Gray Codes and Enumerative Coding for Vector Spaces

Moshe Schwartz, *Senior Member, IEEE*

***Abstract*—Gray codes for vector spaces are considered in two graphs: the Grassmann graph, and the projective-space graph, both of which have recently found applications in network coding. For the Grassmann graph, constructions of cyclic optimal codes are given for all parameters. As for the projective-space graph, two constructions for specific parameters are provided, as well some nonexistence results. Furthermore, encoding and decoding algorithms are given for the Grassmannian Gray code, which induce an enumerative-coding scheme. The computational complexity of the algorithms is at least as low as known schemes, and for certain parameter ranges, the new scheme outperforms previously known ones.**

***Index Terms*—Enumerative coding, Grassmannian, Gray codes, projective-space graph.**

I. INTRODUCTION

GRAY codes, named after their inventor, Frank Gray [16], were originally defined as a listing of all the binary words, each appearing exactly once, such that adjacent words in the list differ by the value of a single bit. Since then, numerous generalizations were made, where today, a Gray code usually means a listing of the elements of some space, such that each element appears no more than once, and adjacent elements are "similar." What constitutes similarity usually depends on the application of the code.

The use of Gray codes has reached a wide variety of areas, such as storage and retrieval applications [2], processor allocation [3], statistics [5], hashing [10], puzzles [15], ordering documents [20], signal encoding [21], data compression [23], circuit testing [24], measurement devices [26], and recently also modulation schemes for flash memories [6], [17], [35]. For a survey on Gray codes the reader is referred to [25].

In the past few years, interest has grown in q-analogs of combinatorial structures, in which vectors and subsets are replaced by vector spaces over a finite field. Two prominent examples are the Grassmann graph $\mathcal{G}_q(n,k)$, and the projective-space graph $\mathcal{P}_q(n)$. The former contains all the k-dimensional subspaces of an n-dimensional vector space over $\mathrm{GF}(q)$, and is the q-analog of the Johnson graph, whereas the latter contains all the subspaces of an n-dimensional vector space, and acts as the q-analog of the Hamming graph.

Manuscript received June 09, 2013; accepted October 08, 2013. Date of publication October 21, 2013; date of current version December 20, 2013. This work was supported in part by the ISF under Grant 134/10.

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

Communicated by O. Milenkovic, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2013.2286616

Examples of such q-analogs structures are codes and anticodes in the Grassmann graph [11], [27], Steiner systems [1], reconstruction problems [34], and the middle-levels problem [7]. But what has begun as a purely theoretical area of research has recently found an important application to network coding, starting with the work of Koetter and Kschischang [19], and continuing with [8], [9], [13], [14], [29]–[31], [33].

In this paper, we study q-analogs of Gray codes, which are Hamiltonian circuits in the projective-space graph, and q-analogs for constant-weight Gray codes, which are Hamiltonian circuits in the Grassmann graph. For the former, we present nonexistence results (both for cyclic and noncyclic codes), as well as constructions for specific parameters based on the middle-levels problem discussed in [7]. For the latter, we provide constructions for cyclic optimal Gray codes for all parameters, as well as encoding and decoding functions. The construction has many degrees of freedom, resulting in a large number of Gray codes, which we bound from below.

As a side effect of the Gray-code construction and the encoding and decoding algorithms we provide, we obtain an enumerative-coding scheme for the Grassmannian space. A general enumerative-coding algorithm due to Cover [4] was recently used as the basis for an enumerative-coding scheme specifically designed for the Grassmannian space $\mathcal{G}_q(n,k)$ by Silberstein and Etzion [28], who provided encoding and decoding algorithms with complexity $O(M[nk]n)$, where $M[m]$ denotes the number of operations required for multiplying two numbers with m digits each. Another work by Medvedeva [22] suggested only a decoding algorithm with complexity $O(M[n^2]\log n)$. We provide encoding and decoding algorithm that not only arrange the subspaces in a Gray code, but also operate in $O(M[nk]n)$ time, the same complexity as the algorithms of [28]. We provide another decoding algorithm of complexity $O(M[nk]k\log k)$, which outperforms the decoding algorithm of [28] when $k\log k = o(n)$ (for example, when $k = O(n^{1-\epsilon})$ for some $0 < \epsilon < 1$), and outperforms the decoding algorithm of [22] when $k = o(\sqrt{n})$.

The paper is organized as follows. In Section II, we provide the basic definitions and notation used throughout the paper. In Section III, we construct Grassmannian Gray codes, as well as provide encoding and decoding functions. We continue in Section IV by studying subspace Gray codes. We conclude in Section V with a summary and open problems.

II. PRELIMINARIES

Throughout the paper, we shall maintain a notation consisting of uppercase letters for vector spaces, sometimes with a superscript indicating the dimension. We shall denote vectors by lower-case letters, and scalars by Greek letters. For a vector space W over some finite field $\mathrm{GF}(q)$, we let $\dim(W)$ denote the dimension of W. For two subspaces, W_1 and W_2, W_1+W_2 will denote their sum. If that sum happens to be a direct sum, we will stress that fact by denoting it as $W_1 \oplus W_2$. For a vector $v \in \mathrm{GF}(q)^n$, we shall denote the space spanned by v as $\langle v \rangle$.

Let W^n be some fixed n-dimensional vector space over $\mathrm{GF}(q)$. For an integer $0 \leqslant k \leqslant n$, we denote by $\begin{bmatrix} W^n \\ k \end{bmatrix}$ the set of all k-dimensional subspaces of W^n.

Definition 1: The Grassmann graph $\mathcal{G}_q(n,k)=(V,E)$ is defined by the vertex set $V=\begin{bmatrix} W^n \\ k \end{bmatrix}$, and two vertices $W_1, W_2 \in V$ are connected by an edge iff $\dim(W_1 \cap W_2)=k-1$.

It is easy to verify that the graph metric for $\mathcal{G}_q(n,k)$ has the distance function

$$d_G(W_1,W_2)=k-\dim(W_1\cap W_2). \tag{1}$$

This is the q-analog of the Johnson metric over constant-weight binary vectors. If $v_1, v_2 \in \{0,1\}^n$ are two binary vectors of length n, each with weight k, i.e., $\mathrm{wt}(v_1)=\mathrm{wt}(v_2)=k$, then the Johnson distance is defined by

$$d_J(v_1,v_2)=k-\mathrm{wt}(v_1\wedge v_2),$$

where $\wedge$ is a bit-wise AND.

More generally, (1) is a special case of the injection distance (see [29])

$$\begin{aligned} d_I(W_1,W_2)=\max\{&\dim(W_1),\dim(W_2)\} \\ &-\dim(W_1\cap W_2). \end{aligned}$$

This is the q-analog of the asymmetric Hamming distance defined for $v_1, v_2 \in \{0,1\}^n$ as

$$d_A(v_1,v_2)=\max\{\mathrm{wt}(v_1),\mathrm{wt}(v_2)\}-\mathrm{wt}(v_1\wedge v_2).$$

The q-number of k is defined as

$$[k]_q=1+q+q^2+\cdots+q^{k-1}=\frac{q^k-1}{q-1}.$$

By abuse of notation, we denote

$$[k]_q!=[k]_q[k-1]_q\ldots[1]_q.$$

The *Gaussian coefficient* is defined for n, k, and q as

$$\begin{aligned}\begin{bmatrix} n \\ k \end{bmatrix}_q &= \frac{[n]_q!}{[k]_q![n-k]_q!} \\ &= \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\ldots(q-1)}.\end{aligned}$$

It is well known that the number of k-dimensional subspaces of an n-dimensional space over $\mathrm{GF}(q)$ is given by $\begin{bmatrix} n \\ k \end{bmatrix}_q$. Furthermore, the Gaussian coefficients satisfy the following recursion:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q=\begin{bmatrix} n-1 \\ k \end{bmatrix}_q+q^{n-k}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q,$$

as well as the symmetry

$$\begin{bmatrix} n \\ k \end{bmatrix}_q=\begin{bmatrix} n \\ n-k \end{bmatrix}_q,$$

for all integers $0 \leqslant k \leqslant n$ (for example, see [32]).

Another graph of interest is the following.

Definition 2: The *projective-space graph* $\mathcal{P}_q(n)=(V,E)$ is defined by the vertex set $V=\bigcup_{k=0}^n \begin{bmatrix} W^n \\ k \end{bmatrix}$, and two vertices $W_1, W_2 \in V$ are connected by an edge iff

$$\dim(W_1+W_2)-\dim(W_1\cap W_2)=1.$$

One can easily see that the graph metric of $\mathcal{P}_q(n)$ has the distance function

$$d_S(W_1,W_2)=\dim(W_1+W_2)-\dim(W_1\cap W_2),$$

for any two subspaces $W_1, W_2 \in \mathcal{P}_q(n)$. We would like to note that this distance measure as an exact q-analog of the Hamming distance measure over binary vectors. Indeed, if $v_1, v_2 \in \{0,1\}^n$ are two binary vectors of length n, then the Hamming distance between the two is

$$d_H(v_1,v_2)=\mathrm{wt}(x\vee y)-\mathrm{wt}(x\wedge y),$$

where $\vee$ is a bitwise OR.

Equivalently, two vertices, W_1 and W_2 are connected in $\mathcal{P}_q(n)$ iff $|\dim(W_1)-\dim(W_2)|=1$, and either $W_1 \subset W_2$ or $W_2 \subset W_1$.

We now provide the definitions for the Gray codes that we study in this paper.

Definition 3: Let W^n be an n-dimensional vector space over $\mathrm{GF}(q)$. An $(n,k;q)$-Grassmannian Gray code $\mathcal{C}$ is a sequence of distinct subspaces

$$\mathcal{C}=C_0,C_1,\ldots,C_{P-1},$$

where $C_i \in \begin{bmatrix} W^n \\ k \end{bmatrix}$, and where C_i and C_{i+1} are neighbors in $\mathcal{G}_q(n,k)$, for all $0 \leqslant i \leqslant P-2$. We say P is the size of the code $\mathcal{C}$. If C_0 and C_{P-1} are neighbors in $\mathcal{G}_q(n,k)$ then $\mathcal{C}$ is said to be *cyclic* and P is its *period*. If $P=\begin{bmatrix} n \\ k \end{bmatrix}_q$, then $\mathcal{C}$ is called *optimal*.

A similar definition holds for the graph $\mathcal{P}_q(n)$.

Definition 4: Let W^n be an n-dimensional vector space over $\mathrm{GF}(q)$. An $(n;q)$-subspace Gray code $\mathcal{C}$ is a sequence of distinct subspaces

$$\mathcal{C}=C_0,C_1,\ldots,C_{P-1},$$

where $C_i \in \bigcup_{k=0}^n \begin{bmatrix} W^n \\ k \end{bmatrix}$, and where C_i and C_{i+1} are neighbors in $\mathcal{P}_q(n)$ for all $0 \leqslant i \leqslant P-2$. We say P is the size of the code $\mathcal{C}$. If C_0 and C_{P-1} are neighbors in $\mathcal{P}_q(n)$ then $\mathcal{C}$ is said to be *cyclic* and P is its *period*. If $P=\sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_q$, then $\mathcal{C}$ is called *optimal*.

III. Grassmannian Gray Codes

In this section, we will study Grassmannian Gray codes. We will first describe a construction, and later introduce and analyze encoding and decoding algorithms. These algorithms may be used as an enumerative-coding scheme.

A. Construction

The construction we describe is recursive in nature. We will be constructing an $(n,k;q)$-Grassmannian Gray code by combining together an $(n-1,k;q)$-code with an

$(n-1,k-1;q)$-code. We start by introducing two useful lemmas.

Lemma 5: Let W^n be an n-dimensional vector space over $\mathrm{GF}(q)$. Let W^{n-1} and W^{k-1} be $(n-1)$-dimensional and $(k-1)$-dimensional subspaces of W^n, respectively, where

$$W^{k-1} \subseteq W^{n-1} \subset W^n.$$

Then, there are q^{n-k} vectors $v_0,\dots,v_{q^{n-k}-1} \in \mathrm{GF}(q)^n$ such that

1) $\left(W^{k-1} \oplus \langle v_i \rangle\right) \cap W^{n-1} = W^{k-1}$.
2) The subspaces $W^{k-1} \oplus \langle v_i \rangle$ are distinct.

Proof: To maintain the first requirement, it is obvious that $v_i \in W^n \setminus W^{n-1}$. We have

$$\left|W^n \setminus W^{n-1}\right| = q^n - q^{n-1}$$

vectors to choose from. However, having chosen a vector $v \in W^n \setminus W^{n-1}$, to maintain the second requirement we cannot choose vectors of the form $\alpha v + w$, where $w \in W^{k-1}$ and $\alpha \in \mathrm{GF}(q) \setminus \{0\}$. Since there are $(q-1)q^{k-1}$ distinct choices of α and w, resulting in distinct forbidden vectors, the maximal number of vectors we can choose which maintain the two requirements is given by

$$\frac{q^n - q^{n-1}}{(q-1)q^{k-1}} = q^{n-k}.$$

■

A closer look at the proof of Lemma 5 reveals that W^{k-1} induces an equivalence relation on the vectors of $W^n \setminus W^{n-1}$, where $v, v' \in W^n \setminus W^{n-1}$ are equivalent if there exist $\alpha \in \mathrm{GF}(q) \setminus \{0\}$ and $w \in W^{k-1}$ such that $v' = \alpha v + w$. A set of vectors whose existence is guaranteed by Lemma 5 is merely a list of representatives from each of the equivalence classes induced by W^{k-1}. For such a vector v and a subspace W^{k-1}, we shall denote the equivalence class of v induced by W^{k-1} as $[v]_{W^{k-1}}$.

Lemma 6: Let W^{n-1} and W^n be as in Lemma 5. Assume W_1^{k-1} and W_2^{k-1} are two distinct $(k-1)$-dimensional subspaces of W^{n-1}. Then, for any $v \in W^n \setminus W^{n-1}$ we have

$$[v]_{W_1^{k-1}} \neq [v]_{W_2^{k-1}}.$$

Proof: We observe that

$$\left\langle [v]_{W_1^{k-1}} \right\rangle = \langle v \rangle \oplus W_1^{k-1} \quad \text{and} \left\langle [v]_{W_2^{k-1}} \right\rangle = \langle v \rangle \oplus W_2^{k-1}.$$

Let us assume to the contrary that

$$[v]_{W_1^{k-1}} = [v]_{W_2^{k-1}}.$$

We therefore have

$$\begin{aligned} W_1^{k-1} &= W^{n-1} \cap \left(\langle v \rangle \oplus W_1^{k-1}\right) \\ &= W^{n-1} \cap \left\langle [v]_{W_1^{k-1}} \right\rangle \\ &= W^{n-1} \cap \left\langle [v]_{W_2^{k-1}} \right\rangle \\ &= W^{n-1} \cap \left(\langle v \rangle \oplus W_2^{k-1}\right) \\ &= W_2^{k-1}, \end{aligned}$$

which is a contradiction. ■

Intuitively speaking, Lemma 6 states that the equivalence classes that partition $W^n \setminus W^{n-1}$ and are induced by distinct $(k-1)$-dimensional subspaces of W^{n-1}, do not contain two identical classes. This fact will be used later in the construction.

We shall now build an $(n,k;q)$-Grassmannian Gray code by combining an $(n-1,k;q)$-code with an $(n-1,k-1;q)$-code.

Construction A: Let W^n be an n-dimensional vector space over $\mathrm{GF}(q)$. We can write W^n as the direct sum $W^n = W^{n-1} \oplus W^1$, where $\dim(W^{n-1}) = n-1$ and $\dim(W^1) = 1$.

Let us assume the existence of two cyclic optimal Grassmannian Gray codes: an $(n-1,k;q)$-code $\mathcal{C}'$, and an $(n-1,k-1;q)$-code $\mathcal{C}''$. In both cases, we assume the ambient vector space is W^{n-1}. For convenience, let us denote the code sequences as

$$\begin{aligned} \mathcal{C}' &= C'_0, C'_1, \dots, C'_{P'-1}, \\ \mathcal{C}'' &= C''_0, C''_1, \dots, C''_{P''-1}. \end{aligned}$$

From these two codes, we shall construct a new $(n,k;q)$-Grassmannian Gray code.

We start with C''_0, and choose equivalence-class representatives $v''_{0,0},\dots,v''_{0,q^{n-k}-1}$ by Lemma 5. Continuing to C''_1, again we choose equivalence-class representatives, $v''_{1,0},\dots,v''_{1,q^{n-k}-1}$, where we make sure

$$[v''_{0,q^{n-k}-1}]_{C''_0} \cap [v''_{1,0}]_{C''_1} \neq \emptyset,$$

i.e., that the last equivalence class chosen for C''_0, and the first equivalence class chosen for C''_1, have a nonempty intersection.

We continue in the same manner, where for C''_i we choose equivalence-class representatives $v''_{i,0},\dots,v''_{i,q^{n-k}-1}$, where also

$$[v''_{i-1,q^{n-k}-1}]_{C''_{i-1}} \cap [v''_{i,0}]_{C''_i} \neq \emptyset.$$

Finally, for $C''_{P''-1}$, the last subspace in C', we need both a nonempty intersection of

$$[v''_{P''-2,q^{n-k}-1}]_{C''_{P''-2}} \cap [v''_{P''-1,0}]_{C''_{P''-1}} \neq \emptyset,$$

as well as a nonempty intersection of

$$[v''_{P''-1,q^{n-k}-1}]_{C''_{P''-1}} \cap [v''_{0,0}]_{C''_0} \neq \emptyset,$$

i.e., with the first equivalence class induced by the first subspace C_0. Since, by Lemma 6, $[v''_{0,0}]_{C''_0}$ has a nonempty intersection with at least two equivalence classes induced by $C''_{P''-1}$, we can always find a suitable set of representatives.

We now construct the auxiliary sequence $\mathcal{C}^*$ as follows:

$$\begin{aligned} \mathcal{C}^* = {} & C''_0 \oplus \left\langle v''_{0,0} \right\rangle, C''_0 \oplus \left\langle v''_{0,1} \right\rangle, \dots, C''_0 \oplus \left\langle v''_{0,q^{n-k}-1} \right\rangle, \\ & C''_1 \oplus \left\langle v''_{1,0} \right\rangle, C''_1 \oplus \left\langle v''_{1,1} \right\rangle, \dots, C''_1 \oplus \left\langle v''_{1,q^{n-k}-1} \right\rangle, \\ & \vdots \\ & C''_{P''-1} \oplus \left\langle v''_{P''-1,0} \right\rangle, \dots, C''_{P''-1} \oplus \left\langle v''_{P''-1,q^{n-k}-1} \right\rangle. \end{aligned}$$

In a more concise form,

$$C^* = C^*_0, C^*_1, \dots, C^*_{P''q^{n-k}-1}$$

is a sequence of length $P''q^{n-k}$ in which the ith element is the subspace

$$\mathcal{C}_i^* = C''_{\lfloor i/q^{n-k}\rfloor} \oplus \left\langle v''_{\lfloor i/q^{n-k}\rfloor, i \bmod q^{n-k}} \right\rangle.$$

We now turn to use the code $\mathcal{C}'$. Let us choose an arbitrary index $0 \leqslant j \leqslant P'-1$, and denote $U = C'_j \cap C'_{j+1}$, where the indices are taken modulo P'. We observe that $U \subseteq W^{n-1}$ is a $(k-1)$-dimensional subspace.

Since $\mathcal{C}'$ contains all the $(k-1)$-dimensional subspaces of W^{n-1}, let i be the index such that $C''_i = U$. Finally, we also choose an arbitrary index $0 \leqslant \ell \leqslant q^{n-k}-2$.

We now construct the code $\mathcal{C}$ by inserting a shifted version of $\mathcal{C}'$ into the auxiliary $\mathcal{C}^*$ as follows:

$$\begin{aligned}\mathcal{C} = C_0^*, C_1^*, \ldots, C^*_{iq^{n-k}+\ell}\\ C'_{j+1}, C'_{j+2}, \ldots, C'_{P'-1}, C'_0, C'_1, \ldots, C'_j\\ C^*_{iq^{n-k}+\ell+1}, \ldots, C^*_{P''q^{n-k}-1}.\end{aligned} \tag{2}$$

□

Theorem 7: The sequence $\mathcal{C}$ of subspaces from Construction A is a cyclic optimal $(n,k;q)$-Grassmannian Gray code.

Proof: We start by showing that the subspaces in the code are all distinct. We first note that the subspaces in $\mathcal{C}^*$ are distinct from those in $\mathcal{C}'$, since all the former intersect W^{n-1} in a $(k-1)$-dimensional subspace, while all the latter intersect W^{n-1} in a k-dimensional subspace. To continue, the subspaces of $\mathcal{C}'$ are distinct by virtue of $\mathcal{C}'$ being a Grassmannian Gray code. Finally, we show that the subspaces of $\mathcal{C}^*$ are distinct. Assume

$$C''_{i_1} \oplus \left\langle v''_{i_1,j_1}\right\rangle = C''_{i_2} \oplus \left\langle v''_{i_2,j_2}\right\rangle.$$

Then,

$$\begin{aligned}C''_{i_1} &= \left(C''_{i_1} \oplus \left\langle v''_{i_1,j_1}\right\rangle\right) \cap W^{n-1}\\ &= \left(C''_{i_2} \oplus \left\langle v''_{i_2,j_2}\right\rangle\right) \cap W^{n-1} = C''_{i_2}.\end{aligned}$$

Since $\mathcal{C}''$ is a Grassmannian Gray code, we must have $i_1 = i_2$. We thus have

$$C''_{i_1} \oplus \left\langle v''_{i_1,j_1}\right\rangle = C''_{i_1} \oplus \left\langle v''_{i_1,j_2}\right\rangle.$$

Since the vectors $v''_{i_1,0}, \ldots, v''_{i_1,q^{n-k}-1}$ were chosen from distinct equivalence classes, we again must have $j_1 = j_2$. Hence, all the subspaces of $\mathcal{C}$ are distinct.

Next, we show that any two subspaces which are adjacent in the list, intersect in a $(k-1)$-dimensional subspace. This is certainly true for adjacent subspaces in $\mathcal{C}'$ since they form an $(n-1,k;q)$-Grassmannian Gray code. For $\mathcal{C}^*$, we have

$$\left(C''_i \oplus \left\langle v''_{i,j}\right\rangle\right) \cap \left(C''_i \oplus \left\langle v''_{i,j+1}\right\rangle\right) = C''_i$$

and so the intersection is $(k-1)$-dimensional. Furthermore, C''_i and C''_{i+1} intersect in a $(k-2)$-dimensional subspace, since they come from a $(n-1,k-1;q)$-Grassmannian Gray code. Since, by construction,

$$[v''_{i,q^{n-k}-1}]_{C''_i} \cap [v''_{i+1,0}]_{C''_{i+1}} \neq \emptyset,$$

we have

$$\dim\left(\left(C''_i \oplus \left\langle v''_{i,q^{n-k}-1}\right\rangle\right) \cap \left(C''_{i+1} \oplus \left\langle v''_{i+1,0}\right\rangle\right)\right) = k-1.$$

Let i, j, and ℓ, be as in (2). We can also easily verify that at the insertion points of $\mathcal{C}'$ into $\mathcal{C}^*$, we have

$$\begin{aligned}\dim\left(C^*_{iq^{n-k}+\ell} \cap C'_{j+1}\right) = k-1,\\ \dim\left(C^*_{iq^{n-k}+\ell+1} \cap C'_{j}\right) = k-1,\end{aligned}$$

and thus, all adjacent subspaces in the sequence are also adjacent in the graph $\mathcal{G}_q(n,k)$. This also proves the code is cyclic.

Finally, to show that the code is optimal we need to show that it contains all the k-dimensional subspaces of W^n. Since $\mathcal{C}'$ and $\mathcal{C}''$ are optimal, we have

$$\begin{aligned}|\mathcal{C}| &= |\mathcal{C}'| + q^{n-k}|\mathcal{C}''|\\ &= \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q = |W^n|.\end{aligned}$$

■

Theorem 8: For every $n \geqslant 1$ and $0 \leqslant k \leqslant n$ there exists a cyclic optimal $(n,k;q)$-Grassmannian Gray code.

Proof: Because of the recursive nature of Construction A, the only thing we need to prove is that the basis for the recursion exists. This is trivially true since $(n,n;q)$-Grassmannian Gray codes and $(n,0;q)$-Grassmannian Gray codes which are cyclic and optimal are the unique sequence of length 1 containing the full vector space, and the trivial space of dimension 0, respectively. ■

We can get a lower bound on the number of distinct $(n,k;q)$-Grassmannian Gray codes that result from this construction, thus getting a lower bound on the number of such codes in general. The counting requires the following lemma.

Lemma 9: Let W^{n-1} and W^{n-1} be as in Lemma 5, and let $C_1, C_2 \subset W^{n-1}$ be two $(k-1)$-dimensional subspaces such that $\dim(C_1 \cap C_2) = k-2$. Then, for any $v_1 \in W^n \setminus W^{n-1}$, there exist exactly q distinct subspaces of the form $C_2 \oplus \langle v_2 \rangle$, for some $v_2 \in W^n \setminus W^{n-1}$, such that

$$\dim\left(\left(C_1 \oplus \langle v_1\rangle\right) \cap \left(C_2 \oplus \langle v_2\rangle\right)\right) = k-1.$$

Proof: Let $w_1, w_2, \ldots, w_{k-2}$ be a basis for $C_1 \cap C_2$. Let us further denote

$$\begin{aligned}C_1 = \langle w_1, \ldots, w_{k-2}, u_1\rangle,\\ C_2 = \langle w_1, \ldots, w_{k-2}, u_2\rangle.\end{aligned}$$

Given $v_1 \in W^n \setminus W^{n-1}$, in order to obtain a subspace $W_2 \oplus \langle v_2\rangle$ with the desired intersection dimension we must choose $v_2 \in W^n \setminus W^{n-1}$ such that the equation

$$\sum_{i=1}^{k-2} \alpha_i w_i + \alpha u_1 + \beta v_1 = \sum_{i=1}^{k-2} \gamma_i w_i + \gamma u_2 + \delta v_2,$$

holds for some choice of scalar coefficients $\alpha_i, \gamma_i, \alpha, \beta, \gamma, \delta \in \mathrm{GF}(q)$, with $\beta \neq 0$. We thus choose

$$v_2 = \frac{1}{\delta}\sum_{i=1}^{k-2}(\alpha_i - \gamma_i)w_i + \alpha u_1 - \gamma u_2 + \beta v_1.$$

Since multiplying v_2 by a scalar does not change the subspace $C_2 \oplus \langle v_2 \rangle$, we may conveniently choose $\delta = \beta^{-1}$. Hence,

$$v_2 = \sum_{i=1}^{k-2}\frac{\alpha_i - \gamma_i}{\beta}w_i + \frac{\alpha}{\beta}u_1 - \frac{\gamma}{\beta}u_2 + v_1.$$

Finally, we note that adding a vector from C_2 to v does not change the subspace $C_2 \oplus \langle v_2 \rangle$. We may therefore eliminate any linear combination of $w_1, \dots, w_{k-2}, u_2$ from v. By denoting $\epsilon = \alpha/\beta$, we are left with choosing

$$v_2 = v_1 + \epsilon u_1,$$

and there are exactly q choices for $\epsilon \in \mathrm{GF}(q)$ which result in distinct subspaces as required. ■

We are now ready to state the lower bound on the number of distinct $(n, k; q)$-Grassmannian Gray codes resulting from Construction A. We note that codes which are cyclic shifts of one another are still counted as distinct codes.

Theorem 10: The number of distinct $(n, k; q)$-Grassmannian Gray codes resulting from Construction A is lower bounded by

$$\prod_{i=1}^{n-k}\prod_{j=1}^{k}\left((q-1)q^{i-1}\left((q^i-1)!q\right)^{\left[\begin{smallmatrix} i+j-1 \\ j-1 \end{smallmatrix}\right]_q}\right)^{\binom{n-i-j}{n-k-i}}.$$

Proof: Let us denote the number of $(n, k; q)$-Grassmannian Gray codes by $T(n, k; q)$. If either $k = n$ or $k = 0$, then $T(n, k; q) = 1$, which agrees with the claimed lower bound. Let us therefore consider the case of $0 < k < n$.

During the construction process, we first choose an $(n-1, k-1; q)$-code, which can be done in $T(n-1, k-1; q)$ ways. We then need to choose the vectors $v''_{i,j}$ to obtain the subspaces $C''_i \oplus \langle v''_{i,j} \rangle$. For $i = 0$, we can arrange the q^{n-k} subspaces in $(q^{n-k})!$ ways. For subsequent values of i, $1 \leqslant i \leqslant \left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix}\right]_q - 2$, we can choose the first subspace $C''_i \oplus \langle v''_{i,0} \rangle$ in one of q ways, according to Lemma 9. The rest of the subspaces may be chosen arbitrarily in any one of $(q^{n-k}-1)!$ ways. Finally, for $i = \left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix}\right]_q - 1$, both the first subspace and last subspace are chosen from a set of q subspaces. At the worst case, we can choose them both in one of $q(q-1)$ ways, and the rest of the subspaces in $(q^{n-k}-2)!$.

We then choose an $(n-1, k; q)$-code, which can be done in $T(n-1, k; q)$ ways. We rotate and insert it into the code constructed so far. However, since we already count cyclic shifts of codes as distinct, we shall assume we do not rotate it, to avoid overcounting. We, thus, only have to choose where to insert it, in one of $q^{n-k} - 1$ ways.

Combining all of the above, we reach the recursion

$$T(n, k; q) \geqslant T(n-1, k-1; q)T(n-1, k; q) \cdot \\ \cdot (q-1)q^{n-k-1}\left((q^{n-k}-1)!q\right)^{\left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix}\right]_q}.$$

Solving the recursion, with the base cases of $T(n, n; q) = 1$ and $T(n, 0; q) = 1$, gives the desired lower bound. ■

B. Algorithms

We now describe algorithms related to Grassmannian Gray codes. The algorithms we consider are as follows.

1) Encoding—Finding the ith element in the code.
2) Decoding—Finding the index in the list of a given element of the code.

We will specialize Construction A to allow for simpler algorithms.

We require some more notation. Throughout this section, we denote by e_i the ith standard unit vector, i.e., the vector all of whose entries are 0 except for the ith one being 1. The length of the vector will be implied by the context. The entries of a length n vector will be indexed by $0, 1, \dots, n-1$. The $n \times n$ identity matrix will be denoted by I_n, and the $n_1 \times n_2$ all-zero matrix by $0_{n_1 \times n_2}$.

A k-dimensional subspace W^k of an n-dimensional space can be represented by a $k \times n$ matrix whose rows form a basis for W^k. Many choices for such a matrix exist, and we shall be interested in a unique one. We will first describe the reduced row echelon form matrix, which is known to be unique, and then transform it to obtain our representation.

In a reduced row echelon form matrix, the leading coefficient of each row is 1, and it is the only nonzero element in its column. Furthermore, the leading coefficient of each row is strictly to the right of the leading coefficient of the previous row.

Assume M is a $k \times n$ matrix of rank k in reduced row echelon form, $k \leqslant n$. We denote the set of k indices of columns containing leading coefficients as $\Lambda(M) \subseteq \{0, 1, \dots, n-1\}$. We apply the following simple recursive transformation τ to M: If $k = 0$ then $\tau(M)$ is the degenerate empty matrix with 0 rows. Otherwise, assume $k \geqslant 1$. If the last column of M is all zeros, then $\tau(M) = [\tau(M^*)|0_{k\times 1}]$, where M^* is the $k\times(n-1)$ matrix obtained from M by deleting the last column. If the last column of M is not all zeros, let i be the index of the first row from the bottom which does not contain a zero in the last column. We multiply the ith row by a scalar such that its last entry is 1. We then subtract suitable scalar multiples of the ith row from other rows of M so that the resulting matrix M' has a single nonzero entry in the last column (a 1 located in the ith row). We then delete the ith row and the last column to get the $(k-1)\times(n-1)$ matrix M''. We recursively take $\tau(M'')$, append a column of 0s to its right, and reinsert the ith column which we previously removed. The result is defined as $\tau(M)$.

Example 11: Let M be the 3×5 reduced row echelon form matrix

$$M = \begin{pmatrix} 1 & 0 & 3 & 0 & 1 \\ 0 & 1 & 2 & 0 & 4 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix},$$

where the entries are from $\mathrm{GF}(5)$. We then have

$$\tau(M) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 4 & 1 & 0 \\ 0 & 0 & 0 & 3 & 1 \end{pmatrix}.$$

□

It is easily seen that $\tau(M)$ is in row echelon form, but not in *reduced* row echelon form, i.e., the leading coefficient of each row is nonzero (but not necessarily 1), the entries below a leading coefficient are 0 (but not necessarily 0 above it), and the leading coefficient of each row is strictly to the right of the leading coefficient of the previous row. We note that $\Lambda(M) = \Lambda(\tau(M))$.

Thus, for a k-dimensional subspace W^k, and the unique reduced row echelon form matrix M whose rows form a basis for W^k, we shall call $\tau(M)$ the *canonical* matrix representation of W^k. To avoid excessive notation, we shall refer to both the subspace and its canonical matrix as W^k. We say W^k is *simple* if

$$W^k = [I_k|0_{n-k}].$$

We now start with specializing Construction A. First, during the construction we require a choice of W^n and W^{n-1}. We choose both to be simple subspaces.

Next, in the construction we have $\mathcal{C}'' = C''_0, \dots, C''_{P''-1}$, and for each C''_i, a $(k-1)$-dimensional subspace of W^{n-1}, we find q^{n-k} vectors from $W^n \setminus W^{n-1}$, denoted $v''_{i,0}, \dots, v''_{i,q^{n-k}-1}$. We make this choice explicit: let C''_i be a $(k-1) \times (n-1)$ canonical matrix. Let $0 \leqslant r_{i,0} < r_{i,1} < \dots < r_{i,n-k-1} \leqslant n-2$ be the elements in $\{0, 1, \dots, n-2\} \setminus \Lambda(C''_i)$. We note that $e_{r_{i,\ell}}$ is not in the subspace C''_i, for all ℓ. For an integer $0 \leqslant j \leqslant q^{n-k}-1$, let $[j]_\ell$ denote its ℓth digit when written in base q, i.e.,

$$j = \sum_{\ell=0}^{n-k-1} [j]_\ell q^\ell,$$

where $[j]_\ell \in \{0, 1, \dots, q-1\}$. For convenience, we also denote the elements of $\mathrm{GF}(q)$ as $\alpha_0, \alpha_1, \dots, \alpha_{q-1}$, in some fixed order, where $\rho(\cdot)$ gives the reverse mapping, i.e., $\rho(\alpha_i) = i$. We now choose

$$v''_{i,j} = e_{n-1} + \sum_{\ell=0}^{n-k-1} \alpha_{[j]_\ell} e_{r_{i,\ell}}.$$

In Construction A, when inserting a shifted version of $\mathcal{C}'$, a parameter $0 \leqslant \ell \leqslant q^{n-k}-2$ is chosen. We shall call this parameter the *insertion offset*. In this instance, we will always choose $\ell = 0$.

Finally, we say a cyclic optimal $(n, k; q)$-Grassmannian Gray code, $\mathcal{C} = C_0, C_1, \dots, C_{P-1}$, is *simple*, if C_0 is simple, and $C_0 \cap C_{P-1}$ is simple.

Lemma 12: Let $\mathcal{C}'$ be a simple cyclic optimal $(n-1, k; q)$-Grassmannian Gray code, and $\mathcal{C}''$ be a simple cyclic optimal $(n-1, k-1; q)$-Grassmannian Gray code. Let $\mathcal{C} = C_0, C_1, \dots, C_{P-1}$ be the cyclic optimal $(n, k; q)$-Grassmannian Gray code created by Construction A, with an insertion offset $\ell = 0$. Then its shifted version,

$$\overline{\mathcal{C}} = C_1, C_2, \dots, C_{P-1}, C_0,$$

is a simple cyclic optimal $(n, k; q)$-Grassmannian Gray code.

Proof: The fact that $\overline{\mathcal{C}}$ is a cyclic optimal $(n, k; q)$-code is trivial. It remains to prove the code is simple. Let us denote

$$\mathcal{C}' = C'_0, C'_1, \dots, C'_{P'-1},$$
$$\mathcal{C}'' = C''_0, C''_1, \dots, C''_{P''-1}.$$

Since $\mathcal{C}'$ is simple, we have that C'_0 is simple, and that $C'_0 \cap C'_{P'-1}$ is simple. The latter intersection determines where $\mathcal{C}'$ is inserted in $\mathcal{C}^*$, i.e., between the q^{n-k} subspaces derived from the simple $(k-1)$-dimensional space. Since $\mathcal{C}''$ is also simple, it is inserted in the first set of q^{n-k} subspaces derived from C''_0. By using an insertion offset $\ell = 0$, we have that $C_1 = C'_0$, and that $C_1 \cap C_0 = C''_0$. Thus, $\overline{\mathcal{C}}$ is simple. ■

We are now in a position to state simple encoding and decoding functions. The encoding function

$$\mathcal{E}_{n,k;q} : \left\{0, 1, \dots, \begin{bmatrix} n \\ k \end{bmatrix}_q - 1\right\} \to \begin{bmatrix} W^n \\ k \end{bmatrix},$$

maps an index m to the mth subspace in the $(n, k; q)$-Grassmannian Gray code $\overline{\mathcal{C}}$ constructed above. Using the observations so far, we can easily state that

$$\mathcal{E}_{n,k;q}(m) = \begin{cases} [I_k|0_{k\times(n-k)}] & k = 0 \text{ or } k = n, \\ [\mathcal{E}_{n-1,k;q}(m)|0_{k\times 1}] & m \leqslant \left[\begin{smallmatrix} n-1 \\ k \end{smallmatrix}\right]_q - 1, \\ \begin{bmatrix} \mathcal{E}_{n-1,k-1;q}(i)|0_{(k-1)\times 1} \\ v''_{i,j} \end{bmatrix} & \text{otherwise,} \end{cases}$$

where

$$i = \left\lfloor \frac{1}{q^{n-k}} \left(m - \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + 1 \right) \right\rfloor \bmod \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$$
$$j = \left(m - \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + 1 \right) \bmod q^{n-k}$$
$$v''_{i,j} = e_{n-1} + \sum_{\ell=0}^{n-k-1} \alpha_{[j]_\ell} e_{r_{i,\ell}}.$$

We also note, that in the last case, where the vector $v''_{i,j}$ is appended as another row to the generating matrix, the vector is inserted between the correct rows such that the resulting matrix is canonical.

The decoding function,

$$\mathcal{D}_{n,k;q} : \begin{bmatrix} W^n \\ k \end{bmatrix} \to \left\{0, 1, \dots, \begin{bmatrix} n \\ k \end{bmatrix}_q - 1\right\},$$

is defined as the reverse of the encoding function, i.e.,

$$\mathcal{D}_{n,k;q}\left(\mathcal{E}_{n,k;q}(m)\right) = m,$$

for all $0 \leqslant m \leqslant \left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q - 1$.

To describe the decoding function we need some preparation work. Assume the input to the decoding function is a k-dimensional subspace W^k, which will also denote a canonical matrix whose row span is W^k.

Since W^{n-1} is simple, checking whether $W^k \subseteq W^{n-1}$ amounts to checking whether the last column of W^k contains only 0s. If this is not the case, then $\dim(W^k \cap W^{n-1}) = k-1$, and by construction there is a unique row with a nonzero entry in the last coordinate. We denote this row v'', and its last coordinate must be 1. Furthermore, we remove this row and the last column from W^k and denote the resulting canonical matrix by W^{k-1}. Finally, like before, let $0 \leqslant r_0 < r_1 < \dots < r_{n-k-1} \leqslant n-2$ be elements of $\{0, 1, \dots, n-2\} \setminus \Lambda(W^{k-1})$.

With this notation, we can now easily find that

$$\mathcal{D}_{n,k;q}(W^k) = \begin{cases} 0 & k=0 \text{ or } k=n, \\ \mathcal{D}_{n-1,k;q}(W^k) & W^k \subseteq W^{n-1}, \\ i & \text{otherwise}, \end{cases} \tag{3}$$

where

$$i = \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + \left(\left(q^{n-k} \cdot \mathcal{D}_{n-1,k-1;q}(W^{k-1}) - 1 + \sum_{\ell=0}^{n-k-1} \rho\left(e_{r_\ell} \cdot v''\right) q^\ell \right) \bmod q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q \right).$$

We also note that in the case of $W^k \subseteq W^{n-1}$, when applying $\mathcal{D}_{n-1,k;q}$ to W^k we remove the last column of W^k, which is an all-zero column.

C. Complexity Analysis

The goal of this section is to bound the number of operations required to perform the encoding and decoding procedures described in the previous section.

For our convenience, we assume throughout this section that integers are represented in base q. Thus, multiplying and dividing by q amount to simple shift operations on the list of digits.

Another simplification is enabled by the following lemma.

Lemma 13: Let $\mathcal{C} = C_0, C_1, \dots, C_{P-1}$ be an $(n,k;q)$-Grassmannian Gray code. Then the dual code,

$$\mathcal{C}^\perp = C_0^\perp, C_1^\perp, \dots, C_{P-1}^\perp,$$

is an $(n, n-k; q)$-Grassmannian Gray code. If $\mathcal{C}$ is cyclic, then so is $\mathcal{C}^\perp$. Also, if $\mathcal{C}$ is optimal, then so is $\mathcal{C}^\perp$.

Proof: Obviously $\dim(C_i^\perp) = n-k$ for all i. Since $(C_i^\perp)^\perp = C_i$, the elements of $\mathcal{C}^\perp$ are all distinct. To verify that adjacent elements in $\mathcal{C}^\perp$ are also adjacent in $\mathcal{G}_q(n, n-k)$ we use simple linear algebra. For all i,

$$C_i^\perp \cap C_{i+1}^\perp = \left(C_i + C_{i+1}\right)^\perp.$$

Since $\dim(C_i \cap C_{i+1}) = k-1$, we have

$$\begin{aligned} \dim(C_i + C_{i+1}) &= \dim(C_i) + \dim(C_{i+1}) \\ &\quad - \dim(C_i \cap C_{i+1}) \\ &= k+1. \end{aligned}$$

It then follows that

$$\dim(C_i^\perp \cap C_{i+1}^\perp) = n - \dim\left(C_i + C_{i+1}\right)^\perp = n-k-1,$$

hence, $C_i^\perp$ and $C_{i+1}^\perp$ are adjacent in $\mathcal{G}_q(n, n-k)$. If we take all indices modulo P, then $\mathcal{C}^\perp$ is cyclic if $\mathcal{C}$ is cyclic. Finally, $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$ implies that $\mathcal{C}^\perp$ is optimal if $\mathcal{C}$ is optimal. ∎

In light of Lemma 13, we will assume throughout that $2k \leqslant n$, and in particular, that $n-k = \Theta(n)$.

An important ingredient in the analysis is the complexity of multiplying two numbers, each with m digits. We denote this number as $M[m]$. Using the Schönhage-Strassen algorithm, we have $M[m] = O(m \log m \log\log m)$ (for example, see [18]). We can alternatively use the more recent algorithm due to Fürer [12], for which $M[m] = O(m \log m 2^{\log^* m})$. We also note that division of two numbers with m digits each also requires $O(M[m])$ operations [18].

We now turn to the analysis of the decoding algorithm. We observe that all the integers involved require at most nk digits to represent. As a first step, we compute $\begin{bmatrix} n \\ k \end{bmatrix}_q$. It was shown in [28] that the complexity of this is $O(M[nk]k)$.[1] As was also shown in [28], from this Gaussian coefficient we may derive $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$ and $\begin{bmatrix} n-1 \\ k \end{bmatrix}_q$ by

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q \cdot \frac{q^n - 1}{q^k - 1}, \tag{4}$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \cdot \frac{q^n - 1}{q^{n-k} - 1}, \tag{5}$$

with additional $O(M[nk])$ operations.

As we examine the algorithm as given in (3), even though it is presented as a recursive algorithm, it is a tail recursion, and so, may be considered as an iterative process. At the beginning of each iteration, we check the last column of the matrix to see if it is all 0s. This takes $O(k)$ time.

For the second case of (3), when $W^k \subseteq W^{n-1}$, we delete the last column, taking $O(k)$ time. For the third case of (3), we need to compute $\begin{bmatrix} n-1 \\ k \end{bmatrix}_q$ and $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$ from $\begin{bmatrix} n \\ k \end{bmatrix}_q$, taking $O(M[nk])$ operations. Multiplication by q amounts to a simple shift operation, and addition and subtraction of numbers with nk digits takes $O(nk)$ time. We note that finding the numbers r_ℓ for $0 \leqslant \ell \leqslant n-k-1$ is easily seen to take at most $O(n)$ time. Deleting a row and a column takes $O(n)$ time. Finally, we note that the sole purpose of the modulo operation is to transform a possible -1 outcome into $q^{n-k}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q - 1$ which may be done in $O(nk)$ time (since we have already computed $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$). The total number of operations for the last case of the decoding procedure is therefore bounded by $O(M[nk])$. Since the total number of rounds is at most n, the entire algorithm may be run in time $O(M[nk]n)$. The same analysis holds for the encoding algorithm.

Theorem 14: The computation complexity of the encoding and decoding algorithms is $O(M[nk]n)$.

The complexity of the algorithms from [28] is the same as those presented in this paper. However, the algorithms here also provide a Gray ordering of the subspaces. We also mention [22], in which only a decoding algorithm was suggested, without Gray coding, achieving complexity of $O(M[n^2]\log n)$.

We can, however, improve the complexity of the decoding procedure for a certain asymptotic range of k by changing the

[1] To be more precise, it was shown in [28] that computing $\begin{bmatrix} n-1 \\ k \end{bmatrix}_q$ takes $O(kn(n-k)\log n \log\log n)$ operations. To facilitate a comparison with the complexity analysis we perform, and by taking $n-k = \Theta(n)$ due to Lemma 13, we may rewrite the result of [28] as $O(M[nk]k)$. We will implicitly perform this translation whenever comparing with [28], and later, with [22].

way we compute (3). We start by changing the way we compute the Gaussian coefficients. By definition,

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}.$$

Our strategy to compute this value is to compute separately the numerator and denominator, and then perform division. To compute the numerator, we partition the k parentheses into pairs and compute their product, partition the $k/2$ results into pairs, and so on. For ease of presentation, we can assume k is a power of 2 to avoid rounding, and this has no effect on the overall complexity. Initially, each of the numbers in the numerator may be represented by n digits in base q. Thus, the total number of operations to compute the numerator is

$$\sum_{i=1}^{\log k} \frac{k}{2^i} M[2^{i-1}n] = \frac{nk}{2} \sum_{i=1}^{\log k} \frac{M[2^{i-1}n]}{2^{i-1}n} \leqslant M[nk/2]\log k,$$

where the last inequality is due to the fact that $M[m]/m$ is a nondecreasing function. The same analysis applies to the denominator. Finally, we need to divide the numerator and denominator, each with at most nk digits, thus requiring additional $O(M[nk])$ operations. It follows that computing $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$ requires $O(M[nk]\log k)$.

The analysis of the remaining part of the algorithm is nearly the same. The only difference is that we do not use (4) and (5) at every iteration. Instead, whenever we find ourselves in the third case of (3) we compute the necessary Gaussian coefficients from scratch. We now make the crucial observation that the algorithm takes at most n iterations, at most k of which take the third case of (3). Thus, the total number of operations for a decoding procedure is $O(M[nk]k\log k)$.

Theorem 15: The decoding algorithm may be run using $O(M[nk]k\log k)$ operations.

We note that when $k\log k = o(n)$ (for example, when $k = O(n^{1-\epsilon})$ for some $0 < \epsilon < 1$) the decoding algorithm we presented outperforms the decoding algorithm of [28], including the $O(n^2k^2)$ decoding algorithm of [28] for the smaller range of $k < \log n \log\log n$. Furthermore, when $k = o(\sqrt{n})$, the decoding algorithm we presented outperforms the decoding algorithm of [22].

IV. Subspace Gray Codes

This section is devoted to study of subspace Gray codes. Unlike optimal Grassmannian Gray codes, which exist for all parameters, the case of subspace Gray codes appears to be more complicated. We begin with a nonexistence result, and then continue to constructing subspace Gray code for a limited set of cases.

A. Nonexistence Results

The next theorem shows that for half of the parameter space, optimal subspace Gray codes do not exist.

Theorem 16: There are no optimal $(n;q)$-subspace Gray codes (cyclic or not) when $n \geqslant 2$ is even, except for the noncyclic case with $n=2$ and $q=2$.

Proof: Let $n = 2m$, $m \geqslant 1$. Assume to the contrary such a code $\mathcal{C}$ exists, and $\mathcal{C} = C_0, C_1, \dots, C_{P-1}$. By the definition of the code, every time an m-dimensional subspace appears in the sequence, it is followed by an $(m+1)$-dimensional subspace or an $(m-1)$-dimensional subspace, except if it is the last in the sequence and the code is not cyclic. Since the code is optimal, all subspaces appear and so we must have

$$\begin{bmatrix} 2m \\ m+1 \end{bmatrix}_q + \begin{bmatrix} 2m \\ m-1 \end{bmatrix}_q \geqslant \begin{bmatrix} 2m \\ m \end{bmatrix}_q - 1. \tag{6}$$

If the code is cyclic, a stronger inequality must hold, since the last subspace is followed by the first subspace, and so

$$\begin{bmatrix} 2m \\ m+1 \end{bmatrix}_q + \begin{bmatrix} 2m \\ m-1 \end{bmatrix}_q \geqslant \begin{bmatrix} 2m \\ m \end{bmatrix}_q. \tag{7}$$

However,

$$\frac{\left[\begin{smallmatrix} 2m \\ m \end{smallmatrix}\right]_q}{\left[\begin{smallmatrix} 2m \\ m+1 \end{smallmatrix}\right]_q + \left[\begin{smallmatrix} 2m \\ m-1 \end{smallmatrix}\right]_q} = \frac{\left[\begin{smallmatrix} 2m \\ m \end{smallmatrix}\right]_q}{2\left[\begin{smallmatrix} 2m \\ m-1 \end{smallmatrix}\right]_q} = \frac{1}{2}\cdot\frac{q^{m+1}-1}{q^m-1} > 1, \tag{8}$$

for all $q \geqslant 2$, and thus, (7) never holds, and no cyclic optimal code exists.

Continuing with the noncyclic case, in light of (8), the only way for (6) to hold is that

$$\begin{bmatrix} 2m \\ m+1 \end{bmatrix}_q + \begin{bmatrix} 2m \\ m-1 \end{bmatrix}_q = \begin{bmatrix} 2m \\ m \end{bmatrix}_q - 1.$$

Using (8), we therefore need

$$\begin{bmatrix} 2m \\ m \end{bmatrix}_q = 1 + \frac{2q^m - 2}{q^{m+1} - 2q^m + 1}. \tag{9}$$

When $q \geqslant 4$, and for all $m \geqslant 1$, we have

$$0 < 2q^m - 2 < q^{m+1} - 2q^m + 1,$$

and so the RHS of (9) is not an integer.

When $q = 3$, for similar reasons, the RHS of (9) is not an integer except when $m = 1$, but then

$$\begin{bmatrix} 2 \\ 1 \end{bmatrix}_3 = 4 \neq 2 = 1 + \frac{2\cdot 3^1 - 2}{3^2 - 2\cdot 3^1 + 1}.$$

Finally, when $q = 2$, (9) becomes

$$\begin{bmatrix} 2m \\ m \end{bmatrix}_2 = 2^{m+1} - 1.$$

We observe that

$$\begin{aligned}\begin{bmatrix} 2m \\ m \end{bmatrix}_2 &= \frac{[2m]_2!}{[m]_2![m]_2!} \\ &= \frac{(2^{2m}-1)(2^{2m-1}-1)\dots(2^{m+1}-1)}{(2^m-1)(2^{m-1}-1)\dots(2^1-1)} \\ &\geqslant 2\frac{2^{2m-1}\cdot 2^{2m-2}\cdot\dots\cdot 2^m}{2^m\cdot 2^{m-1}\cdot\dots\cdot 2^1} \\ &= 2^{m(m-1)}.\end{aligned}$$

For $m \geqslant 3$, we have

$$2^{m(m-1)} > 2^{m+1} - 1.$$

Thus, to complete the proof we only need to check the case of $m = 2$, for which we find that

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_2 = 35 \neq 7 = 2^3 - 1.$$

■

We note that there does indeed exist an optimal noncyclic $(2;2)$-subspace Gray code:

$$\mathcal{C} = \langle(1,0)\rangle, \langle(0,0)\rangle, \langle(0,1)\rangle, \langle(0,1),(1,0)\rangle, \langle(1,1)\rangle.$$

B. Constructions

We now turn to the question of whether cyclic optimal $(n;q)$-subspace Gray codes exist when n is odd. The answer is trivial when $n = 1$. We also answer this in the positive for the cases of $n = 3, 5$ by using the q-analog solution to the middle-level problem given in [7]. We first describe the q-analog of the middle-level problem, and then show how a solution there gives a cyclic optimal subspace Gray code.

Let $n = 2m+1$ be an odd positive integer, and let W^n be a vector space over $\mathrm{GF}(q)$. We consider the following graph $\mathcal{M}_q(2m+1)$: the vertex set of the graph is $\begin{bmatrix} W^n \\ m \end{bmatrix} \cup \begin{bmatrix} W^n \\ m+1 \end{bmatrix}$, and two vertices W_1 and W_2 are connected by an edge iff $W_1 \subset W_2$ or $W_2 \subset W_1$. An $(n;q)$-subspace Gray code for the middle levels is a Hamiltonian path in $\mathcal{M}_q(n)$, and it is cyclic if it is a Hamiltonian circuit.

Etzion [7] proved the following theorem.

Theorem 17 [7]: For any q, a power of a prime, there exists a cyclic optimal $(3;q)$-subspace Gray code for the middle levels.

Using Theorem 17, we can prove the following theorem.

Theorem 18: For any q, a power of a prime, there exists a cyclic optimal $(3;q)$-subspace Gray code.

Proof: Let $\mathcal{C}'$ be the code guaranteed by Theorem 17,

$$\mathcal{C}' = C_0, C_1, \ldots, C_{P'-1},$$

where

$$P' = \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q + \begin{bmatrix} 3 \\ 2 \end{bmatrix}_q = 2(q^2+q+1).$$

We note that P' is even. Since this code contains all the subspaces in the middle levels, the only two vertices of $\mathcal{P}_q(3)$ not covered are W^3, the entire space, and W^0, the 0-D trivial subspace.

Since $\mathcal{C}'$ is cyclic, let us assume, without loss of generality, that $\dim(C_0) = 1$. We now pick an arbitrary odd integer $1 \leqslant i \leqslant P'-3$, and construct the sequence

$$\mathcal{C} = W^0, C_0, C_1, \ldots, C_i, W^3, C_{P'-1}, C_{P'-2}, \ldots, C_{i+1}.$$

We contend that $\mathcal{C}$ is a cyclic optimal $(3;q)$-subspace Gray code. Trivially, $\mathcal{C}$ contains all the subspaces of W^3 exactly once. Furthermore, since originally $\dim(C_i) = 1$ iff i is even, and $\dim(C_i) = 2$ iff i is odd, the resulting sequence is indeed a cyclic subspace Gray code. ■

For the construction of $(5;q)$-subspace Gray codes, we require a more in-depth view of Etzion's construction from [7]. Let $w \in \mathrm{GF}(q)^n$ be a vector of length n over $\mathrm{GF}(q)$. Since $\mathrm{GF}(q^n)$ may be viewed as the vector space $\mathrm{GF}(q)^n$, by abuse of notation, we may identify w with its equivalent element in $\mathrm{GF}(q^n)$. Thus, from now on, if $\alpha \in \mathrm{GF}(q^n)$ is some element, we denote by αw the product, in $\mathrm{GF}(q^n)$, of α with the equivalent of w in $\mathrm{GF}(q^n)$.

Let W_1 and W_2 be two m-dimensional subspaces of W^n over some finite field $\mathrm{GF}(q)$. We say W_1 and W_2 are equivalent if there exists some $\alpha \in \mathrm{GF}(q^n)$ such that

$$W_1 = \alpha W_2 = \{\alpha w \mid w \in W_2\}.$$

It is easy to see that this is indeed an equivalence relation, and the equivalence classes were called *necklaces* in [7]. As also noted in [7], if $\gcd(n,m) = 1$ then the size of any equivalence class is $\begin{bmatrix} n \\ 1 \end{bmatrix}_q$, and in particular, does not depend of m.

Etzion proved the following two theorems, which will be the starting point for our next construction.

Theorem 19 [7]: Let $n = 2m+1$ and let W^n be an n-dimensional vector space over $\mathrm{GF}(q)$, with $\alpha \in \mathrm{GF}(q^n)$ a primitive element. Assume

$$\mathcal{L} = X_0, Y_0, X_1, Y_1, \ldots, X_{s-1}, Y_{s-1}$$

is a sequence of distinct necklaces representatives such that

$$X_i \in \begin{bmatrix} W^n \\ m \end{bmatrix} \qquad Y_i \in \begin{bmatrix} W^n \\ m+1 \end{bmatrix},$$

and

$$X_i \subset Y_i \qquad Y_i \supset X_{i+1}.$$

If $\alpha^\ell X_0 \subset Y_{s-1}$ with $\gcd(\ell, \begin{bmatrix} n \\ 1 \end{bmatrix}_q) = 1$, then

$$\mathcal{C} = \mathcal{L}, \alpha^\ell \mathcal{L}, \alpha^{2\ell}\mathcal{L}, \ldots, \alpha^{\left(\begin{bmatrix} n \\ 1 \end{bmatrix}_q - 1\right)\ell}\mathcal{L},$$

is a cyclic $(n;q)$-subspace Gray code for the middle levels.

Theorem 20 [7]: For any q, a power of a prime, and $n = 5$, there exists a sequence as in Theorem 19, resulting in a cyclic optimal $(5;q)$-subspace Gray code for the middle levels.

While Theorem 19 refers to subspaces in the middle levels, it can be easily generalized.

Theorem 21: Let W^n be an n-dimensional vector space over $\mathrm{GF}(q)$, and let $\alpha \in \mathrm{GF}(q^n)$ be a primitive element. Assume $\mathcal{L} = X_0, X_1, \ldots, X_{s-1}$ is a path in $\mathcal{P}_q(n)$ visiting only representatives of distinct necklaces. If all the visited necklaces are of equal size N, $\alpha^\ell X_0$ and X_{s-1} are adjacent in $\mathcal{P}_q(n)$, and $\gcd(\ell, N) = 1$, then

$$\mathcal{C} = \mathcal{L}, \alpha^\ell\mathcal{L}, \alpha^{2\ell}\mathcal{L}, \ldots, \alpha^{(N-1)\ell}\mathcal{L},$$

is a cyclic $(n;q)$-subspace Gray code.

Proof: It can be easily verified that all adjacent elements in $\mathcal{C}$ are adjacent in $\mathcal{P}_q(n)$ (including the first and last one), and since all necklaces are of equal size, all the elements of $\mathcal{C}$ are distinct. ■

We are now in a position to state and prove a construction for $(5;q)$-subspace Gray codes.

Theorem 22: For any q, a power of a prime, there exists a cyclic optimal $(5;q)$-subspace Gray code.

Proof: Let W^5 be a 5-D vector space over $\mathrm{GF}(q)$. Since 5 is prime, the sizes of necklaces of dimensions 1 through 4 are all the same and equal to $\left[\begin{smallmatrix}5\\1\end{smallmatrix}\right]_q$. In particular, this means that there is exactly one necklace of dimension 1, and exactly one necklace of dimension 4.

Let

$$\mathcal{L} = X_0, Y_0, X_1, Y_1, \ldots, X_{s-1}, Y_{s-1},$$

be a sequence of necklaces representatives, $\dim(X_i) = 2$, $\dim(Y_i) = 3$, as in Theorem 20, where

$$s = \begin{bmatrix}5\\2\end{bmatrix}_q \Big/ \begin{bmatrix}5\\1\end{bmatrix}_q = \begin{bmatrix}5\\3\end{bmatrix}_q \Big/ \begin{bmatrix}5\\1\end{bmatrix}_q = q^2 + 1 \geqslant 2.$$

We construct $\mathcal{L}'$ by reversing the order of Y_0 and X_1, and inserting two new necklaces

$$\mathcal{L}' = X_0, X_0 \cap X_1, X_1, Y_0, Y_0 + Y_1, Y_1, \ldots, X_{s-1}, Y_{s-1}.$$

Since $X_0, X_1 \subset Y_0$, while $X_0 \neq X_1$, $\dim(X_0) = \dim(X_1) = 2$, and $\dim(Y_0) = 3$, we must have

$$\dim(X_0 \cap X_1) = 1.$$

Furthermore, $Y_0, Y_1 \supset X_1$, and $Y_0 \neq Y_1$, hence

$$\dim(Y_0 + Y_1) = \dim(Y_0) + \dim(Y_1) - \dim(Y_0 \cap Y_1) = 4.$$

The sequence $\mathcal{L}'$ clearly satisfies the requirements of Theorem 21. Let $\mathcal{C}'$ be the cyclic $(5; q)$-subspace Gray code constructed in Theorem 21 using $\mathcal{L}'$. It is easily seen that $\mathcal{C}'$ contains all of the subspaces of W^5 except for W^5 and W^0, the trivial 0-D subspace. We use a series of subsequence reversals, similar to the above reversal, to make room to insert W^0 and W^5.

The code $\mathcal{C}'$ is comprised of subsequence blocks of the form $\alpha^{i\ell}\mathcal{L}'$,

$$\mathcal{C}' = \mathcal{L}', \alpha^{\ell}\mathcal{L}', \alpha^{2\ell}\mathcal{L}', \ldots, \alpha^{\left(\left[\begin{smallmatrix}5\\1\end{smallmatrix}\right]_q - 1\right)\ell}\mathcal{L}'.$$

There are $\left[\begin{smallmatrix}5\\1\end{smallmatrix}\right]_q$ such blocks, each of length $s + 2 = q^2 + 3$. We now zoom in on the first two blocks, $\mathcal{L}'$ and $\alpha^{\ell}\mathcal{L}'$. First, in the block $\mathcal{L}'$, we reverse the order of the third, fourth, and fifth elements, thus obtaining

$$\mathcal{L}'' = X_0, X_0 \cap X_1, Y_0 + Y_1, Y_0, X_1, Y_1, \ldots, X_{s-1}, Y_{s-1}.$$

We do the same in $\alpha^{\ell}\mathcal{L}'$ and obtain $\alpha^{\ell}\mathcal{L}''$. We note that except for $X_0 \cap X_1$ and $Y_0 + Y_1$, any two adjacent elements in the sequence are also adjacent in $\mathcal{P}_q(n)$.

Next, in the combined two blocks $\mathcal{L}'', \alpha^{\ell}\mathcal{L}''$, we reverse the sequence of elements starting from $Y_0 + Y_1$ and ending with $\alpha^{\ell}(X_0 \cap X_1)$, and then insert W^5 and W^0 to obtain

$$\begin{aligned}\mathcal{L}^* = {} & X_0, X_0 \cap X_1, W^0, \alpha^{\ell}(X_0 \cap X_1), \alpha^{\ell}X_0,\\ & Y_{s-1}, X_{s-1}, Y_{s-2}, X_{s-2} \ldots, Y_2, X_2,\\ & Y_1, X_1, Y_0, Y_0 + Y_1, W^5, \alpha^{\ell}(Y_0 + Y_1), \alpha^{\ell}Y_0,\\ & \alpha^{\ell}X_1, \alpha^{\ell}Y_1, \ldots, \alpha^{\ell}X_{s-1}, \alpha^{\ell}Y_{s-1}.\end{aligned}$$

It is now easy to verify that $\mathcal{L}^*$ describes a path in $\mathcal{P}_q(n)$, and that replacing the first two blocks in $\mathcal{C}'$ with $\mathcal{L}^*$ gives

$$\mathcal{C} = \mathcal{L}^*, \alpha^{2\ell}\mathcal{L}', \alpha^{3\ell}\mathcal{L}', \ldots, \alpha^{\left(\left[\begin{smallmatrix}5\\1\end{smallmatrix}\right]_q - 1\right)\ell}\mathcal{L}',$$

which is indeed a cyclic optimal $(5; q)$-subspace Gray code. ■

We remark in passing that the choices for which subsequences to reverse in the proof were made specific for ease of presentation. A similar more general construction can be described, in which the reversal process allows for more choices of reversal positions.

V. Conclusion

We studied optimal Gray codes for subspaces in two settings: the Grassmann graph, and the projective-space graph. In the first case, we were able to construct cyclic optimal Gray codes for all parameters using a recursive construction. In addition, simple recursive encoding and decoding functions were provided. These algorithm induce an enumerative-coding scheme, which is at least as efficient as known schemes, and for certain parameters, surpasses them.

In the case of the projective-space graph, it was shown that there are no optimal Gray codes (cyclic or not) in the projective-space graph of even dimension. For odd dimensions, we were able to show a construction for dimensions 3 and 5, which are derived from constructions for the middle-levels problem of the same dimension.

Some related open questions arise. The first is whether there exist cyclic optimal subspace Gray codes for *all* even dimensions. The second question is whether a reverse connection exists which derives optimal codes for the middle-levels problem from a subspace Gray code. Even in three dimensions the answer to the latter is not clear.

We also note that Gaussian coefficients obey another recursion, namely,

$$\begin{aligned}\begin{bmatrix}n\\k\end{bmatrix}_q &= \begin{bmatrix}n-1\\k\end{bmatrix}_q + q^{n-k}\begin{bmatrix}n-1\\k-1\end{bmatrix}_q\\ &= q^k\begin{bmatrix}n-1\\k\end{bmatrix}_q + \begin{bmatrix}n-1\\k-1\end{bmatrix}_q.\end{aligned}$$

While Construction A uses the former, it is unclear whether a different construction may use the latter, perhaps resulting in other more efficient enumerative-coding schemes.

Acknowledgment

The author would like to thank T. Etzion for valuable discussions which contributed to the content of this paper. The author would also like to thank M. Médard for hosting him at MIT during his sabbatical.

References

[1] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, and A. Wassermann, "Existence of q-analogs of Steiner systems," Apr. 2013 [Online]. Available: http://arxiv.org/pdf/1304.1462v2

[2] C. C. Chang, H. Y. Chen, and C. Y. Chen, "Symbolic Gray code as a data allocation scheme for two-disc systems," *Comput. J.*, vol. 35, pp. 299–305, 1992.

[3] M. Chen and K. G. Shin, “Subcube allocation and task migration in hypercube machines,” *IEEE Trans. Comput.*, vol. 39, no. 9, pp. 1146–1155, 1990.
[4] T. Cover, “Enumerative source encoding,” *IEEE Trans. Inf. Theory*, vol. IT-19, no. 1, pp. 73–77, Jan. 1973.
[5] P. Diaconis and S. Holmes, “Gray codes for randomization procedures,” *Stat. Comput.*, vol. 4, pp. 287–302, 1994.
[6] E. En Gad, M. Langberg, M. Schwartz, and J. Bruck, “Constant-weight Gray codes for local rank modulation,” *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7431–7442, Nov. 2011.
[7] T. Etzion, “The q-analog of the middle levels problem,” Mar. 2013 [Online]. Available: http://arxiv.org/pdf/1303.7110v1
[8] T. Etzion and N. Silberstein, “Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams,” *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 2909–2919, Jul. 2009.
[9] T. Etzion and A. Vardy, “Error-correcting codes in projective space,” *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1165–1173, Feb. 2011.
[10] C. Faloutsos, “Gray codes for partial match and range queries,” *IEEE Trans. Softw. Eng.*, vol. 14, no. 10, pp. 1381–1393, Oct. 1988.
[11] P. Frankl and R. M. Wilson, “The Erdös-Ko-Rado theorem for vector spaces,” *J. Combinatorial Theory Ser. A*, vol. 43, pp. 228–236, 1986.
[12] M. Fürer, “Faster integer multiplication,” *SIAM J. Comput.*, vol. 39, pp. 979–1005, Sep. 2009.
[13] M. Gadouleau and Z. Yan, “Constant-rank codes and their connection to constant-dimension codes,” *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3207–3216, Jul. 2010.
[14] M. Gadouleau and Z. Yan, “Packing and covering properties of subspace codes for error control in random linear network coding,” *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2097–2108, May 2010.
[15] M. Gardner, “The curious properties of the Gray code and how it can be used to solve puzzles,” *Sci. Amer.*, vol. 227, pp. 106–109, 1972.
[16] F. Gray, “Pulse code communication,” Mar. 1953, U.S. Patent 2632058.
[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] D. E. Knuth, *The Art of Computer Programming Volume 2: Seminumerical Algorithms*, 3rd ed. Reading, MA, USA: Addison-Wesley, 1997.
[19] R. Koetter and F. R. Kschischang, “Coding for errors and erasures in random network coding,” *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.
[20] R. M. Losee, “A Gray code based ordering for documents on shelves: Classification for browsing and retrieval,” *J. Amer. Soc. Inf. Sci.*, vol. 43, pp. 312–322, 1992.
[21] J. M. Ludman, “Gray codes generation for MPSK signals,” *IEEE Trans. Commun.*, vol. COM-29, no. 10, pp. 1519–1522, Oct. 1981.
[22] Y. Medvedeva, “Fast enumeration for Grassmannian space,” in *Proc. IEEE Int. Symp. Probl. Redund. Inf. Control Syst.*, St. Petersburg, Russia, Sep. 2012, pp. 48–52.
[23] D. Richards, “Data compression and Gray-code sorting,” *Inf. Process. Lett.*, vol. 22, pp. 201–205, 1986.
[24] J. Robinson and M. Cohn, “Counting sequences,” *IEEE Trans. Comput.*, vol. C-30, no. 1, pp. 17–23, May 1981.
[25] C. D. Savage, “A survey of combinatorial Gray codes,” *SIAM Rev.*, vol. 39, no. 4, pp. 605–629, Dec. 1997.
[26] M. Schwartz and T. Etzion, “The structure of single-track Gray codes,” *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2383–2396, Nov. 1999.
[27] M. Schwartz and T. Etzion, “Codes and anticodes in the Grassmann graph,” *J. Combinatorial Theory Ser. A*, vol. 97, no. 1, pp. 27–42, Jan. 2002.
[28] N. Silberstein and T. Etzion, “Enumerative coding for Grassmannian space,” *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 365–374, Jan. 2011.
[29] D. Silva and F. R. Kschischang, “On metric for error correction in network coding,” *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5479–5490, Dec. 2009.
[30] D. Silva, F. R. Kschischang, and R. Koetter, “A rank-metric approach to error control in random network coding,” *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.
[31] V. Skachek, “Recursive code construction for random networks,” *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1378–1382, Mar. 2010.
[32] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2001.
[33] S. T. Xia and F. W. Fu, “Johnson type bounds on constant dimension codes,” *Designs, Codes Cryptography*, vol. 50, pp. 163–172, 2009.
[34] E. Yaakobi, M. Schwartz, M. Langberg, and J. Bruck, “Sequence reconstruction for Grassmann graphs and permutations,” presented at the IEEE Int. Symp. Inf. Theory, Istanbul, Turkey, Jul. 2013.
[35] 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.

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 is currently on a sabbatical as a visiting scientist in the Research Laboratory of Electronics, MIT, in Cambridge, MA.

Dr. Schwartz 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.