Codes in Permutations and Error Correction for Rank Modulation

Alexander Barg*,† Arya Mazumdar*

***Abstract*—Codes for rank modulation have been recently proposed as a means of protecting flash memory devices from errors. We study basic coding theoretic problems for such codes, representing them as subsets of the set of permutations of n elements equipped with the Kendall tau distance. We derive several lower and upper bounds on the size of codes. These bounds enable us to establish the exact scaling of the size of optimal codes for large values of n. We also show the existence of codes whose size is within a constant factor of the sphere packing bound for any fixed number of errors.**

I. Introduction

Codes in permutations form a classical subject of coding theory. Various metric functions on the symmetric group $\mathfrak{S}_n$ have been considered, giving rise to diverse combinatorial problems. The most frequently studied metric on $\mathfrak{S}_n$ is the Hamming distance. Codes in $\mathfrak{S}_n$ with the Hamming distance, traditionally called permutation arrays, have been a subject of a large number of papers; see, e.g., the works by Blake et al. [1] and Colbourn et al. [5].

In this paper we are interested in a different metric on $\mathfrak{S}_n$ which we proceed to define. Let $\sigma = (\sigma(1), \dots, \sigma(n))$ be a permutation of the set $[n] = \{1, 2, \dots, n\}$. The *Kendall tau distance* $d_\tau(\sigma, \pi)$ from σ to another permutation π is defined as the minimum number of transpositions of pairwise adjacent elements required to change σ into π. Denote by $X_n = (\mathfrak{S}_n, d_\tau)$ the metric space of permutations on n elements equipped with the distance d_τ.

The Kendall distance originates in statistics and has been adopted as a measure of quality of codes under the so-called rank modulation scheme first considered by Chadwick and Kurz [3]. In this scheme, the transmitted sequences are given by permutations of n elements while information is carried by the relative magnitude (rank) of elements in the permutation rather than by the absolute value of the elements. The motivation for considering this scheme in [3] stems from systems in which transmitted signals are subjected to impulse noise that changes the value of the signal substantially but has less effect on the relative magnitude of the neighboring signals. Recently (and independently of [3]) rank modulation was suggested by Jiang et al. [7], [8] as a means of efficient writing of information into flash memories. Rewriting the contents of a group of memory cells is easy if one needs to increase the charges of the cells or leave some of them unchanged and impractical if some of the charges need to be decreased. Furthermore, reliability of the data stored in flash memory is affected by the drift in the charge of the cells caused for instance by aging devices or other reasons. Since the drift in different cells may occur at different speed, errors introduced in the data are adequately accounted for by tracking the relative value of adjacent cells, i.e., the Kendall distance between the groups of cells in memory. These considerations make rank modulation suitable for coding for flash memories. More details of both the writing and the error processes in memory are given in [7] and references in that paper.

The focus of our work is on bounds and constructions of codes in the Kendall space X_n. Coding-theoretic considerations call for estimating the volume of the sphere in X_n because it can be used to derive basic bounds on the size of codes. As it turns out, results available in the literature do not lead to meaningful bounds on the code size. Regarding specific code families for correcting Kendall errors, the only previous work is that by Jiang et al. [7] who constructed a family of single-error-correcting codes of size $M \geq \frac{1}{2}(n-1)!$, i.e., at least half the maximum possible.

Our results. In this paper we discuss several possible ways to bound the size of codes for rank modulation of a given distance, often calling them rank permutation codes. Since the maximum value of the distance in X_n is $\binom{n}{2}$, this leaves a number of possibilities for the scaling rate of the distance for asymptotic analysis, ranging from $d = O(n)$ to $d = \Theta(n^2)$. These turn out to be the two extremes for the size of optimal rank permutation codes. Namely, earlier work in combinatorics of permutations implies that a code with distance $d = \Theta(n^2)$ occupies a vanishing proportion of the space X_n while a code of distance $O(n)$ can take a close-to-one proportion of its volume. We cover the intermediate cases, showing that the size of optimal codes with distance $d \sim n^{1+\epsilon}, 0 < \epsilon < 1$ scales as $\exp((1-\epsilon)n \ln n)$. It is interesting that unlike many other asymptotic coding problems, the Kendall space of permutations affords an exact answer for the growth rate of the size of optimal codes. The proof of the bounds relies on weight-preserving embeddings of X_n into other metric spaces which provide insights into the asymptotic size of codes.

We also show the existence of a family of rank permutation

This work was supported by NSF grants CCF0830699, CCF0916919, CCF0635271, and DMS0807411. A more detailed version of this paper is available as a preprint, arXiv:0908.4094.

*Department of ECE and Institute for Systems Research, University of Maryland, College Park, 20742, USA.
†Dobrushin Mathematical Laboratory, Institute for Problems of Information Transmission, Russian Academy of Science, Moscow, Russia.
Authors' e-mails: {abarg,arya}@umd.edu.

codes that correct a constant number of errors and have size within a constant factor of the sphere packing bound. The construction relies on the well-known Bose-Chowla Theorem in additive number theory.

Section II of our paper is devoted to the relation of the Kendall metric space to other metric spaces related to permutations. In Section III we use these insights to derive bounds on codes for rank modulation, and conduct their asymptotic analysis. Section IV contains a construction of t-error-correcting rank permutation codes.

II. Weight-preserving embeddings of the Kendall metric space

We begin with recalling basic properties of the distance d_τ such as its relation to the number of inversions in the permutation, and weight-preserving embeddings of $\mathfrak{S}_n$ into other metric spaces. Their proofs and a detailed discussion are found for instance in Knuth [9].

The distance d_τ is a right-invariant metric which means that $d_\tau(\sigma_1,\sigma_2) = d_\tau(\sigma_1\sigma,\sigma_2\sigma)$ for any $\sigma,\sigma_1,\sigma_2 \in \mathfrak{S}_n$ where the operation is the usual multiplication of permutations. Therefore, we can define the weight of the permutation σ as its distance to the identity permutation $e=(1,2,\ldots,n)$.

Because of the invariance, the graph whose vertices are indexed by the permutations and edges connect permutations one Kendall step apart, is regular of degree $n-1$. At the same time it is not distance-regular, and so the machinery of algebraic combinatorics does not apply to the analysis of the code structure. The diameter of the space X_n equals $N \triangleq \binom{n}{2}$ and is realized by pairs of opposite permutations such as $(1,2,3,4)$ and $(4,3,2,1)$.

The main tool to study properties of d_τ is provided by the inversion vector of the permutation. An inversion in a permutation $\sigma \in \mathfrak{S}_n$ is a pair $(\sigma(i),\sigma(j))$ such that $i<j$ and $\sigma(i)>\sigma(j)$. It is easy to see that $d_\tau(\sigma,e) = I(\sigma)$, the total number of inversions in σ. Therefore, for any two permutations σ_1,σ_2 we have $d_\tau(\sigma_1,\sigma_2) = I(\sigma_2\sigma_1^{-1}) = I(\sigma_1\sigma_2^{-1})$. In other words,

$$d_\tau(\sigma,\pi) = |\{(i,j)\in[n]^2 : i\neq j, \pi(i)>\pi(j), \sigma(i)<\sigma(j)\}|.$$

To a permutation $\sigma\in\mathfrak{S}_n$ we associate an *inversion vector* $\boldsymbol{x}_\sigma \in G_n \triangleq \mathbb{Z}_2\times\cdots\times\mathbb{Z}_n$, where $\boldsymbol{x}_\sigma(i) = |\{j : j<i+1, \sigma(j)>\sigma(i+1)\}|, i=1,\ldots,n-1$ and $\mathbb{Z}_m$ is the set of integers modulo m. It is well known that the mapping from permutations to the space of inversion vectors is one-to-one, and any permutation can be easily reconstructed from its inversion vector. Moreover,

$$I(\sigma) = \sum_{i=1}^{n-1} x_\sigma(i). \tag{1}$$

For the type of errors that we consider below we introduce the following ℓ_1 distance function on G_n :

$$d(\boldsymbol{x},\boldsymbol{y}) = \sum_{i=1}^{n-1} |x(i)-y(i)| \qquad (\boldsymbol{x},\boldsymbol{y}\in G_n) \tag{2}$$

where the computations are performed over the integers, and write $\|\boldsymbol{x}\|$ for the corresponding weight function (this is not a properly defined norm because G_n is not a linear space). For instance, let $\sigma_1=(2,1,4,3), \sigma_2=(2,3,4,1)$, then $x_{\sigma_1}=101, x_{\sigma_2}=003$. To compute the distance $d_\tau(\sigma_1,\sigma_2)$ we find

$$I(\sigma_2\sigma_1^{-1}) = I((1,4,3,2)) = \|(0,1,2)\| = 3.$$

Observe that the mapping $\sigma\to\boldsymbol{x}_\sigma$ is a weight-preserving bijection between X_n and the set G_n. At the same time, since the groups $\mathfrak{S}_n$ and G_n are not isomorphic (one is commutative while the other is not), this mapping is not distance-preserving. However, a weaker property is true, namely,

$$d_\tau(\sigma_1,\sigma_2) \geq d(\boldsymbol{x}_{\sigma_1},\boldsymbol{x}_{\sigma_2}). \tag{3}$$

Indeed, transposing two neighboring entries of a permutation σ changes the inversion count $I(\sigma)$ by one, so the mapping $X_n\to G_n$ preserves distances to the identity permutation. Thus, if there exists a code in G_n with ℓ_1 distance d then there exists a code in X_n with Kendall distance at least d.

Another embedding of X_n is given by mapping each permutation to a binary N-dimensional vector $\boldsymbol{a}$ whose coordinates are indexed by the pairs $(i,j)\subset[n]^2, i<j$, and $a_{(i,j)}=1$ if the pair (i,j) is an inversion and $a_{(i,j)}=0$ otherwise. Clearly the Hamming weight of $\boldsymbol{a}$ equals $I(\sigma)$, and so this mapping is an isometry between X_n and a subset of the Hamming space. This mapping was first considered in [4].

III. Bounds on the size of rank permutation codes

An (n,M,d) code $\mathcal{C}\subset X_n$ is a set of M permutations in which any two distinct permutations are at least d distance units apart. Let $A(n,d)$ be the maximum size of the code in X_n with distance d. For the purposes of asymptotic analysis we define the rate of a code $\mathcal{C}\subset X_n$ of size M as $R(\mathcal{C}) = \frac{\ln M}{\ln n!}$. Let

$$\mathscr{C}(d) = \lim_{n\to\infty} \frac{\ln A(n,d)}{\ln n!}$$

be the capacity of rank permutation codes of distance d (our proof of Theorem 3.1 will imply that the limit exists). The main result of this section is given in the following theorem whose proof is given in Sections III-B and III-C below.

Theorem 3.1:

$$\mathscr{C}(d) = \begin{cases} 1 & \text{if } d=O(n) \\ 1-\epsilon & \text{if } d=\Theta(n^{1+\epsilon}),\ 0<\epsilon<1 \\ 0 & \text{if } d=\Theta(n^2). \end{cases} \tag{4}$$

A. A Singleton bound

Theorem 3.2: Let $d>n-1$, then

$$A(n,d) \leq \left\lfloor 3/2 + \sqrt{n(n-1)-2d+1/4}\right\rfloor !. \tag{5}$$

Proof : Let $\mathcal{C}$ be an (n,M,d) code. Since the metric d_τ is right invariant, we can assume that $\mathcal{C}$ contains the identity permutation e.

Let $k\leq n$ and $\mathcal{C}_k\in\mathfrak{S}_k$ be a code derived from $\mathcal{C}$ in the following way. Let $\phi_k:\mathfrak{S}_n\to\mathfrak{S}_k$ be a mapping that acts on σ by deleting elements $k+1,\ldots,n$ from it. Thus, $\phi_k(\sigma)$ is a

permutation on k elements that maintains the relative positions of the elements of $[k]$ given by σ.

Let k be the greatest number such that ϕ_k is not injective. Then ϕ_{k+1} is injective, and $M \le (k+1)!$. Suppose that permutations $\sigma_1, \sigma_2 \in \mathfrak{S}_n$ are such that $\phi_k(\sigma_1) = \phi_k(\sigma_2)$. Because of the last equality, none of the k symbols in $\sigma_2\sigma_1^{-1}$ contain pairs that form inversions. Therefore,

$$d \le d_\tau(\sigma_1, \sigma_2) \le \binom{n}{2} - \binom{k}{2}.$$

This gives $k \le 1/2(1 + \sqrt{4n(n-1) - 8d + 1})$, which proves inequality (5). This estimate is nontrivial if $\frac{3}{2} + \sqrt{n(n-1) - 2d + 1/4} < n$ which is equivalent to the condition $d > n - 1$. ∎

To gain insight into this bound, let $d = \delta N$. Using the inequality $m! \le (m/2)^m$ in (5), we obtain the asymptotic inequality

$$A(n,d) \le \exp(n(\ln n)\sqrt{1-\delta}(1 + c(\ln n)^{-1})),$$

where the constant c does not depend on n. As we will show in the next section, the $\sqrt{1-\delta}$ in this bound can in fact be improved to a quantity that decays as $(\ln n)^{-1}$ as n grows.

B. Sphere packing bounds

Denote by $B_r = B_r(X_n)$ the sphere of radius r in the Kendall space X_n. Clearly,

$$n!/|B_{2r}| \le A(n, 2r+1) \le n!/|B_r|. \tag{6}$$

The embeddings of X_n into other metric spaces considered in the previous section can be used to derive estimates of $A(n,d)$ based on these inequalities. In particular, computing the volume of the metric ball in G_n and using (3), we will derive a lower bound in (6). At the same time, both lower and upper bounds will follow from the embedding of X_n in the Hamming space H_N described above.

Let $K_n(k) = |\{\sigma \in \mathfrak{S}_n : I_n(\sigma) = k\}|$ be the number of permutations with k inversions. The next theorem is a combination of results of Margolius [11] and Louchard and Prodinger [10], stated here in the form suitable for our context.

Theorem 3.3: There exist constants c_1 and c_2 such that

$$\begin{aligned} K_n(k) &\le \exp(c_1 n) && \text{if } k = O(n), \\ K_n(k) &= n!/\exp(c_2 n) && \text{if } k = \Theta(n^2). \end{aligned}$$

The implicit constants in this theorem can be found in cited references.

From this theorem and inequalities (6), we obtain the two boundary cases of the expression for $\mathscr{C}(d)$ in (4).

C. Bounds from embedding in the ℓ_1 space

In this section we prove the remaining case of Theorem 3.1. Our idea is to derive bounds on $\mathscr{C}(d)$ by relating the Kendall metric to the ℓ_1 metric on $\mathfrak{S}_n$. From the results of Diaconis and Graham [6],

$$1/2 D(\sigma_1, \sigma_2) \le d_\tau(\sigma_1, \sigma_2) \le D(\sigma_1, \sigma_2). \tag{7}$$

where $D(\sigma_1, \sigma_2) = \sum_{i=1}^n |\sigma_1(i) - \sigma_2(i)|$. Therefore, any code $\mathcal{C} \subset \mathfrak{S}_n$ with Kendall distance d must have ℓ_1 distance at least d and any code $\mathcal{C} \subset \mathfrak{S}_n$ with ℓ_1 distance d must have Kendall distance at least $d/2$.

Proposition 3.4: Let $B_r(H_n, \boldsymbol{x})$ be the metric sphere of radius r with center at $\boldsymbol{x}$ in the space $H_n = \{1, 2, \dots, n\}^n$ with the ℓ_1 metric. Then the maximum size of a code in X_n with distance d satisfies

$$\frac{n!}{\max_{\boldsymbol{x} \in H_n} |B_{2d-1}(H_n, \boldsymbol{x})|} \le A(n,d) \le \frac{n^n}{\min_{\boldsymbol{x} \in H_n} |B_t(H_n, \boldsymbol{x})|},$$

where $t = \lfloor (d-1)/2 \rfloor$.

Proof: Under the trivial embedding $\mathfrak{S}_n \to H_n$ the ℓ_1 distance does not change, so any code $\mathcal{C}$ in $\mathfrak{S}_n$ with ℓ_1 distance d is also a code in H_n with the same distance and as such, must satisfy the Hamming bound. Together with (7) this gives the upper bound of our statement.

Turning to the lower bound, let us perform the standard "Gilbert procedure" in the space of permutations with respect to the ℓ_1 distance, aiming for a code $\mathcal{D}$ with ℓ_1 distance m. The resulting code satisfies

$$|\mathcal{D}| \max_{\sigma \in \mathfrak{S}_n} |B_{m-1}(\mathfrak{S}_n, \sigma)| \ge n!.$$

Since $|B_r(H_n, \sigma)| \ge |B_r(\mathfrak{S}_n, \sigma)|$, we can replace the volume in $\mathfrak{S}_n$ with the volume in H_n in the last inequality. Viewed as a packing of X_n, the code $\mathcal{D}$ will then have Kendall distance at least $m/2$. ∎

Below we consider only spheres in the space H_n and omit the reference to it from the notation $B_r(H_n, \cdot)$.

Lemma 3.5: Let $\mathbf{1} = (1, 1, \dots, 1) \in H_n$. Then for any $\boldsymbol{z}, \boldsymbol{y} \in H_n$,

$$2^{-n}|B_r(\boldsymbol{z})| \le |B_r(\mathbf{1})| \le |B_r(\boldsymbol{y})|.$$

Proof: Suppose that $\boldsymbol{x} = (x_1, x_2, \dots, x_n) \in B_r(\mathbf{1})$ and $\mathbf{1} \ne \boldsymbol{y} = (y_1, y_2, \dots, y_n) \in H_n$. Consider the mapping $\zeta : B_r(\mathbf{1}) \to B_r(\boldsymbol{y})$ where $\boldsymbol{x} \mapsto \boldsymbol{u}$, where $\boldsymbol{u} = (u_1, u_2, \dots, u_n)$ is given by

$$u_i = \begin{cases} y_i + (x_i - 1) & \text{if } y_i + (x_i - 1) \le n \\ n - (x_i - 1) & \text{if } y_i + (x_i - 1) > n. \end{cases}$$

Clearly $\boldsymbol{u} \in H_n$ and $x_1 - 1 \ge |u_i - y_i|$ for $i = 1, \dots, n$, so every point within distance r of $\mathbf{1}$ is sent to a point within distance r of $\boldsymbol{y}$. Furthermore, this mapping is injective because if $\boldsymbol{x}_1, \boldsymbol{x}_2$ are two distinct points in $B_r(\mathbf{1})$ then their images can coincide only if in some coordinates

$$y_i + (x_{1,i} - 1) = n - (x_{2,i} - 1).$$

However, the left-hand side of this equality is $\ge y_i$ while the right-hand side is $< y_i$ by definition of u_i. This proves the right inequality.

To prove the lower bound, write $B_r(\boldsymbol{z})$ as $\boldsymbol{z} + D_r(\boldsymbol{z})$, where $D_r(\boldsymbol{z})$ is the set of differences:

$$D_r(\boldsymbol{z}) = \{\boldsymbol{u} \in \mathbb{Z}^n : |u_i| \le n-1, 1 \le i \le n; \sum_{i=1}^n |u_i| \le r \text{ and } \boldsymbol{z} + \boldsymbol{u} \in H_n\}.$$

Writing $B_r(\mathbf{1})$ in the same way as $\mathbf{1} + D_r^+$, we have

$$D_r^+ = \{\boldsymbol{u} \in \mathbb{Z}^n : 0 \le u_i \le n-1;\ \sum_{i=1}^{n} |u_i| \le r\}.$$

By taking the absolute values of the coordinates, any point in $D_r(\boldsymbol{z})$ is sent to a point in D_r^+, and no more than 2^n points have the same image under this mapping. This proves our claim. ∎

These arguments give rise to the next proposition.

Proposition 3.6:

$$\frac{n!}{2^n \sum_{r=0}^{2d-1} Q(n,r)} \le A(n,d) \le \frac{n^n}{\sum_{r=0}^{t} Q(n,r)}, \qquad (8)$$

where $Q(n,r) = \sum_{i\ge 0}(-1)^i \binom{n}{i}\binom{n+r-ni-1}{r-ni}$.
This claim is almost obvious because, by the previous lemma,

$$\frac{n!}{2^n |B_{2d-1}(\mathbf{1})|} \le |\mathcal{C}| \le \frac{n^n}{|B_t(\mathbf{1})|}$$

Next,

$$|B_s(\mathbf{1})| = \sum_{r=0}^{s} Q(n,r),$$

where $Q(n,r)$ is the number of integer solutions of the equation $x_1 + x_2 + \ldots + x_n = r$, where $0 \le x_1 \le n-1$, $1 \le i \le n$. The expression for $Q(n,r)$ given in the statement is well known.

In the remainder of this section we estimate the asymptotic behavior of this bound and derive an estimate of the code capacity.

Lemma 3.7: Suppose that $r < n^2/\ln n$. Then

$$\binom{n+r-1}{r} - n\binom{r-1}{r-n} \le Q(n,r) \le \binom{n+r-1}{r}.$$

From the foregoing arguments we now have the following explicit bounds on $A(n,d)$:

$$\frac{n!}{2^n \binom{n+2d-1}{2d-1}} \le A(n,d) \le \frac{n^n}{\sum_{r=0}^{t}\left(\binom{n+r-1}{r} - n\binom{r-1}{r-n}\right)}. \quad (9)$$

Here the right part is obvious and for the left inequality we used (8), Lemma 3.7, and the identity $\sum_{i\le n}\binom{s+i}{i} = \binom{s+n+1}{n}$.

Now we are ready to complete the proof of Theorem 3.1. Assume that $d = \Theta(n^{1+\epsilon})$ for some $0 < \epsilon < 1$. From (9),

$$A(n,d) \le \frac{n^n}{\binom{n+t-1}{n-1} - n\binom{t-1}{t-n}}$$

It can be shown that starting with some n we can estimate the denominator below by $1/2\binom{n+t-1}{n-1}$. Therefore,

$$A(n,d) \le \frac{2n^n}{\binom{n+t-1}{t}} \le \frac{2n^n(n-1)^{n-1}}{(n+t-1)^{n-1}}.$$

Next

$$\frac{\ln A(n,\Theta(n^{1+\epsilon}))}{n\ln n} \le 2 - (1+\epsilon) + o(1) = 1 - \epsilon + o(1).$$

On the other hand, using

$$\binom{n+2d-1}{2d-1} \le \left(\frac{(n+2d)e}{n}\right)^n < (2e^2)^n\Theta(n^{n\epsilon})$$

and $n! > (n/3)^n$, we obtain from (9)

$$A(n,d) \ge \frac{n^n}{(12e^2)^n\Theta(n^{n\epsilon})}.$$

Taking the logarithms and the limit, we find that $\mathscr{C}(d) \ge 1-\epsilon$. This completes the proof of Theorem 3.1.

D. Bounds from embedding in Hamming space

Since the embedding of X_n into the Hamming space $\mathcal{H}_N$ of dimension $N = \binom{n}{2}$ is isometric, the known results for codes correcting Hamming errors can be used to derive estimates and constructions for codes in the Kendall space.

Given the image of a code $\mathcal{C} \subset X_n$ in $\mathcal{H}_N$ it is easy to reconstruct the code $\mathcal{C}$ itself. Indeed, it is immediate to find the inversion vector of a permutation σ given the image of σ in $\mathcal{H}_N$, and then to recover σ from its inversion vector.

Of course, not every code in $\mathcal{H}_N$ will have a code in X_n corresponding to it. The next simple proposition shows that nevertheless, binary codes in $\mathcal{H}_N$ can be used to claim existence of good rank permutation codes.

Proposition 3.8: Suppose that there exists a binary linear $[\binom{n}{2}, k]$ code $\mathcal{A}$. Then there exists an $(n, \ge \frac{n!}{2^{N-k}}, d)$ rank permutation code.

For example, using binary BCH codes we can show the existence of a t-error-correcting rank permutation code of size $\frac{n!}{(N+1)^t} = \frac{n!}{O(n^{2t})}$. This falls short of the sphere-packing bound which implies that the size of a t-error-correcting code in X_n is at most $M \le O(\frac{n!}{n^t})$. In the next section we use a different method to construct codes that achieve the sphere packing bound to within a constant factor for any given t.

IV. Towards optimal t-error-correcting codes

The representation of permutations by inversion vectors provides a way to construct error-correcting rank permutation codes. In this section we construct codes in the ℓ_1 space of inversion vectors G_n and claim the existence of rank permutation codes by the inequality on the code distances (3).

We begin with constructing codes over the integers that correct additive errors. Once this is accomplished, we will be able to claim existence of good rank permutation codes. Let A be some subset of $\mathbb{Z}$ and let A^L be the space of L-tuples of integers from A equipped with the ℓ_1 distance (2). A code $\mathcal{D} \subset A^L$ is said to correct t additive errors if for any two distinct code vectors $\boldsymbol{x}, \boldsymbol{y}$ and any $\boldsymbol{e}_1, \boldsymbol{e}_2 \in \mathbb{Z}^L$, both of weight at most t,

$$\boldsymbol{x} + \boldsymbol{e}_1 \ne \boldsymbol{y} + \boldsymbol{e}_2.$$

We assume that A and t are such that $\mathcal{D}$ is well defined: for instance, below we will take $A = \mathbb{Z}_s$ where s is some integer sufficiently large compared to t.

If in the above definition $\boldsymbol{e}_i \ge 0$ for all i, the code is said to correct t *asymmetric* errors. However below we need to consider the general case, focusing on a particular way of constructing codes which we proceed to describe.

Definition 4.1: Let $m \geq L$ and let $h_1, \ldots, h_L, 0 < h_i < m, i = 1, \ldots, L$ be a set of integers. Define the code as follows:

$$\mathcal{C} = \Big\{ \boldsymbol{x} \in A^L \Big| \sum_{i=1}^{L} h_i x_i \equiv 0 \mod m \Big\}. \tag{10}$$

This code construction was first proposed by Varshamov and Tenenholtz [12] for correction of one asymmetric error (it was rediscovered later by Constantin and Rao, 1979 and, in a slightly different context, by Golomb and Welch, 1970). Generalizations to more that one error as well as to arbitrary finite groups were studied by Varshamov, 1973, Delsarte and Piret, 1981, and others; however, these works dealt with asymmetric errors. Below we extend this construction to the symmetric case.

Proposition 4.2: The code $\mathcal{C}$ defined in (10) corrects t additive errors if and only if for all $\boldsymbol{e} \in \mathbb{Z}^L, \|\boldsymbol{e}\| \leq t$ the sums $\sum_{i=1}^{L} e_i h_i$ are all distinct and nonzero modulo m.
This proposition is obvious as it amounts to saying that all the syndromes of error vectors of weight up to t are different and nonzero.

We will need the following theorem [2].

Theorem 4.3: (Bose-Chowla) Let q be a power of a prime and $m = (q^{t+1} - 1)/(q - 1)$. There exist $q + 1$ integers $j_0 = 0, j_1, \ldots, j_q$ in $\mathbb{Z}_m$ such that the sums

$$j_{i_1} + j_{i_2} + \ldots + j_{i_t} \quad (0 \leq i_1 \leq i_2 \leq \ldots \leq i_t \leq q)$$

are all different modulo m.

This theorem provides a way of constructing an asymmetric t-error-correcting code of length q. This is because for any error vector $\boldsymbol{e}$ with $||\boldsymbol{e}|| \leq t < m$ such that $e_i \geq 0$, the sums $\sum_{i=1}^{q} e_i j_i$ involve at most t of the numbers j_i and thus are all different.

Theorem 4.4: For $1 \leq i \leq q + 1$ let

$$h_i = \begin{cases} j_{i-1} + \frac{t-1}{2} m & \text{for } t \text{ odd} \\ j_{i-1} + \frac{t}{2} m & \text{for } t \text{ even} \end{cases}$$

where the numbers j_i are given by the Bose-Chowla theorem. Let $m_t = t(t + 1)m$ if t is odd and $m_t = t(t + 2)m$ if t is even. For all $\boldsymbol{e} \in \mathbb{Z}^{q+1}$ such that $||\boldsymbol{e}|| \leq t$ the sums $\sum_{i=1}^{q+1} e_i h_i$ are all distinct and nonzero modulo m_t.
Proof : Let t be odd and let $H = \{0, h_1, \ldots, h_{q+1}\}$. We have

$$(t - 1)m/2 \leq h_i < (t + 1)m/2.$$

(i) For any $k_1 \leq k_2 \leq \ldots \leq k_t \in H$, the sums $\sum_{i=1}^{t} k_i$ are all distinct modulo m and therefore also modulo m_t. These sums are also nonzero modulo m except for the case when all the k_i's are 0.

(ii) Moreover, for any $k_1 \leq k_2 \ldots \leq k_{2t} \in H$, the sum

$$\sum_{i=1}^{2t} k_i < m_t,$$

and is therefore nonzero modulo m_t.

(iii) Finally, for any $0 < k_1 \leq k_2 \leq \ldots \leq k_{2t} \in H$ and any $r < t$,

$$\sum_{i=2t-r+1}^{2t} k_i < r\frac{t+1}{2}m \leq (2t - r)\frac{t-1}{2}m \leq \sum_{i=1}^{2t-r} k_i.$$

Let us now suppose now that there exist $\boldsymbol{e}_1, \boldsymbol{e}_2 \in \mathbb{Z}^{q+1}$ both of weight at most t such that

$$\text{either } \sum_{i=1}^{q+1} e_{1i} h_i = 0 \text{ or } \sum_{i=1}^{q+1} e_{1i} h_i = \sum_{i=1}^{q+1} e_{2i} h_i.$$

However assuming this contradicts properties (i)-(iii) above.

The claim for t even is proved in an analogous way. ∎

Together with Proposition 4.2 this theorem implies the existence of a t-error-correcting code $\mathcal{C}$ of length $n - 1$ over the alphabet $\mathbb{Z}_n$ that corrects t additive errors. Recall that our goal is to construct a t-error-correcting code over the set of inversion vectors G_n which is a subset of $\mathbb{Z}_n^{n-1}$. Since $\mathcal{C}$ is a group code with respect to addition modulo m_t, its cosets in $\mathbb{Z}_n^{n-1}$ partition of this space into disjoint equal parts. At least one such coset contains $M \geq n!/m_t$ vectors from G_n. Invoking (3) we now establish the main result of this section.

Theorem 4.5: Let $m = ((n - 2)^{t+1} - 1)/(n - 3)$, where $n - 2$ is a power of a prime. There exists a t-error-correcting rank permutation code in $\mathfrak{S}_n$ whose size satisfies

$$M \geq \begin{cases} n!/(t(t + 1)m) & (t \text{ odd}) \\ n!/(t(t + 2)m) & (t \text{ even}). \end{cases}$$

ACKNOWLEDGMENT. The authors are grateful to Gregory Kabatiansky for a useful discussion of this work.

REFERENCES

[1] I. F. Blake, G. Cohen, and M. Deza, "Coding with permutations," *Inform. and Control*, vol. 43, no. 1, pp. 1–19, 1979.

[2] R. C. Bose and S. Chowla, "Theorems in the additive theory of numbers," *Commentarii Mathematici Helvetici*, vol. 37, no. 1, pp. 141-147, December 1962.

[3] H. Chadwick and L. Kurz, "Rank permutation group codes based on Kendall's correlation statistic," *IEEE Trans. Inform. Theory*, vol. 15, no. 2, pp. 306-315, 1969.

[4] H. Chadwick and I. Reed, "The equivalence of rank permutation codes to a new class of binary codes,"*IEEE Trans. Inform. Theory*, vol. 16, no. 5, pp. 640–641, 1970.

[5] C. J. Colbourn, T. Kløve, and A. C. H. Ling, "Permutation arrays for power line communications and mutually orthogonal Latin squares," *IEEE Trans. Inform. Theory*, vol. 50, no. 6, pp. 1289–1291, 2004.

[6] P. Diaconis and R. L. Graham, "Spearman's footrule as a measure of disarray," *Journal of the Royal Statistical Society, Series B*, vol. 39, no. 2, pp. 262-268, 1977.

[7] A. Jiang, M. Schwartz, and J. Bruck, "Error-correcting codes for rank modulation," *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Canada, July 2008, pp. 1736–1740.

[8] A. Jiang, R. Matescu, M. Schwartz, and J. Bruck, "Rank modulation for flash memories," *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Canada, July 2008, pp. 1731–1735.

[9] D. E. Knuth, *The Art of Computer Programming, Volume 3: Sorting and Searching*, Reading. MA: Addison-Wesley, 1973.

[10] G. Louchard and H. Prodinger, "The number of inversions in permutations: A saddle point approach," *Journal of Integer Sequences*, vol. 6, 2003, Article 03.2.8 (electronic).

[11] B.H. Margolius, "Permutations with inversions," *Journal of Integer Sequences*, vol. 4, no. 2, 2001, Article 01.2.4, 13 pp. (electronic).

[12] R. R. Varshamov and G. M. Tenenholtz, "A code for correcting a single asymmetric error," *Automat. Telemekh.*, vol. 26, no. 2, pp. 288–292, 1965.