8] \bmod^+ 7 = \{6,7,1\}$

It then follows that

$$\bigcup_{i \in [n]} A_{i \mapsto f_0(i)} = [n],$$

and by Lemma 3, f_0 is $(\tilde{r}, G_n)$-exposed. ■

Example 7: For $n = 7$, from (5) *we get*

$$f_0 = [5, ?, 6, ?, 1, 7, ?],$$

where ? represents entries that can be mapped arbitrarily so as to complete a permutation from S_7. Denote $g = (1, 2, 3, 4, 5, 6, 7)$, so that $G_7 = \langle g \rangle$. Table I shows the entries of f_0 which were mapped to $B \cup T$, and the permutations $g^k \in G_7$ by which they are 3-exposed. It also details the relevant $A_{i \mapsto f_0(i)}$ sets. We conclude that $r(G_7) \geq 4$, since f_0 is $(3, G_7)$-exposed. From Lemma 5 we have $r(G_7) \leq 4$. Thus $r(G_7) = 4$. □

The upper bound of Lemma 5 and the lower bound of Lemma 6 do not match exactly. The gap between the two is eliminated in the following theorem, by improving the upper bound, thus giving the exact covering radius of G_n.

Theorem 8: For all $n \in \mathbb{N}$,

$$r(G_n) = n - \left\lfloor \frac{\sqrt{4n+1}+1}{2} \right\rfloor.$$

Proof: For $n = 1, 2$ we already know that $r(G_n) = 0$, agreeing with the claimed expression. Therefore we consider $n \geq 3$. By Lemma 5 and Lemma 6 we have

$$n - \left\lfloor \frac{\sqrt{4n+1}+1}{2} \right\rfloor \leq r(G_n) \leq n - \left\lceil \frac{\sqrt{4n+1}-1}{2} \right\rceil.$$

Using straightforward analysis, one can see that the lower and upper bounds agree, except when $n = t(t+1)$, $t \in \mathbb{N}$, where there is a gap of 1 between the bounds. To prove the claim we shall strengthen the upper bound to match the lower bound.

For the remainder of the proof we focus on the case of $n = t(t+1)$, $t \in \mathbb{N}$. In this case, there is no need for the floor or ceiling operations, and we would like to prove that

$$r(G_n) = n - \frac{\sqrt{4n+1}+1}{2} = t^2 - 1.$$

Denote $\tilde{r} \triangleq t^2 - 1$, and assume to the contrary that there exists $f \in S_n$ that is $(\tilde{r}, G_n)$-exposed. Then,

$$\begin{aligned}
n &\overset{(a)}{=} \left| \bigcup_{j \in [n]} A_{f^{-1}(j) \mapsto j} \right| \leq \sum_{j \in [n]} \left| A_{f^{-1}(j) \mapsto j} \right| \\
&\overset{(b)}{=} (n - \tilde{r} - 1)(n - \tilde{r}) = t(t+1) = n,
\end{aligned}$$

where (a) follows from Lemma 3, and (b) is taken from (3). It follows that the sets $A_{f^{-1}(j)\mapsto j}$, $j \in [n]$, are all disjoint, and they form a partition of $[n]$.

Define a *B-set* to be any set of the form $A_{f^{-1}(j_B)\mapsto j_B}$, with $j_B \in B$, and a *T-set* to be any set $A_{f^{-1}(j_T)\mapsto j_T}$, with $j_T \in T$. Since $\tilde{r} \geq \frac{n}{2} - 1$, we have $B \cap T = \emptyset$, and thus no B-set is also a T-set. As noted above, the B-sets and T-sets partition $[n]$, and therefore there exists some T-set immediately to the left (cyclically) of a B-set. More precisely, there exist $j_B \in B$ and $j_T \in T$ such that

$$\begin{aligned} A_{f^{-1}(j_T)\mapsto j_T} &= [k, k+\ell_T] \bmod^+ n, \\ A_{f^{-1}(j_B)\mapsto j_B} &= [k+\ell_T+1, k+\ell_T+\ell_B] \bmod^+ n, \end{aligned}$$

for some $k, \ell_B, \ell_T \in [n]$. But by Lemma 4,

$$\begin{aligned} A_{f^{-1}(j_T)\to j_T} &= [f^{-1}(j_T) - j_T + \tilde{r} + 2, f^{-1}(j_T)] \bmod^+ n, \\ A_{f^{-1}(j_B)\to j_B} &= [f^{-1}(j_B) + 1, \\ &\qquad f^{-1}(j_B) + n - \tilde{r} - j_B] \bmod^+ n, \end{aligned}$$

implying $f^{-1}(j_B) = f^{-1}(j_T)$, and therefore $j_B = j_T$, but then $B \cap T \neq \emptyset$, a contradiction. ■

IV. Codes Constructed From the Cyclic Group

Using G_n as a covering code, now that its covering radius has been determined, has severe limitations. Most notably, there is just one code of each length, and no flexibility in code parameters. We overcome this by providing a more general code construction which uses G_n as an internal building block. This construction is a generalization of the covering-code construction of [6] and [25] . It enables us to construct a covering code $C_n \subseteq S_n$, using existing covering codes $C_m \subseteq S_m$, $m \leq n$.

A. Code Construction and Parameters

Before describing the construction we first define permutation projections.

Definition 9: Let $I = \{i_1, i_2, \dots, i_m\} \subseteq [n]$ be a subset of indices, $i_1 < i_2 < \dots < i_m$. For a permutation $f \in S_n$ we define $f|_I$ to be the permutation in S_m that preserves the relative order of the sequence $f(i_1), f(i_2), \dots, f(i_m)$, i.e., $g = f|_I$ if for all $j, j' \in [m]$, we have $g(j) < g(j')$ if and only if $f(i_j) < f(i_{j'})$. We also define

$$f|^I \triangleq \left(f^{-1}|_I\right)^{-1}.$$

Intuitively, from the definition above, to compute $f|_I$ we take its one-line notation, keep only the *coordinates* of f from I, and then rename them to the elements of $[m]$ while keeping the relative order. In contrast, to compute $f|^I$, we keep only the one-line notation *values* of f that are from I, and rename those to $[m]$ while keeping the relative order.

Example 10: Let $n = 6$, $f = [6, 1, 3, 5, 2, 4] \in S_6$, and $I = \{3, 5, 6\}$. Then

$$f|_I = [2, 1, 3],$$

since we keep entries 3, 5, and 6 of f, giving us $[3, 2, 4]$, which we then rename to $[2, 1, 3]$. Similarly, we have

$$f|^I = [3, 1, 2],$$

since we keep the values 3, 5, and 6 of f, giving us $[6, 3, 5]$, which we then rename to $[3, 1, 2]$. □

To simplify notation, it will become convenient to define a projection using the empty set. Thus, for $I = \emptyset$ and $f \in S_n$ we define $f|_I = f|^I \triangleq []$, where $[]$ denotes the unique permutation over zero elements.

We now present the code construction.

Construction A: Let $m, n \in \mathbb{N}$, $m \leq n$. We define the indices sets

$$I_i \triangleq [im+1, (i+1)m] \cap [n],$$

for all $i \in [0, \lfloor \frac{n}{m} \rfloor]$. We construct the code $C_n \subseteq S_n$ defined by

$$C_n \triangleq \left\{ f \in S_n \ : \ f|^{I_i} \in C_{|I_i|}, i \in \left[0, \left\lfloor \frac{n}{m} \right\rfloor\right] \right\},$$

where $C_{|I_i|} \subseteq S_{|I_i|}$ are covering codes, called the building-block codes. □

We note that in the above construction, all the indices sets are of size m, except for the last one which is of size $n \bmod m$. Thus, when $m|n$ the last indices set is empty, and $C_0 \triangleq \{[]\} = \{\mathrm{Id}\} \subseteq S_0$ is degenerate, containing only the unique empty (identity) permutation. We define $r(C_0) \triangleq 0$. We also mention that a more general construction is possible, in which the indices sets form an arbitrary partition of $[n]$.

The code construction of [6] and [25] is a special case of Construction A, in which $C_m \triangleq \{\mathrm{Id}\} \subseteq S_m$, and $C_{n \bmod m} \triangleq \{\mathrm{Id}\} \subseteq S_{n \bmod m}$.

Lemma 11: The code C_n from Construction A is an (n, M, r) code, where

$$M = \frac{n!}{(m!)^{\lfloor n/m \rfloor}(n \bmod m)!} \left|C_m\right|^{\lfloor n/m \rfloor} \left|C_{n \bmod m}\right|,$$

and

$$r = \max\left\{r(C_m), r(C_{n \bmod m})\right\}.$$

Proof: The cardinality of the code, M, is easily obtainable by noting that we first need to partition the n coordinates into $\lfloor \frac{n}{m} \rfloor$ sets of size m, and one set of size $n \bmod m$. There are

$$\binom{n}{m, m, \dots, m, n \bmod m} = \frac{n!}{(m!)^{\lfloor n/m \rfloor}(n \bmod m)!}$$

ways of doing so. We then assign values to each set from the corresponding set I_i. The number of ways to do so is exactly $|C_m|^{\lfloor n/m \rfloor} |C_{n \bmod m}|$.

The covering radius is also straightforward. Given a permutation $f \in S_n$, assume the values of I_i are found in positions given by $J_i \subseteq [n]$. By the properties of the code $C_{|I_i|}$, there exists a codeword $g \in C_n$, such that the restrictions of f and g to positions J_i are at most $r(C_{|I_i|})$ distance apart. Since we can make this hold for all $i \in [0, \lfloor \frac{n}{m} \rfloor]$ simultaneously, we have

$$r \leq \max\left\{r(C_m), r(C_{n \bmod m})\right\}.$$

This is met with equality, since we can easily find a permutation $f \in S_n$ within this distance from C_n: take $f' \in S_m$

such that $d(f', C_m) = r(C_m)$. Construct $f \in S_n$ such that $f|^{I_0} = f'$ and then $d(f, C_n) \geq r(C_m)$. If necessary, repeat analogously for $C_{n \bmod m}$ to obtain a permutation $f \in S_n$ such that $d(f, C_n) \geq r(C_{n \bmod m})$. ■

Next, we take a closer look at this code construction using G_n as the building-block code.

Corollary 12: Let $m, n \in \mathbb{N}$, $m \leq n$. Then the code C_n from Construction A, with building-block codes $C_m = G_m$ and $C_{n \bmod m} = G_{n \bmod m}$, is an (n, M, r) code, where

$$M = \begin{cases} \frac{n!}{((m-1)!)^{\frac{n}{m}}}, & n \equiv 0 \pmod{m}, \\ \frac{n!}{((m-1)!)^{\lfloor \frac{n}{m} \rfloor}((n \bmod m)-1)!}, & n \not\equiv 0 \pmod{m}, \end{cases}$$

and

$$r = m - \left\lfloor \frac{\sqrt{4m+1}+1}{2} \right\rfloor.$$

Here we use the convention that $G_0 = \{[]\}$.

Proof: The proof follows from substituting the parameters of the cyclic group into Lemma 11, and noting that $r(G_m)$ is monotone non-decreasing in m. ■

Lemma 13: Let $n, m \in \mathbb{N}$, $m \leq n$. Then the code C_n of Construction A with $C_m = G_m$ and $C_{n \bmod m} = G_{n \bmod m}$, has the following rate,

$$R = -\rho \left\lfloor \frac{1}{\rho} \right\rfloor \log_2 \rho - \left(1 - \rho \left\lfloor \frac{1}{\rho} \right\rfloor\right) \log_2 \left(1 - \rho \left\lfloor \frac{1}{\rho} \right\rfloor\right) + o(1), \quad (6)$$

where $\rho \triangleq \rho(C_n)$ is the normalized covering radius of C_n, $R \triangleq R(C_n)$ is the rate of C_n, and $o(1)$ denotes a function that tends to 0 as n tends to infinity.

Proof: From Corollary 12

$$\rho = \frac{r(C_n)}{n-1} = \frac{m - \left\lfloor \frac{\sqrt{4m+1}+1}{2} \right\rfloor}{n-1} = \frac{m}{n} - o(1).$$

Therefore, $m = n\rho + o(n)$. Notice that $n \bmod m = n - m \left\lfloor \frac{n}{m} \right\rfloor$, hence, by rewriting $|C_n|$ from Corollary 12 we get

$$\begin{aligned} |C_n| &= 2^{Rn} \\ &= \frac{n!}{(m!)^{\lfloor \frac{n}{m} \rfloor}(n \bmod m)!} m^{\lfloor \frac{n}{m} \rfloor}(n \bmod m) \\ &= \frac{n! \cdot \ (n\rho + o(n))^{\left\lfloor \frac{n}{n\rho+o(n)} \right\rfloor}}{((n\rho+o(n))!)^{\left\lfloor \frac{n}{n\rho+o(n)} \right\rfloor}} \\ &\quad \cdot \frac{\left(n - (n\rho+o(n))\left\lfloor \frac{n}{n\rho+o(n)} \right\rfloor\right)}{\left(n - (n\rho+o(n))\left\lfloor \frac{n}{n\rho+o(n)} \right\rfloor\right)!}. \end{aligned}$$

It is now a matter of using Stirling's approximation (e.g., [8]),

$$n! = \left(\frac{n}{e}\right)^n 2^{o(n)},$$

and standard analysis techniques, to arrive at the desired form. ■

We observe that (6) is the same as the rate obtained by the construction of [6] and [25], which uses only $C_m = \{\mathrm{Id}\}$. However, the rate is a rather crude measure. Upon closer inspection, we shall now show the code parameters of Corollary 12 are superior to those of [6] and [25] along certain asymptotics. We first provide an example.

Example 14: Describing an arbitrary permutation from S_{24} requires $\log_2(24!) \approx 79$ bits of information. If instead of describing the arbitrary permutation precisely we allow a distortion of at most 8 in the ℓ_∞-norm, then using the covering-code construction of [6] and [25], a code C'_{24} of length $n = 24$ and covering radius 8 has size

$$\left|C'_{24}\right| = \frac{24!}{9!^2 \cdot 6!},$$

requiring $\log_2 \left|C'_{24}\right| \approx 32.6$ bits. However, by choosing $n = 24$ and $m = 12$, the code C_{24} from Construction A using these parameters also has covering radius

$$r(G_{12}) = 12 - \left\lfloor \frac{\sqrt{4 \cdot 12 + 1}+1}{2} \right\rfloor = 8,$$

and size

$$|C_{24}| = \frac{24!}{11!^2}.$$

Thus, only $\log_2 |C_{24}| \approx 28.5$ bits are required. □

Let us consider the case of $n = tm$, where $t, m \in \mathbb{N}$. We use Construction A with $C_m = G_m$ to obtain a code we denote as C_n^{cyc}. This code has cardinality given by Corollary 12,

$$M_n^{\mathrm{cyc}} = \frac{(mt)!}{((m-1)!)^t}.$$

Its covering radius is

$$r \triangleq r(C_n^{\mathrm{cyc}}) = m - \left\lfloor \frac{\sqrt{4m+1}+1}{2} \right\rfloor.$$

For a fair comparison with the code of [6] and [25], we construct one with the same length n, and same covering radius r. Such a code is a special case of Construction A using the building-block codes $C_{r+1} = \{\mathrm{Id}\}$ and $C_{n \bmod (r+1)} = \{\mathrm{Id}\}$. We call the resulting code C_n^{Id}, and its cardinality (see also [6]) is given by

$$M_n^{\mathrm{Id}} = \frac{(mt)!}{((r+1)!)^{\left\lfloor \frac{n}{r+1} \right\rfloor}(n \bmod (r+1))!}.$$

For the comparison, we first observe that

$$r \leq m - \sqrt{m} + 1. \quad (7)$$

We also recall Stirling's approximation in more detail,

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \leq n! \leq \sqrt{2\pi n} \cdot e^{\frac{1}{12n}} \left(\frac{n}{e}\right)^n. \quad (8)$$

We now have

$$\begin{aligned} M_n^{\mathrm{cyc}} &= \frac{(tm)! \cdot m^t}{(m!)^t} \\ &\overset{\text{(a)}}{\leq} \frac{\sqrt{2\pi tm}\left(\frac{tm}{e}\right)^{tm} e^{\frac{1}{12tm}} \cdot m^t}{\left(\frac{m}{e}\right)^{tm}(2\pi m)^{\frac{t}{2}}} \\ &\overset{\text{(b)}}{\leq} 2\sqrt{t} \cdot m^t t^{tm}, \end{aligned}$$

where (a) is obtained by using (8), and (b) is by rearrangement and noting that $e^{\frac{1}{12tm}} \leq 2$.

To bound M^{Id} we write

$$n = tm = q(r+1) + s,$$

where $q, s \in \mathbb{Z}$, $s \in [0, r]$. We then have

$$\begin{aligned}
M_n^{\mathrm{Id}} &= \frac{(tm)!}{((r+1)!)^q \cdot s!} \\
&\overset{(a)}{\geq} \frac{\sqrt{2\pi tm}\left(\frac{tm}{e}\right)^{tm}}{(2\pi(r+1))^{\frac{q}{2}} e^{\frac{q}{12(r+1)}} \left(\frac{r+1}{e}\right)^{(r+1)q}} \\
&\quad \cdot \frac{1}{(2\pi s)^{\frac{1}{2}} e^{\frac{q}{12(r+1)}+\frac{1}{12s}} \left(\frac{s}{e}\right)^s} \\
&\overset{(b)}{\geq} \frac{t^{tm}}{\left(\frac{r+1}{m}\right)^{(r+1)q} \left(\frac{s}{m}\right)^s 2^{2t+1}(2\pi tm)^t} \\
&\overset{(c)}{\geq} \frac{t^{tm}}{\left(\frac{r+1}{m}\right)^{tm} 2^{2t+1}(2\pi tm)^t} \\
&\overset{(d)}{\geq} \frac{t^{tm}}{\left(1 - \frac{1}{\sqrt{m}} + \frac{2}{m}\right)^{tm} 2^{2t+1}(2\pi tm)^t} \\
&\overset{(e)}{\geq} \frac{t^{tm}}{\left(e^{-\sqrt{m}+2}\right)^t 2^{2t+1}(2\pi tm)^t},
\end{aligned}$$

where (a) is due to (8), (b) is by rearrangement and noting that $q \leq 2t$, (c) is due to $s \leq m$, (d) is due to (7), and (e) is due to $1 + x \leq e^x$. It now follows that

$$\frac{M^{\mathrm{cyc}}}{M^{\mathrm{Id}}} \leq 2^{2t+2}\sqrt{t}(2\pi t)^t \left(m^2\ e^{-\sqrt{m}+2}\right)^t.$$

Thus, for any fixed $t \in \mathbb{N}$, and m tending to infinity, the codes C_n^{cyc} are sub-exponentially better than C_n^{Id} of [6] and [25] in terms of size.

The comparison may be performed in a more general setting. Assume Construction A is used with length n and building-block codes G_m, where m does not necessarily divide n. Denote the size of the resulting code by $M_{n,m}^{\mathrm{cyc}}$ (see Corollary 12). For comparison, we take the construction of [6] and [25] of same length n, and same covering radius, $m - \left\lfloor \frac{\sqrt{4m+1}+1}{2} \right\rfloor$, and denote its size by $M_{n,m}^{\mathrm{Id}}$. Figure 1 shows a comparison between $M_{n,m}^{\mathrm{cyc}}$ and $M_{n,m}^{\mathrm{Id}}$. In particular, the dark ridges of Figure 1(a) along $n = tm$, $t \in \mathbb{N}$, are predicted by our previous analysis.

As a final note, we mention the fact that we may improve the parameters of Corollary 12 by picking $C_m = G_m$, but $C_{n \bmod m} = \{\mathrm{Id}\}$, whenever $(n \bmod m) - 1 \leq r(G_m)$, as this would decrease the resulting code size while maintaining its covering radius.

B. Covering-Codeword Algorithm

A common task associated with covering codes is, given a covering code $C \subseteq S_n$ and a permutation $f \in S_n$, to find a codeword $g \in C$ such that $d(f, g) \leq r(C)$, i.e., find a codeword covering f. The code G_n has only few codewords, and a trivial algorithm measuring the distance between the given f and each of the n codewords of G_n (returning an $r(G_n)$-covering codeword) runs in $O(n^2)$ time. However, this might be improved upon, and we now describe a more efficient algorithm.

Algorithm 1 Finding a Covering Codeword $g \in G_n$

Input: any permutation $f \in S_n$
Output: a codeword $g \in G_n$ with $d(f, g) \leq r(G_n)$
Initialization: V is an array of size n, $V[i] \leftarrow 0$, $\forall i \in [n]$, $a \leftarrow \left\lfloor \frac{\sqrt{4n+1}-1}{2} \right\rfloor$
for $i = 1$ to n **do**
  if $f(i) \leq a$ **then**
    for $j = i+1$ to $i + a - (f(i) - 1)$ **do**
      $V\left[j \bmod^+ n\right] \leftarrow 1$
    end for
  else if $f(i) \geq n - a + 1$ **then**
    for $j = i - (a - (n - f(i))) + 1$ to i **do**
      $V\left[j \bmod^+ n\right] \leftarrow 1$
    end for
  end if
end for
for $i = 1$ to n **do**
  if $V[i] = 0$ **then**
    return $[n-i+2, \ldots, n, 1, \ldots, n-i+1] \in G_n$
  end if
end for

Lemma 15: Let $n \in \mathbb{N}$ and $f \in S_n$. Algorithm 1 returns a codeword $g \in G_n$ such that $d(f, g) \leq r(G_n)$.

Proof: Let $\tilde{r} \triangleq r(G_n)$, which means $a = n - \tilde{r} - 1$. The inner loops on j assign 1 to the entries of V corresponding to the elements of $A_{i \mapsto f(i)}$ (see proof of Lemma 6). Hence, at the end of the first for loop on i,

$$V[i] = 0 \iff i \notin \bigcup_{i \in [n]} A_{i \mapsto f(i)}.$$

The second for loop on i finds $i \in [n]$ such that $V[i] = 0$. From Theorem 8, such i must exist. We conclude that the codeword $g \in G_n$, such that $g(i) = 1$, $\tilde{r}$-covers f, and we return it. ■

Algorithm 1 is more efficient than the trivial brute-force algorithm. We note that $a = O(\sqrt{n})$, and therefore, each of the inner loops is entered $O(\sqrt{n})$ times, performing $O(\sqrt{n})$ iterations each time. Thus, in total, the algorithm runs in $O(n)$ time.

Having this algorithm for the building-block code G_n, we may extend it in a natural way to the code studied in Corollary 12 to also run in $O(n)$ time. We omit the tedious details.

V. Relabeling the Cyclic Group

Following the definition of the *natural* transitive cyclic group,

$$G_n \triangleq \langle (1, 2, \ldots, n) \rangle \subseteq S_n,$$

as given in Definition 2, it is tempting to ask what happens when we take a non-natural transitive cyclic group.

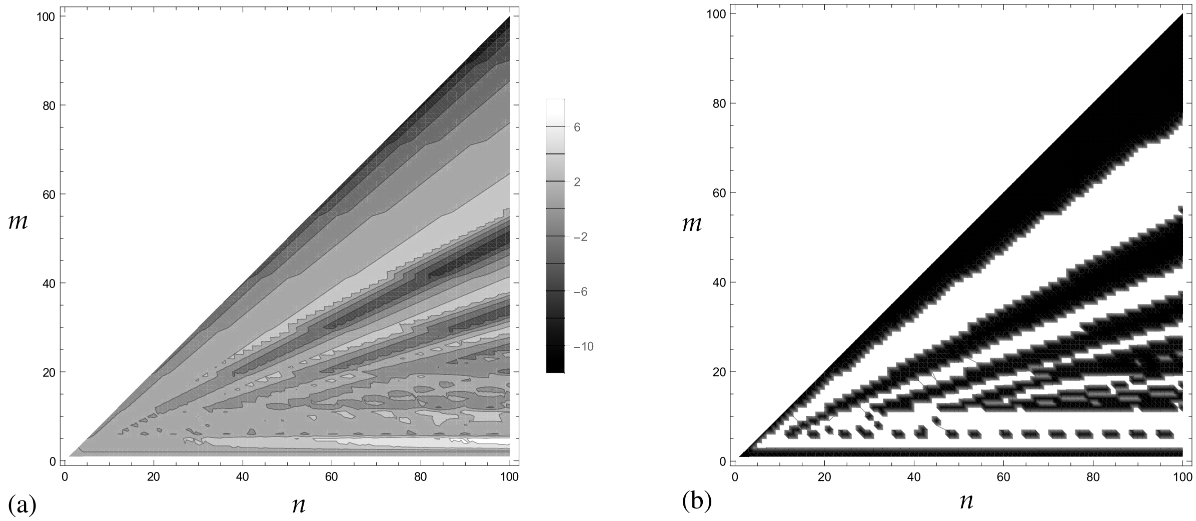

Fig. 1. A comparison between $M^{\mathrm{cyc}}_{n,m}$ and $M^{\mathrm{Id}}_{n,m}$, where (a) shows $\log_{10}(M^{\mathrm{cyc}}_{n,m}/M^{\mathrm{Id}}_{n,m})$ (darker colors imply values of n and m for which Construction A out-performs the construction of [6] and [25]), and (b) shows a black/white quantization of (a), where black positions imply $M^{\mathrm{cyc}}_{n,m} \geq M^{\mathrm{Id}}_{n,m}$.

Thus, we are interested in the groups of the form

$$G_n^h \triangleq hG_nh^{-1} \triangleq \left\langle h(1,2,\dots,n)h^{-1}\right\rangle = \langle (h(1),h(2),\dots,h(n))\rangle \subseteq S_n,$$

for some $h \in S_n$. A similar, more general question, was asked in [24], where an error-correcting code $C \subseteq S_n$ was *relabeled* by conjugation,

$$C^h \triangleq hCh^{-1} \triangleq \left\{hgh^{-1} \ : \ g \in C\right\},$$

$h \in S_n$, and its minimum distance was studied as a function of C and h. It was shown there that the minimum distance could drastically change due to relabeling, moving from the minimum possible 1, to the maximum possible $n-1$, for some codes. Additionally, every error-correcting code could be relabeled so that its minimum distance is reduced to either 1 or 2. In this section we study the covering radius of relabelings of G_n.

Definition 16: Let $C \subseteq S_n$ be a covering code. We denote by $\mathcal{L}_{\min}(C)$ (respectively, $\mathcal{L}_{\max}(C)$) the minimal (respectively, maximal) achievable covering radius among all relabelings of C, i.e.,

$$\mathcal{L}_{\min}(C) \triangleq \min_{h\in S_n} r(C^h),$$
$$\mathcal{L}_{\max}(C) \triangleq \max_{h\in S_n} r(C^h).$$

We first consider $\mathcal{L}_{\max}(G_n)$. Again, the cases of $n=1,2$ are degenerate, and we therefore only consider $n \geq 3$.

Theorem 17: For all $n \in \mathbb{N}$, $n \geq 3$,

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

Proof: Let $h \in S_n$ be any permutation. We begin by noting that since G_n is a transitive group, so is G_n^h. Thus, Lemma 3 and Lemma 4 apply. Now Lemma 5 also holds for G_n^h since it only relies on the two above-mentioned lemmas. Thus,

$$\mathcal{L}_{\max}(G_n) \leq n - \left\lceil \frac{\sqrt{4n+1}-1}{2} \right\rceil.$$

Additionally, whenever $n \neq t(t+1)$, $t \in \mathbb{N}$, we have by Theorem 8

$$\mathcal{L}_{\max}(G_n) \geq r(G_n) = n - \left\lfloor \frac{\sqrt{4n+1}+1}{2} \right\rfloor = n - \left\lceil \frac{\sqrt{4n+1}-1}{2} \right\rceil.$$

Let us define

$$a \triangleq \left\lceil \frac{\sqrt{4n+1}-1}{2} \right\rceil, \quad \tilde{r} \triangleq n-a-1.$$

To complete this proof, we must show that for values of n such that $n = t(t+1)$, $t \in \mathbb{N}$, $t \geq 2$, there exists $h \in S_n$ such that $r(G_n^h) = n-a$. Notice that in this case, $\frac{\sqrt{4n+1}-1}{2}$ is an integer, which yields $n = a(a+1)$.

We contend that the permutation $h \triangleq (1,2) \in S_n$ will suffice, proving it by constructing a permutation $f_0 \in S_n$ such that f_0 is $(\tilde{r}, G_n^h)$-exposed, giving us

$$r(G_n^h) \geq d(f_0, G_n^h) \geq \tilde{r}+1 = n-a.$$

We construct a permutation $f_0 \in S_n$ as follows:

$$f_0(i) \triangleq \begin{cases} 1, & i=1, \\ n, & i=2, \\ n-a+1, & i=3, \\ a-k, & i=\binom{k+1}{2}+a+2, \\ & k\in[0,a-2], \\ n-a+1+\ell, & i=n-a+2-\binom{\ell+1}{2}, \\ & \ell \in [a-2], \\ \text{arbitrary}, & \text{otherwise}, \end{cases} \tag{9}$$

for all $i \in [n]$, and where arbitrary entries are set in a way that completes f_0 to a permutation.

We first note that f_0 is well defined. The domain intervals in the definition are disjoint since $a \geq 2$, $n = a(a+1) = 2\binom{a+1}{2}$, and

$$\binom{a-1}{2} + a + 2 < 2\binom{a+1}{2} - a + 2 - \binom{a-1}{2}.$$

As for the range intervals, the fourth and fifth cases in (9) are $[2, a]$ and $[n-a+2, n-1]$ respectively, and are clearly disjoint, and disjoint from the first three cases. These two sets will be of further interest, so we define

$$\tilde{B} \triangleq B \setminus \{1\} = [2, a],$$
$$\tilde{T} \triangleq T \setminus \{n-a+1, n\} = [n-a+2, n-1].$$

Thus, $\tilde{B} \cap \tilde{T} = \emptyset$.

With $g \triangleq (1, 2, \dots, n) \in S_n$, and $G_n \triangleq \langle g \rangle$, we write the elements of G_n^h explicitly,

$$\begin{aligned} h_0 &\triangleq hg^0h^{-1} = [1, 2, \dots, n], \\ h_1 &\triangleq hg^1h^{-1} = [3, 1, 4, 5, \dots, n, 2], \\ h_2 &\triangleq hg^2h^{-1} = [4, 3, 5, 6, \dots, n, 2, 1], \\ h_i &\triangleq hg^ih^{-1} = [i+2, i+1, i+3, i+4, \dots, n, \\ &\qquad 2, 1, 3, 4, \dots, i], \quad i \in [3, n-3], \\ h_{n-2} &\triangleq hg^{n-2}h^{-1} = [n, n-1, 2, 1, 3, 4, \dots, n-2], \\ h_{n-1} &\triangleq hg^{n-1}h^{-1} = [2, n, 1, 3, 4, \dots, n-1]. \end{aligned}$$

To prove that f_0 is $(\tilde{r}, G_n^h)$-exposed we shall use Lemma 3.

The mapping $1 \mapsto f_0(1) = 1$ is $\tilde{r}$-exposed by $\{h_{n-a-1}, h_{n-a}, \dots, h_{n-2}\}$, hence,

$$A_{1\mapsto 1}^{G_n^h} = [4, a+3].$$

The mapping $2 \mapsto f_0(2) = n$ is $\tilde{r}$-exposed by $\{h_0, h_1, \dots, h_{a-1}\}$, hence

$$\begin{aligned} A_{2\mapsto n}^{G_n^h} &= [n-a+3, n+2] \bmod^+ n \\ &= \{n-a+3, n-a+4, \dots, n, 1, 2\}. \end{aligned}$$

The mapping $3 \mapsto f_0(3) = n-a+1$ is $\tilde{r}$-exposed solely by h_{n-1}, thus

$$A_{2\mapsto n-a+1}^{G_n^h} = \{3\}.$$

Now consider a mapping $i_B \mapsto f_0(i_B) = j_B$, with $j_B \in \tilde{B}$, and we get

$$A_{i_B\mapsto j_B}^{G_n^h} = [i_B + 2, i_B + 2 + a - j_B],$$

and in total,

$$\begin{aligned} \bigcup_{j_B \in \tilde{B}} A_{f_0^{-1}(j_B)\mapsto j_B}^{G_n^h} &= \left[a+4, \binom{a+1}{2} + 3\right] \\ &= \left[a+4, \frac{n}{2} + 3\right]. \end{aligned}$$

Similarly, for $i_T \mapsto f_0(i_T) = j_T$ such that $j_T \in \tilde{T}$ we get

$$A_{i_T\mapsto j_T}^{G_n^h} = [i_T + n - j_T - a + 2, i_T + 1],$$

and in total,

$$\begin{aligned} \bigcup_{j_T \in \tilde{T}} A_{f_0^{-1}(j_T)\mapsto j_T}^{G_n^h} &= \left[n - \binom{a+1}{2} + 4, n - a + 2\right] \\ &= \left[\frac{n}{2} + 4, n - a + 2\right]. \end{aligned}$$

In conclusion, taking the union of all the above we obtain

$$\bigcup_{j \in [n]} A_{f_0^{-1}(j)\mapsto j}^{G_n^h} = [n],$$

and by Lemma 3 we have that f_0 is $(\tilde{r}, G_n^h)$-exposed. ∎

We now move on to studying $\mathcal{L}_{\min}$. Unlike $\mathcal{L}_{\max}$, we provide only a weak lower bound on $\mathcal{L}_{\min}$, which depends only on the size of the code. We recall the definition of a ball of radius r and centered at $g \in S_n$,

$$\mathcal{B}_{n,r}(g) \triangleq \{f \in S_n \ : \ d(f, g) \leq r\}.$$

Since the ℓ_∞-metric is right invariant, the size of a ball does not depend on the choice of center, and thus we denote its size as $|\mathcal{B}_{n,r}|$.

Lemma 18: Let $C \subseteq S_n$ be a code. If $\tilde{r} \in \mathbb{N}$ is such that

$$|C| \cdot |\mathcal{B}_{n,\tilde{r}-1}| < |S_n|, \tag{10}$$

then

$$\mathcal{L}_{\min}(C) \geq \tilde{r}.$$

Proof: The claim is quite trivial. Inequality (10) simply states that $|C|$ balls of radius $\tilde{r} - 1$ cannot cover S_n, hence $r(C) \geq \tilde{r}$. For all $h \in S_n$ we have $|C| = |C^h|$, hence $r(C^h) \geq \tilde{r}$. ∎

Specializing Lemma 18 to $|C| = n$, gives us the following corollary, which applies to G_n as well.

Corollary 19: For all large enough $n \in \mathbb{N}$, if $C \subseteq S_n$ with $|C| = n$, then

$$\mathcal{L}_{\min}(C) \geq n - \left\lceil \sqrt{2n \ln n + 2n} \right\rceil.$$

Proof: The following upper bound on the size of a ball is given in [15],

$$|\mathcal{B}_{r,n}| \leq \begin{cases} ((2r+1)!)^{\frac{n-2r}{2r+1}} \prod_{i=r+1}^{2r} (i!)^{\frac{2}{i}}, & 0 \leq r \leq \frac{n-1}{2}, \\ (n!)^{\frac{2r+2-n}{n}} \prod_{i=r+1}^{n-1} (i!)^{\frac{2}{i}}, & \frac{n-1}{2} \leq r \leq n-1, \end{cases}$$

and whose proof is an immediate application of Bregman's upper bound on the permanent. We contend that only the second case of this bound is of relevance to us, as we will prove shortly. Thus, if we find $\tilde{r} \geq \frac{n+1}{2}$ such that

$$\begin{aligned} \frac{|C| \cdot |\mathcal{B}_{n,\tilde{r}-1}|}{|S_n|} &= \frac{|\mathcal{B}_{n,\tilde{r}-1}|}{(n-1)!} \\ &\leq \frac{1}{(n-1)!} (n!)^{\frac{2\tilde{r}-n}{n}} \prod_{i=\tilde{r}}^{n-1} (i!)^{\frac{2}{i}} < 1, \end{aligned} \tag{11}$$

then by Lemma 18 we will have $\mathcal{L}_{\min}(C) \geq \tilde{r}$.

Let us therefore define the auxiliary function,

$$F(n,\tilde{r}) \triangleq \frac{1}{(n-1)!}(n!)^{\frac{2\tilde{r}-n}{n}}\prod_{i=\tilde{r}}^{n-1}(i!)^{\frac{2}{i}}.$$

As a first step we show that for all $n \geq 11$,

$$F\left(n,\left\lceil\frac{n+1}{2}\right\rceil\right) < 1.$$

Due to parity, we consider the cases of even n and odd n separately. We shall prove the former, and omit the proof for odd n since it is similar. For the case of even n, we prove the claim for $n = 12$, and then show the function is monotonically decreasing in n.

For $n = 12$ we have,

$$F(12,7) \approx 0.9644 < 1.$$

Next, we consider

$$\begin{aligned}\frac{F\left(n,\frac{n+2}{2}\right)}{F\left(n+2,\frac{n+4}{2}\right)} &= \frac{n\cdot(n!)^{\frac{2-n}{n}}\cdot\prod_{i=\frac{n+2}{2}}^{n-1}(i!)^{\frac{2}{i}}}{(n+2)\cdot((n+2)!)^{-\frac{n}{n+2}}\cdot\prod_{i=\frac{n+4}{2}}^{n+1}(i!)^{\frac{2}{i}}}\\ &= \frac{n(n+1)\cdot\left(\left(\frac{n+2}{2}\right)!\right)^{\frac{4}{n+2}}}{((n+2)!)^{\frac{2}{n+2}}\cdot\ ((n+1)!)^{\frac{2}{n+1}}}\\ &\geq \frac{e^2}{4}\cdot\frac{n}{(n+1)\cdot\ (\pi\ \ (n+2))^{\frac{1}{(n+1)(n+2)}}}\\ &\quad\cdot\frac{1}{e^{\frac{1}{6}\left(\frac{1}{(n+1)^2}+\frac{1}{(n+2)^2}\right)}}\end{aligned}$$

where for the inequality we used (8) and trivial bounding techniques. We now note that $\exp(\frac{1}{6}\left((n+1)^{-2}+(n+2)^{-2}\right))$ and $(\pi\ \ (n+2))^{\frac{1}{(n+1)(n+2)}}$ are monotonically decreasing in n, and $\frac{n}{n+1}$ is monotonically increasing. Hence,

$$\frac{F\left(n,\frac{n+2}{2}\right)}{F\left(n+2,\frac{n+4}{2}\right)} \geq \frac{F\left(12,7\right)}{F\left(14,8\right)} \approx 1.649 > 1,$$

and so $F\left(n,\left\lceil\frac{n+1}{2}\right\rceil\right)$ is monotonically decreasing in n for even n. A similar proof holds for odd n.

Thus far we showed there exists $\tilde{r} \geq \frac{n+1}{2}$ that satisfies (11) (in particular, $\tilde{r} = \lceil(n+1)/2\rceil$ does). We would now like to find such $\tilde{r}$ as large as possible. We observe the following sequence of inequalities, where we take $n \geq 1$, and $\frac{n+1}{2} \leq \tilde{r} \leq n-1$.

$$\begin{aligned}F(n,\tilde{r}) &\triangleq \frac{1}{(n-1)!}(n!)^{\frac{2\tilde{r}-n}{n}}\prod_{i=\tilde{r}}^{n-1}(i!)^{\frac{2}{i}}\\ &\overset{(a)}{\leq} n\cdot\left(\frac{n}{e}\right)^{2\tilde{r}-2n}\cdot\prod_{i=\tilde{r}}^{n-1}(2\pi i)^{\frac{1}{i}}e^{\frac{1}{6i}}\left(\frac{i}{e}\right)^2\\ &\overset{(b)}{\leq} n\cdot n^{2\tilde{r}-2n}\cdot(2\pi\tilde{r})^{\frac{n-\tilde{r}}{\tilde{r}}}e^{\frac{n-\tilde{r}}{6\tilde{r}}}\left(\frac{(n-1)!}{(\tilde{r}-1)!}\right)^2\\ &\overset{(c)}{\leq} n\cdot n^{2\tilde{r}-2n}\cdot\pi n e^{\frac{1}{6}}\cdot\left(\frac{(n-1)!}{(\tilde{r}-1)!}\right)^2\\ &\overset{(d)}{\leq} \pi e^{\frac{1}{6}}e^{\frac{1}{6(n-1)}}e^{2\tilde{r}-2n}n^2\cdot\frac{\left(\frac{n-1}{n}\right)^{2n}\frac{1}{n-1}}{\left(\frac{\tilde{r}-1}{n}\right)^{2\tilde{r}}\frac{1}{\tilde{r}-1}}\\ &\overset{(e)}{\leq} \pi e^{-\frac{109}{60}}e^{2\tilde{r}-2n}n^2\cdot\frac{1}{\left(\frac{\tilde{r}-1}{\tilde{r}}\right)^{2\tilde{r}}\left(\frac{\tilde{r}}{n}\right)^{2\tilde{r}}}\\ &\overset{(f)}{\leq} \pi e^{-\frac{109}{60}}\left(\frac{6}{5}\right)^{12}\cdot e^{2\tilde{r}-2n}n^2\left(\frac{n}{\tilde{r}}\right)^{2\tilde{r}},\end{aligned} \tag{12}$$

where (a) follows from (8), (b) follows by noting that $(2\pi i)^{\frac{1}{i}}$ and $e^{\frac{1}{6i}}$ are decreasing in i and then replacing i by $\tilde{r}$, (c) follows by noting that $(2\pi\tilde{r})^{\frac{n-\tilde{r}}{\tilde{r}}}$ and $e^{\frac{n-\tilde{r}}{6\tilde{r}}}$ are decreasing in $\tilde{r}$ and replacing $\tilde{r}$ by $\frac{n}{2}$, (d) follows again by use of (8), (e) follows by noting that $\exp(\frac{1}{6(n-1)})$ is decreasing in n and substituting $n = 11$, that $((n-1)/n)^{2n} \leq e^{-2}$, and that $\frac{\tilde{r}-1}{n-1} < 1$, and finally, (f) follows by noting that $((\tilde{r}-1)/\tilde{r})^{2\tilde{r}}$ is increasing in $\tilde{r}$ and replacing $\tilde{r}$ (since $n \geq 11$ and $\tilde{r} \geq \frac{n}{2}$) by $\tilde{r} = 6$.

We note that taking $\tilde{r} = n-\sqrt{2n\ln n+2n}$, by (12) we get

$$\lim_{n\to\infty}F(n,n-\sqrt{2n\ln n+2n}) \leq \pi e^{-\frac{109}{60}}\left(\frac{6}{5}\right)^{12}\frac{1}{e^2} < 1.$$

It now follows that for large enough n,

$$F(n,n-\sqrt{2n\ln n+2n}) < 1,$$

and then

$$\mathcal{L}_{\min}(C) \geq n-\left\lceil\sqrt{2n\ln n+2n}\right\rceil,$$

as claimed. ■

VI. Discussion

In this paper we studied covering codes over permutations with the ℓ_∞-metric. We presented a general construction for such codes, Construction A, which uses short building-block codes and combines them into a single longer covering code. This construction is a generalization of the construction appearing both in [6] and [25], noted by choosing the building-block code to be the trivial {Id}.

To improve the overall code parameters, we studied a new building-block code, the naturally labeled transitive cyclic group G_n. This building-block code has length n, size $|G_n| = n$, and covering radius

$$r(G_n) = n-\left\lfloor\frac{\sqrt{4n+1}+1}{2}\right\rfloor,$$

which was determined in Theorem 8. At this point, it is interesting to ask whether the covering radius of G_n may be changed by relabeling, following the example set in [24] for error-correcting codes. It turns out, by Theorem 17 and Corollary 19, that for all large enough n, and all $h \in S_n$,

$$n-\left\lceil\sqrt{2n\ln n+2n}\right\rceil \leq r(G_n^h) \leq n-\left\lceil\frac{\sqrt{4n+1}-1}{2}\right\rceil,$$

implying that the covering radius of G_n is robust under relabeling, in contrast to the volatility of the minimum distance of G_n under relabeling (see [24]). In particular, relabeling does not increase the covering radius of G_n by more than 1.

Finally, we described in Construction A a method of combining short building-block codes into a single longer covering code, C_n. The construction uses a parameter $1 \leq m \leq n$, and results in a code of length n. When used with trivial building-block codes {Id}, Construction A becomes the construction described in [6] and [25], with resulting code size $|C_n| = \frac{n!}{(m!)^{\lfloor n/m \rfloor}(n \bmod m)!}$, and covering radius $r(C_n) = m - 1$. However, when replacing the building-block code with G_m, Construction A provides a code of size

$$|C_n| = \begin{cases} \frac{n!}{((m-1)!)^{\frac{n}{m}}}, & n \equiv 0 \pmod{m}, \\ \frac{n!}{((m-1)!)^{\lfloor \frac{n}{m} \rfloor}((n \bmod m)-1)!}, & n \not\equiv 0 \pmod{m}, \end{cases}$$

and covering radius $r(C_n) = m - \left\lfloor \frac{\sqrt{4m+1}+1}{2} \right\rfloor$, as shown in Corollary 12. Additionally, the code of Construction A admits a linear-time algorithm for decoding.

The methods we described may be extended to larger groups, e.g., the dihedral group, though at a cost of a growing gap between the lower and upper bounds on the covering radius. Thus, in the case of the naturally labeled dihedral group, $D_n \subseteq S_n$, defined by,

$$D_n \triangleq \left\langle (1, 2, \ldots, n), \prod_{i=1}^{\lfloor n/2 \rfloor} (i, n-i) \right\rangle,$$

we can obtain

$$\begin{aligned} n - \left\lfloor \frac{\sqrt{4n+1}+1}{2} \right\rfloor &\geq r(D_n) \\ &\geq \begin{cases} n - \left\lceil \frac{\sqrt{288n+297}-3}{16} \right\rceil, & n \in [4, 9], \\ n - \left\lceil \frac{\sqrt{288n+737}-1}{16} \right\rceil, & n \in [10, 911], \\ n - \left\lceil \frac{\sqrt{18n-18}}{4} \right\rceil, & n \geq 912. \end{cases} \end{aligned}$$

The tedious proof follows the same logic as that presented in Section III, and the interested reader may find it in [13]. We believe a more elegant treatment is needed.

Another gap exhibited in this work is between $\mathcal{L}_{\min}(G_n)$ and $\mathcal{L}_{\max}(G_n)$. First, we note an interesting contrast with the case of error-correcting codes (as described in [24]). When relabeling error-correcting codes, the minimum distance of *any* code, including G_n, may be reduced to either 1 or 2. The minimum distance of G_n is $\lceil n/2 \rceil$, and the best possible minimum distance after relabeling is $n - \left\lceil \frac{\sqrt{4n-3}-1}{2} \right\rceil$, which bears a striking resemblance to $r(G_n)$.

In light of Section III and Section V, it appears that the covering radius of G_n and its conjugate, has much less variance. This is evident from the small gap between $\mathcal{L}_{\min}(G_n)$ and $\mathcal{L}_{\max}(G_n)$, not to mention the fact that $r(G_n) = \mathcal{L}_{\max}(G_n)$ in most cases. We ran a brute-force computer search, checking all possible relabelings of G_n, $n \in [3, 10]$. For this range,

$$\mathcal{L}_{\min}(G_n) = r(G_n) = \mathcal{L}_{\max}(G_n),$$

for all $n \in [3, 10] \setminus \{6\}$, and

$$\mathcal{L}_{\min}(G_6) = r(G_6) = \mathcal{L}_{\max}(G_6) - 1,$$

where of the 6! labeling permutations, 264 give covering radius $3 = r(G_n)$, and 456 give covering radius $4 = \mathcal{L}_{\max}(G_n)$. The gap between $r(G_6)$ and $\mathcal{L}_{\max}(G_6)$ is a consequence of Theorem 17. It is now tempting to conjecture that for all $n \in \mathbb{N}$, $\mathcal{L}_{\min}(G_n) = r(G_n)$. We leave this conjecture, and the determination of the covering radius of other groups, as open questions for future work.

Acknowledgments

The authors would like to thank the associate editor and 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] P. J. Cameron and I. M. Wanless, "Covering radius for sets of permutations," *Discrete Math.*, vol. 293, pp. 91–109, Apr. 2005.

[3] 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.

[4] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: North-Holland, 1997.

[5] M. Deza and T. Huang, "Metrics on permutations, a survey," *J. Combinatorics, Inf. Syst. Sci.*, vol. 23, pp. 173–185, 1998.

[6] F. Farnoud, M. Schwartz, and J. Bruck, "Bounds for permutation rate-distortion," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 703–712, Feb. 2016.

[7] 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.

[8] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*. Reading, MA, USA: Addison-Wesley, 1994.

[9] A. E. Holroyd. (2016). "Perfect snake-in-the-box codes for rank modulation." [Online]. Available: https://arxiv.org/abs/1602.08073

[10] M. Horovitz and T. Etzion, "Constructions of snake-in-the-box codes for rank modulation," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7016–7025, Nov. 2014.

[11] 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.

[12] 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.

[13] R. Karni, "Permutation covering codes under the infinity metric," M.S. thesis, Dept. Elect. Comput. Eng., Ben-Gurion Univ. Negev, Beersheba, Israel, 2016.

[14] P. Keevash and C. Y. Ku, "A random construction for permutation codes and the covering radius," *Des., Codes Cryptograph.*, vol. 41, no. 1, pp. 79–86, 2006.

[15] T. Kløve, "Spheres of permutations under the infinity norm—Permutations with limited displacement," Dept. Inform., Univ. Bergen, Bergen, Norway, Tech. Rep. 376, Nov. 2008.

[16] T. Kløve, "Generating functions for the number of permutations with limited displacement," *Electron. J. Combinat.*, vol. 16, no. 1, pp. 1–11, 2009.

[17] T. Kløve, "Lower bounds on the size of spheres of permutations under the Chebychev distance," *Des., Codes Cryptograph.*, vol. 59, nos. 1–3, pp. 183–191, 2011.

[18] 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.

[19] A. Mazumdar, A. Barg, and G. Zemor, "Constructions of rank modulation codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1018–1029, Feb. 2013.

[20] J. Quistorff, "A survey on packing and covering problems in the Hamming permutation space," *Electron. J. Combinat.*, vol. 13, pp. 1–13, Apr. 2006.

[21] M. Schwartz and I. Tamo, "Optimal permutation anticodes with the infinity norm via permanents of (0, 1)-matrices," *J. Combinat. Theory A*, vol. 118, no. 6, pp. 1761–1774, Aug. 2011.
[22] D. Slepian, "Permutation modulation," *Proc. IEEE*, vol. 53, no. 3, pp. 228–236, Mar. 1965.
[23] 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.
[24] I. Tamo and M. Schwartz, "On the labeling problem of permutation group codes for the infinity metric," *IEEE Trans. Inf. Theory*, vol. 58, no. 10, pp. 6595–6604, Oct. 2012.
[25] D. Wang, A. Mazumdar, and G. W. Wornell, "Compression in the space of permutations," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6417–6431, Dec. 2015.
[26] X. Wang and F.-W. Fu. (2016). "Constructions of snake-in-the-box codes under the ℓ_∞-metric for rank modulation." [Online]. Available: https://arxiv.org/abs/1601.05539
[27] Y. Yehezkeally and M. Schwartz, "Snake-in-the-box codes for rank modulation," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5471–5483, Aug. 2012.
[28] Y. Yehezkeally and M. Schwartz, "Limited-magnitude error-correcting Gray codes for rank modulation," in *Proc. IEEE Int. Symp. Inf. Theory*, Barcelona, Spain, Jul. 2016, pp. 2829–2833.
[29] Y. Zhang and G. Ge, "Snake-in-the-box codes for rank modulation under Kendall's τ-metric," *IEEE Trans. Inf. Theory*, vol. 62, no. 1, pp. 151–158, Jan. 2016.
[30] H. Zhou, M. Schwartz, A. A. Jiang, and J. Bruck, "Systematic error-correcting codes for rank modulation," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 17–32, Jan. 2015.

Ronen Karni received his B.A. from the Department of Computer Science in 2005, and his M.Sc. from the Department of Electrical and Computer Engineering in 2016, both in Ben-Gurion University of the Negev. His research interests include coding theory.

Moshe Schwartz (M'03–SM'10) is an associate professor at the Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Israel. His research interests include algebraic coding, combinatorial structures, and digital sequences.

Prof. Schwartz 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. While on sabbatical 2012–2014, he was a visiting scientist at the Massachusetts Institute of Technology (MIT).

Prof. Schwartz received the 2009 IEEE Communications Society Best Paper Award in Signal Processing and Coding for Data Storage.