Advances in Mathematics of Communications
Volume 5, No. 2, 2011, 177–189
doi:10.3934/amc.2011.5.177

# LARGE CONSTANT DIMENSION CODES AND LEXICODES

Natalia Silberstein and Tuvi Etzion

Computer Science Department
Technion – Israel Institute of Technology
Haifa, 32000, Israel

(Communicated by Eimear Byrne)

Abstract. Constant dimension codes, with a prescribed minimum distance, have found recently an application in network coding. All the codewords in such a code are subspaces of $\mathbb{F}_q^n$ with a given dimension. A computer search for large constant dimension codes is usually inefficient since the search space domain is extremely large. Even so, we found that some constant dimension lexicodes are larger than other known codes. We show how to make the computer search more efficient. In this context we present a formula for the computation of the distance between two subspaces, not necessarily of the same dimension.

## 1. Introduction

Let $\mathbb{F}_q$ be the finite field of size $q$. The set of all $k$-dimensional subspaces of the vector space $\mathbb{F}_q^n$, for any given two nonnegative integers $k$ and $n$, $0 < k < n$, forms the *Grassmannian space* (Grassmannian, in short) over $\mathbb{F}_q$, denoted by $\mathcal{G}_q(n,k)$. It is well known that

$$\left|\mathcal{G}_q(n,k)\right| = \begin{bmatrix} n \\ k \end{bmatrix}_q \stackrel{\text{def}}{=} \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} ,$$

where $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the *$q$-ary Gaussian coefficient*. The Grassmannian space is a metric space, where the *subspace distance* between any two subspaces $X$ and $Y$ in $\mathcal{G}_q(n,k)$, is given by

$$d_S(X,Y) \stackrel{\text{def}}{=} \dim X + \dim Y - 2\dim\big(X \cap Y\big). \tag{1}$$

This is also the definition for the distance between two subspaces of $\mathbb{F}_q^n$ which are not of the same dimension.

We say that $\mathbb{C} \subseteq \mathcal{G}_q(n,k)$ is an $(n, M, d, k)_q$ *code in the Grassmannian*, or *constant-dimension code*, if $M = |\mathbb{C}|$ and $d_S(X,Y) \geq d$ for all distinct elements $X,Y \in \mathbb{C}$. The minimum distance of $\mathbb{C}$, $d_S(\mathbb{C})$, is $d$.

Koetter and Kschischang [10] presented an application of error-correcting codes in $\mathcal{G}_q(n,k)$ to random network coding. This led to an extensive research for construction of large codes in the Grassmannian. Constructions and bounds for such codes were given in [4, 5, 9, 10, 11, 15, 16, 17].

---

2000 *Mathematics Subject Classification:* Primary: 14M15, 94B60; Secondary: 94B65.
*Key words and phrases:* Grassmannian, constant dimension code, lexicode, Ferrers diagram.
This work was supported in part by the Israel Science Foundation (ISF), Jerusalem, Israel, under Grant 230/08.

The motivation for this work is an $(8, 4605, 4, 4)_2$ constant dimension lexicode constructed in [15] which is larger than any other known codes with the same parameters.

*Lexicographic codes*, or *lexicodes*, are greedily generated error-correcting codes which were first developed by Levenshtein [12], and rediscovered by Conway and Sloane [2]. The construction of a lexicode with a minimum distance $d$ starts with the set $\mathcal{S} = \{S_0\}$, where $S_0$ is the first element in a lexicographic order, and greedily adds the lexicographically first element whose distance from all the elements of $\mathcal{S}$ is at least $d$. In the Hamming space, the lexicodes include the optimal codes, such as the Hamming codes and the Golay codes.

To construct a lexicode, we need first to define some order of all subspaces in the Grassmannian. The $(8, 4605, 4, 4)_2$ lexicode found in [15] is based on the Ferrers tableaux form representation of a subspace. First, for completeness, we provide the definitions which are required to define the Ferrers tableaux form representation of subspaces in the Grassmannian, and next, we define the order of the Grassmannian based on this representation.

A *partition* of a positive integer $m$ is a representation of $m$ as a sum of positive integers, not necessarily distinct.

A *Ferrers diagram* $\mathcal{F}$ represents a partition as a pattern of dots with the $i$-th row having the same number of dots as the $i$-th term in the partition [1, 13, 18]. (In the sequel, a *dot* will be denoted by a "•"). A Ferrers diagram satisfies the following conditions.

- The number of dots in a row is at most the number of dots in the previous row.
- All the dots are shifted to the right of the diagram.

The *number of rows (columns)* of the Ferrers diagram $\mathcal{F}$ is the number of dots in the rightmost column (top row) of $\mathcal{F}$. If the number of rows in the Ferrers diagram is $m$ and the number of columns is $\eta$, we say that it is an $m \times \eta$ Ferrers diagram.

Let $X \in \mathcal{G}_q(n, k)$ be a $k$-dimensional subspace in the Grassmannian. We can represent $X$ by the $k$ linearly independent vectors from $X$ which form a unique $k \times n$ generator matrix in *reduced row echelon form* (RREF), denoted by $RE(X)$, and defined as follows:

- The leading coefficient of a row is always to the right of the leading coefficient of the previous row.
- All leading coefficients are *ones*.
- Every leading coefficient is the only nonzero entry in its column.

For each $X \in \mathcal{G}_q(n, k)$ we associate a binary vector of length $n$ and weight $k$, $v(X)$, called the *identifying vector* of $X$, where the *ones* in $v(X)$ are exactly in the positions where $RE(X)$ has the leading *ones*.

The *echelon Ferrers form* of a binary vector $v$ of length $n$ and weight $k$, $EF(v)$, is the $k \times n$ matrix in RREF with leading entries (of rows) in the columns indexed by the nonzero entries of $v$ and "•" in all entries which do not have terminal *zeroes* or *ones* (see [4]). The dots of this matrix form the Ferrers diagram $\mathcal{F}$ of $EF(v)$. If we substitute elements of $\mathbb{F}_q$ in the dots of $EF(v)$ we obtain a generator matrix in RREF of a $k$-dimensional subspace of $\mathcal{G}_q(n, k)$. $EF(v)$ and $\mathcal{F}$ will be called also the echelon Ferrers form and the Ferrers diagram of such a subspace, respectively.

The *Ferrers tableaux form* of a subspace $X$, denoted by $\mathcal{F}(X)$, is obtained by assigning the values of $RE(X)$ in the Ferrers diagram $\mathcal{F}_X$ of $X$. Each Ferrers tableaux form represents a unique subspace in $\mathcal{G}_q(n,k)$.

**Example 1.** Let $X$ be the subspace in $\mathcal{G}_2(7,3)$ with the following generator matrix in RREF:

$$RE(X) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Its identifying vector is $v(X) = 1011000$, and its echelon Ferrers form, Ferrers diagram, and Ferrers tableaux form are given by

$$\begin{bmatrix} 1 & \bullet & 0 & 0 & \bullet & \bullet & \bullet \\ 0 & 0 & 1 & 0 & \bullet & \bullet & \bullet \\ 0 & 0 & 0 & 1 & \bullet & \bullet & \bullet \end{bmatrix}, \quad \begin{array}{cccc} \bullet & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \end{array}, \quad \text{and} \quad \begin{array}{cccc} 0 & 1 & 1 & 0 \\ & 1 & 0 & 1 \\ & 0 & 1 & 1 \end{array}, \text{ respectively.}$$

Let $\mathcal{F}$ be a Ferrers diagram of a subspace $X \in \mathcal{G}_q(n,k)$. $\mathcal{F}$ can be embedded in a $k \times (n-k)$ box. We represent $\mathcal{F}$ by an integer vector of length $n-k$, $(\mathcal{F}_{n-k}, ..., \mathcal{F}_2, \mathcal{F}_1)$, where $\mathcal{F}_i$ is equal to the number of dots in the $i$-th column of $\mathcal{F}$, $1 \le i \le n-k$, where we number the columns from right to left. Note that $\mathcal{F}_{i+1} \le \mathcal{F}_i$, $1 \le i \le n-k-1$.

To define an order of all the subspaces in the Grassmannian we need first to define an order of all the Ferrers diagrams embedded in the $k \times (n-k)$ box. Let $|\mathcal{F}|$ denote the *size* of $\mathcal{F}$, i.e., the number of dots in $\mathcal{F}$. For two Ferrers diagrams $\mathcal{F}$ and $\widetilde{\mathcal{F}}$, we say that $\mathcal{F} < \widetilde{\mathcal{F}}$ if one of the following two conditions holds.

- $|\mathcal{F}| > |\widetilde{\mathcal{F}}|$;
- $|\mathcal{F}| = |\widetilde{\mathcal{F}}|$, and $\mathcal{F}_i > \widetilde{\mathcal{F}}_i$ for the least index $i$ where the two diagrams $\mathcal{F}$ and $\widetilde{\mathcal{F}}$ have a different number of dots.

Now, we define the following order of subspaces in the Grassmannian based on the Ferrers tableaux form representation. Let $X, Y \in \mathcal{G}_q(n,k)$ be two $k$-dimensional subspaces, and $RE(X)$, $RE(Y)$ their related RREFs. Let $v(X)$, $v(Y)$ be the identifying vectors of $X$, $Y$, respectively, and $\mathcal{F}_X$, $\mathcal{F}_Y$ the Ferrers diagrams of $EF(v(X))$, $EF(v(Y))$, respectively. Let $x_1, x_2, ..., x_{|\mathcal{F}_X|}$ and $y_1, y_2, ..., y_{|\mathcal{F}_Y|}$ be the entries of Ferrers tableaux forms $\mathcal{F}(X)$ and $\mathcal{F}(Y)$, respectively. The entries of a Ferrers tableaux form are numbered from right to left, and from top to bottom (see Example 7).

We say that $X < Y$ if one of the following two conditions holds.

- $\mathcal{F}_X < \mathcal{F}_Y$;
- $\mathcal{F}_X = \mathcal{F}_Y$, and $(x_1, x_2, ..., x_{|\mathcal{F}_X|}) < (y_1, y_2, ..., y_{|\mathcal{F}_Y|})$.

**Example 2.** Let $X, Y, Z, W \in \mathcal{G}_2(6,3)$ be given by

$$\mathcal{F}(X) = \begin{array}{ccc} 1 & 1 & 1 \\ 1 & 1 & 1 \\ & & 1 \end{array}, \quad \mathcal{F}(Y) = \begin{array}{ccc} 1 & 0 & 1 \\ & 0 & 0 \\ & 1 & 1 \end{array}, \quad \mathcal{F}(Z) = \begin{array}{ccc} 1 & 1 & 1 \\ & 1 & 1 \\ & & 0 \end{array}, \quad \mathcal{F}(W) = \begin{array}{ccc} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{array}.$$

By the definition, we have that $\mathcal{F}_Y < \mathcal{F}_X < \mathcal{F}_Z = \mathcal{F}_W$. Since $(z_1, z_2, ..., z_{|\mathcal{F}_Z|}) = (1,1,0,1,1,1) < (w_1, ..., w_{|\mathcal{F}_W|}) = (1,1,1,1,1,1)$, it follows that $Y < X < Z < W$.

The construction of lexicodes involves many computations of the distance between two subspaces of $\mathcal{G}_q(n,k)$. In Section 2 we develop a new formula for computation of the distance between two subspaces not necessarily of the same dimension.

This formula will enable a faster computation of the distance between any two subspaces of $\mathcal{G}_q(n,k)$. In Section 3 we examine several properties of constant dimension codes which will enable to simplify the computer search for large lexicodes. In Section 4 we describe a general search method for constant dimension lexicodes. We also present some improvements on the sizes of constant dimension codes. In Section 5 we summarize our results and present several problems for further research.

## 2. Computation of distance between subspaces

The research on error-correcting codes in the Grassmannian in general and on the search for related lexicodes in particular requires many computations of the distance between two subspaces in the Grassmannian. We will examine a more general problem of computation the distance between any two subspaces $X, Y \subseteq \mathbb{F}_q^n$ which do not necessarily have the same dimension. The motivation is to simplify the computations that lead to the next subspace which will be joined to the lexicode.

Let $A * B$ denotes the concatenation $\begin{pmatrix} A \\ B \end{pmatrix}$ of two matrices $A$ and $B$ with the same number of columns. By the definition of the subspace distance (1), it follows that

$$d_S(X,Y) = 2\,\mathrm{rank}(RE(X) * RE(Y)) - \mathrm{rank}(RE(X)) - \mathrm{rank}(RE(Y)). \tag{2}$$

Therefore, the calculation of $d_S(X,Y)$ can be done by using Gauss elimination. In this section we present an improvement on this calculation by using the representation of subspaces by Ferrers tableaux forms, from which their identifying vectors and their RREF are easily determined. We will present an alternative formula for the computation of the distance between two subspaces $X$ and $Y$.

For $X \in \mathcal{G}_q(n,k_1)$ and $Y \in \mathcal{G}_q(n,k_2)$, let $\rho(X,Y)$ $[\mu(X,Y)]$ be a set of indices (of coordinates) with common *zeroes* [*ones*] in $v(X)$ and $v(Y)$, i.e.,

$$\rho(X,Y) = \{i|\ v(X)_i = 0 \text{ and } v(Y)_i = 0\},$$

and

$$\mu(X,Y) = \{i|\ v(X)_i = 1 \text{ and } v(Y)_i = 1\}.$$

Note that $|\rho(X,Y)| + |\mu(X,Y)| + d_H(v(X),v(Y)) = n$, where $d_H(\cdot,\cdot)$ denotes the Hamming distance, and

$$|\mu(X,Y)| = \frac{k_1 + k_2 - d_H(v(X),v(Y))}{2}. \tag{3}$$

Let $X_\mu$ be the $|\mu(X,Y)| \times n$ sub-matrix of $RE(X)$ which consists of the rows with leading *ones* in the columns related to (indexed by) $\mu(X,Y)$. Let $X_{\mu^C}$ be the $(k_1 - |\mu(X,Y)|) \times n$ sub-matrix of $RE(X)$ which consists of all the rows of $RE(X)$ which are not contained in $X_\mu$. Similarly, let $Y_\mu$ be the $|\mu(X,Y)| \times n$ sub-matrix of $RE(Y)$ which consists of the rows with leading *ones* in the columns related to $\mu(X,Y)$. Let $Y_{\mu^C}$ be the $(k_2 - |\mu(X,Y)|) \times n$ sub-matrix of $RE(Y)$ which consists of all the rows of $RE(Y)$ which are not contained in $Y_\mu$.

Let $\widetilde{X}_\mu$ be the $|\mu(X,Y)| \times n$ sub-matrix of $RE(RE(X) * Y_{\mu^C})$ which consists of the rows with leading *ones* in the columns indexed by $\mu(X,Y)$. Intuitively, $\widetilde{X}_\mu$ obtained by concatenation of the two matrices, $RE(X)$ and $Y_{\mu^C}$, and "cleaning" (by adding the corresponding rows of $Y_{\mu^C}$) all the nonzero entries in columns of $RE(X)$ indexed by leading *ones* in $Y_{\mu^C}$. Finally, $\widetilde{X}_\mu$ is obtained by taking only the rows which are indexed by $\mu(X,Y)$. Thus, $\widetilde{X}_\mu$ has all-zeroes columns indexed by

*ones* of $v(Y)$ and $v(X)$ which are not in $\mu(X,Y)$. Hence $\widetilde{X}_\mu$ has nonzero elements only in columns indexed by $\rho(X,Y) \cup \mu(X,Y)$.

Let $\widetilde{Y}_\mu$ be the $|\mu(X,Y)| \times n$ sub-matrix of $RE(RE(Y) * X_{\mu^C})$ which consists of the rows with leading *ones* in the columns indexed by $\mu(X,Y)$. Similarly to $\widetilde{X}_\mu$, it can be verified that $\widetilde{Y}_\mu$ has nonzero elements only in columns indexed by $\rho(X,Y) \cup \mu(X,Y)$.

**Corollary 1.** *Nonzero entries in $\widetilde{X}_\mu - \widetilde{Y}_\mu$ can appear only in columns indexed by $\rho(X,Y)$.*

*Proof.* An immediate consequence since the columns of $\widetilde{X}_\mu$ and $\widetilde{Y}_\mu$ indexed by $\mu(X,Y)$ form a $|\mu(X,Y)| \times |\mu(X,Y)|$ identity matrix. □

**Theorem 2.1.**

$$d_S(X,Y) = d_H(v(X),v(Y)) + 2\,\mathrm{rank}(\widetilde{X}_\mu - \widetilde{Y}_\mu). \tag{4}$$

*Proof.* By (2) it is sufficient to proof that

$$2\,\mathrm{rank}(RE(X) * RE(Y)) = k_1 + k_2 + d_H(v(X),v(Y)) + 2\,\mathrm{rank}(\widetilde{X}_\mu - \widetilde{Y}_\mu). \tag{5}$$

It is easy to verify that

$$\begin{aligned} \mathrm{rank}\begin{pmatrix} RE(X) \\ RE(Y) \end{pmatrix} &= \mathrm{rank}\begin{pmatrix} RE(X) \\ Y_{\mu^C} \\ Y_\mu \end{pmatrix} = \mathrm{rank}\begin{pmatrix} RE(X) \\ Y_{\mu^C} \\ \widetilde{Y}_\mu \end{pmatrix} \\ &= \mathrm{rank}\begin{pmatrix} RE(RE(X) * Y_{\mu^C}) \\ \widetilde{Y}_\mu \end{pmatrix} = \mathrm{rank}\begin{pmatrix} RE(RE(X) * Y_{\mu^C}) \\ \widetilde{Y}_\mu - \widetilde{X}_\mu \end{pmatrix}. \end{aligned} \tag{6}$$

We note that the positions of the leading *ones* in all the rows of $RE(X) * Y_{\mu^C}$ are in $\{1,2,\ldots,n\} \setminus \rho(X,Y)$. By Corollary 1 the positions of the leading *ones* of all the rows of $RE(\widetilde{Y}_\mu - \widetilde{X}_\mu)$ are in $\rho(X,Y)$. Thus, by (6) we have

$$\mathrm{rank}(RE(X) * RE(Y)) = \mathrm{rank}(RE(RE(X) * Y_{\mu^C}) + \mathrm{rank}(\widetilde{Y}_\mu - \widetilde{X}_\mu). \tag{7}$$

Since the sets of positions of the leading *ones* of $RE(X)$ and $Y_{\mu^C}$ are disjoint, we have that $\mathrm{rank}(RE(X) * Y_{\mu^C}) = k_1 + (k_2 - |\mu(X,Y)|)$, and thus by (7)

$$\mathrm{rank}(RE(X) * RE(Y)) = k_1 + k_2 - |\mu(X,Y)| + \mathrm{rank}(\widetilde{Y}_\mu - \widetilde{X}_\mu). \tag{8}$$

Combining (8) and (3) we have

$$2\,\mathrm{rank}(RE(X) * RE(Y)) = k_1 + k_2 + d_H(v(X),v(Y)) + 2\,\mathrm{rank}(\widetilde{Y}_\mu - \widetilde{X}_\mu),$$

and by (5) this proves the theorem. □

**Corollary 2.** *For any two subspaces $X, Y \subseteq \mathbb{F}_q^n$,*

$$d_S(X,Y) \geq d_H(v(X),v(Y)).$$

**Corollary 3.** *Let $X$ and $Y$ be two subspaces such that $v(X) = v(Y)$. Then*

$$d_S(X,Y) = 2\,\mathrm{rank}(RE(X) - RE(Y)).$$

In the sequel we will show how we can use these results to make the search of lexicodes more efficient.

## 3. Analysis of constant dimension codes

In this section we consider some properties of constant dimension codes which will help us to simplify the search for lexicodes. First, we introduce the multilevel structure of a code in the Grassmannian.

All the binary vectors of the length $n$ and weight $k$ can be considered as the identifying vectors of all the subspaces in $\mathcal{G}_q(n,k)$. These $\binom{n}{k}$ vectors partition $\mathcal{G}_q(n,k)$ into the $\binom{n}{k}$ different classes, where each class consists of all subspaces in $\mathcal{G}_q(n,k)$ with the same identifying vector. These classes are called *Schubert cells* [7, p. 147]. Note that each Schubert cell contains all the subspaces with the same given echelon Ferrers form.

According to this partition all the constant dimension codes have a multilevel structure: we can partition all the codewords of a code into different classes (sub-codes), each of which have the same identifying vector. Therefore, the first level of this structure is the set of different identifying vectors, and the second level is the subspaces corresponding to these vectors.

Let $\mathbb{C} \subseteq \mathcal{G}_q(n,k)$ be a constant dimension code, and let $\{v_1, v_2, \ldots, v_t\}$ be all the different identifying vectors of the codewords in $\mathbb{C}$. Let $\{\mathbb{C}_1, \mathbb{C}_2, \ldots, \mathbb{C}_t\}$ be the partition of $\mathbb{C}$ into $t$ sub-codes induced by these $t$ identifying vectors, i.e., $v(X) = v_i$, for each $X \in \mathbb{C}_i$, $1 \leq i \leq t$.

**Remark 1.** We can choose any constant weight code $C$ with minimum Hamming distance $d$ to be the set of identifying vectors. If for each identifying vector $v \in C$ we have a sub-code $\mathbb{C}_v$ for which $v(X) = v$ for each $X \in \mathbb{C}_v$, and $d_S(\mathbb{C}_v) = d$, then by Corollary 2 we obtain a constant dimension code with the same minimum distance $d$. If for all such identifying vectors we construct the maximum size constant dimension sub-codes then we obtain the multilevel construction (ML construction, in short) which was described in [4]. One question that arises in this context is how to choose the best constant weight code for this ML construction.

To understand the structure of a sub-code formed by some Ferrers diagram induced by an identifying vector, we need the following definitions.

For two $m \times \eta$ matrices $A$ and $B$ over $\mathbb{F}_q$ the *rank distance*, $d_R(A,B)$, is defined by

$$d_R(A,B) \stackrel{\text{def}}{=} \operatorname{rank}(A-B) \ .$$

A code $\mathcal{C}$ is an $[m \times \eta, \varrho, \delta]$ *rank-metric code* if its codewords are $m \times \eta$ matrices over $\mathbb{F}_q$, they form a linear subspace of dimension $\varrho$ of $\mathbb{F}_q^{m \times \eta}$, and for each two distinct codewords $A$ and $B$ we have that $d_R(A,B) \geq \delta$. For an $[m \times \eta, \varrho, \delta]$ rank-metric code $\mathcal{C}$ we have $\varrho \leq \min\{m(\eta - \delta + 1), \eta(m - \delta + 1)\}$ (see [3, 8, 14]). This bound is attained for all possible parameters and the codes which attain it are called *maximum rank distance* codes (or MRD codes in short).

Let $v$ be a vector of length $n$ and weight $k$ and let $EF(v)$ be its echelon Ferrers form. Let $\mathcal{F}$ be the Ferrers diagram of $EF(v)$. $\mathcal{F}$ is an $m \times \eta$ Ferrers diagram, $m \leq k$, $\eta \leq n - k$. A code $\mathcal{C}$ is an $[\mathcal{F}, \varrho, \delta]$ *Ferrers diagram rank-metric code* if all codewords of $\mathcal{C}$ are $m \times \eta$ matrices in which all entries not in $\mathcal{F}$ are *zeroes*, it forms a rank-metric code with dimension $\varrho$, and minimum rank distance $\delta$. Let $\dim(\mathcal{F}, \delta)$ be the largest possible dimension of an $[\mathcal{F}, \varrho, \delta]$ code. The following theorem [4] provides an upper bound on the size of such codes.

**Theorem 3.1.** *For a given $i$, $0 \leq i \leq \delta - 1$, if $\nu_i$ is the number of dots in $\mathcal{F}$, which are not contained in the first $i$ rows and are not contained in the rightmost $\delta - 1 - i$ columns, then $\min_i\{\nu_i\}$ is an upper bound on $\dim(\mathcal{F}, \delta)$.*

It is not known whether the upper bound of Theorem 3.1 is attained for all parameters. A code which attains this bound, will be called an MRD (Ferrers diagram) code. This definition generalizes the previous definition of MRD codes, and a construction of such codes is given in [4].

Without loss of generality we will assume that $k \leq n - k$. This assumption can be justified as a consequence of the following lemma [5].

**Lemma 3.2.** *If $\mathbb{C}$ is an $(n, M, d, k)_q$ constant dimension code then $\mathbb{C}^\perp = \{X^\perp : X \in \mathbb{C}\}$, where $X^\perp$ is the orthogonal subspace of $X$, is an $(n, M, d, n-k)_q$ constant dimension code.*

For $X \in \mathcal{G}_q(n, k)$, we define the $k \times (n - k)$ matrix $R(X)$ as the sub-matrix of $RE(X)$ with the columns which are indexed by *zeroes* of $v(X)$. By Corollary 3, for any two codewords $X, Y \in \mathbb{C}_i$, $\mathbb{C}_i \subseteq \mathbb{C}$, $1 \leq i \leq t$, the subspace distance between $X$ and $Y$ can be calculated in terms of rank distance, i.e.,

$$d_S(X, Y) = 2d_R(R(X), R(Y)).$$

For each sub-code $\mathbb{C}_i \subseteq \mathbb{C}$, $1 \leq i \leq t$, we define a Ferrers diagram rank-metric code

$$R(\mathbb{C}_i) \stackrel{\text{def}}{=} \{R(X) : X \in \mathbb{C}_i\}.$$

Note, that such a code is obtained by the inverse operation to the *lifting* operation, defined in [16]. Thus, $R(\mathbb{C}_i)$ will be called the *unlifted code* of the sub-code $\mathbb{C}_i$.

We define the subspace distance between two sub-codes $\mathbb{C}_i$, $\mathbb{C}_j$ of $\mathbb{C}$, $1 \leq i \neq j \leq t$ as follows:

$$d_S(\mathbb{C}_i, \mathbb{C}_j) = \min\{d_S(X, Y) : X \in \mathbb{C}_i, Y \in \mathbb{C}_j\}.$$

By Corollary 2,

$$d_S(\mathbb{C}_i, \mathbb{C}_j) \geq d_H(v_i, v_j).$$

The following lemma shows a case in which the last inequality becomes an equality.

**Lemma 3.3.** *Let $\mathbb{C}_i$ and $\mathbb{C}_j$ be two different sub-codes of $\mathbb{C} \subseteq \mathcal{G}_q(n, k)$, each one contains the subspace whose RREF is the corresponding column permutation of the matrix $(I_k 0_{k\times(n-k)})$, where $I_k$ denotes the $k \times k$ identity matrix and $0_{a\times b}$ denotes an $a \times b$ allzero matrix. Then*

$$d_S(\mathbb{C}_i, \mathbb{C}_j) = d_H(v_i, v_j).$$

*Proof.* Let $X \in \mathbb{C}_i$ and $Y \in \mathbb{C}_j$ be subspaces whose RREF equal to column permutation of the matrix $(I_k 0_{k\times(n-k)})$. It is easy to verify that

$$\text{rank}\begin{pmatrix} RE(X) \\ RE(Y) \end{pmatrix} = \text{rank}\begin{pmatrix} RE(X) \\ Y_{\mu^C} \\ Y_\mu \end{pmatrix} = \text{rank}\begin{pmatrix} RE(X) \\ Y_{\mu^C} \end{pmatrix}. \tag{9}$$

Clearly, $\text{rank}(Y_{\mu^C}) = \frac{d_H(v_i, v_j)}{2}$, and hence, $\text{rank}(RE(X) * RE(Y)) = k + \frac{d_H(v_i, v_j)}{2}$. By (2), $d_S(X, Y) = 2\text{rank}(RE(X) * RE(Y)) - 2k = 2k + d_H(v_i, v_j) - 2k = d_H(v_i, v_j)$, i.e., $d_S(\mathbb{C}_i, \mathbb{C}_j) \leq d_H(v_i, v_j)$. By Corollary 2, $d_S(\mathbb{C}_i, \mathbb{C}_j) \geq d_H(v_i, v_j)$, and hence, $d_S(\mathbb{C}_i, \mathbb{C}_j) = d_H(v_i, v_j)$. □

**Corollary 4.** *Let $v_i$ and $v_j$ be two identifying vectors of codewords in an $(n, M, d, k)_q$ code $\mathbb{C}$. If $d_H(v_i, v_j) < d$ then at least one of the corresponding sub-codes, $\mathbb{C}_i$ and $\mathbb{C}_j$, does not contain the subspace with RREF which is a column permutation of the matrix $(I_k 0_{k\times(n-k)})$. In other words, the corresponding unlifted code is not linear since it does not contain the allzero codeword.*

Assume that we can add codewords to a code $\mathbb{C}$, $d_S(\mathbb{C}) = d$, constructed by the ML construction with a maximal constant weight code (for the identifying vectors) $C$, $d_H(C) = d$. Corollary 4 implies that any corresponding unlifted Ferrers diagram rank-metric code of any new identifying vector will be nonlinear.

The next two lemmas reduce the search domain for constant dimension lexicodes.

**Lemma 3.4.** *Let $\mathbb{C}$ be an $(n, M, d = 2\delta, k)_q$ constant dimension code. Let $\mathbb{C}_1 \subseteq \mathbb{C}$, $v(X) = v_1 = 11\ldots100\ldots0$ for each $X \in \mathbb{C}_1$, be a sub-code for which $R(\mathbb{C}_1)$ attains the upper bound of Theorem 3.1, i.e., $|\mathbb{C}_1| = |R(\mathbb{C}_1)| = q^{(k-\delta+1)(n-k)}$. Then there is no codeword $Y$ in $\mathbb{C}$ such that $d_H(v(Y), v_1) < d$.*

*Proof.* Let $\mathbb{C}$ be a given $(n, M, d = 2\delta, k)_q$ constant dimension code. Since the minimum distance of the code is $d$, the intersection of any two subspaces in $\mathbb{C}$ is at most of dimension $k - \frac{d}{2} = k - \delta$. Therefore, a subspace of dimension $k - \delta + 1$ can be contained in at most one codeword of $\mathbb{C}$.

We define the following set of subspaces:

$$A = \{X \in \mathcal{G}_q(n, k-\delta+1) : \ supp(v(X)) \subseteq supp(v_1)\},$$

where $supp(v)$ is as the set of nonzero entries in $v$. Each codeword of the sub-code $\mathbb{C}_1$ contains $\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q$ subspaces of dimension $k - \delta + 1$, and all subspaces of dimension $k - \delta + 1$ which are contained in codewords of $\mathbb{C}_1$ are in $A$. Since $|\mathbb{C}_1| = q^{(k-\delta+1)(n-k)}$, it follows that $\mathbb{C}_1$ contains $q^{(k-\delta+1)(n-k)} \cdot \begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q$ subspaces of $A$.

Now we calculate the size of $A$. First we observe that

$$A = \big\{X \in \mathcal{G}_q(n, k-\delta+1) : v(X) = ab, \ |a| = k, \ |b| = n-k, \\ w(a) = k-\delta+1, \ w(b) = 0\big\},$$

where $|v|$ and $w(v)$ are the length and the weight of a vector $v$, respectively. Thus $EF(v(X))$ of each $v(X) = ab$, such that $X \in A$, has the form

$$EF(v(X)) = \begin{bmatrix} EF(a) & \bullet & \bullet & \ldots & \bullet \\ & \bullet & \bullet & \ldots & \bullet \\ & \bullet & \bullet & \ldots & \bullet \end{bmatrix}. \tag{10}$$

The number of dots in (10) is $(k - \delta + 1)(n - k)$, and the size of the following set

$$\{EF(a) : |a| = k, \ w(a) = k - \delta + 1\}$$

is $\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q$. Therefore, $|A| = \begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q \cdot q^{(k-\delta+1)(n-k)}$. Hence, each subspace of $A$ is contained in some codeword from $\mathbb{C}_1$. A subspace $Y \in \mathcal{G}_q(n, k)$ with $d_H(v(Y), v_1) = 2\delta - 2i$, $1 \le i \le \delta - 1$, contains some subspaces of $A$, and therefore, $Y \notin \mathbb{C}$. □

**Lemma 3.5.** *Let $\mathbb{C}$ be an $(n, M, d = 2\delta, k)_q$ constant dimension code, where $\delta - 1 \le k - \delta$. Let $\mathbb{C}_2$ be a sub-code of $\mathbb{C}$ which corresponds to the identifying vector*

*$v_2 = abfg$, where $a = \underbrace{11\ldots1}_{k-\delta}$, $b = \underbrace{00\ldots0}_{\delta}$, $f = \underbrace{11\ldots1}_{\delta}$, and $g = \underbrace{00\ldots0}_{n-k-\delta}$. Assume further that $R(\mathbb{C}_2)$ attains the upper bound of Theorem 3.1, i.e., $|\mathbb{C}_2| = |R(\mathbb{C}_2)| = q^{(k-\delta+1)(n-k)-\delta^2}$. Then there is no codeword $Y \in \mathbb{C}$ with $v(Y) = a'b'fg'$, $|a'b'| = k$, $|g'| = n-k-\delta$, such that $d_H(v(Y), v_2) < d$.*

*Proof.* Similarly to the proof of Lemma 3.4, we define the following set of subspaces:

$$B = \{X \in \mathcal{G}_q(n, k-\delta+1) : v(X) = a''bfg \text{ with } |a''| = k-\delta,\ w(a'') = k-2\delta+1\}.$$

As in the previous proof, we can see that $\mathbb{C}_2$ contains $q^{(k-\delta+1)(n-k)-\delta^2} \cdot \begin{bmatrix} k-\delta \\ k-2\delta+1 \end{bmatrix}_q$ subspaces of $B$. In addition, $|B| = \begin{bmatrix} k-\delta \\ k-2\delta+1 \end{bmatrix}_q \cdot q^{(k-2\delta+1)\delta+(k-\delta+1)(n-k-\delta)} = \begin{bmatrix} k-\delta \\ k-2\delta+1 \end{bmatrix}_q \cdot q^{(k-\delta+1)(n-k)-\delta^2}$. Thus each subspace in $B$ is contained in some codeword from $\mathbb{C}_2$. A subspace $Y \in \mathcal{G}_q(n,k)$, such that $v(Y) = a'b'fg'$ ($|a'b'| = k$, $|g'| = n-k-\delta$), with $d_H(v(Y), v_2) = 2\delta - 2i$, $1 \le i \le \delta - 1$, contains some subspaces of $B$, and therefore, $Y \notin \mathbb{C}$. □

## 4. Search for constant dimension lexicodes

In this section we describe our search method for constant dimension lexicodes, and present some resulting codes which are the largest currently known constant dimension codes for their parameters.

To search for large constant dimension code we use the multilevel structure of such codes, described in the previous section. First, we order the set of all binary words of length $n$ and weight $k$ by an appropriate order. The words in this order are the candidates to be the identifying vectors of the final code. In each step of the construction we have the current code $\mathbb{C}$ and the set of subspaces not examined yet. For each candidate for an identifying vector $v$ taken by the given order, we search for a sub-code in the following way: for each subspace $X$ (according to the lexicographic order of subspaces associated with $v$) with the given Ferrers diagram we calculate the distance between $X$ and $\mathbb{C}$, and add $X$ to $\mathbb{C}$ if this distance is at least $d$. By Theorem 2.1 and Corollary 2 it follows that in this process, for some subspaces it is enough only to calculate the Hamming distance between the identifying vectors in order to determine a lower bound on the subspace distance. In other words, when we examine a new subspace to be inserted into the lexicode, we first calculate the Hamming distance between its identifying vector and the identifying vector of a codeword, and only if this distance is smaller than $d$, we calculate the rank of the corresponding matrix, (see (4)). Moreover, by the multilevel structure of a code, we need only to examine the Hamming distance between the identifying vectors of representatives of sub-codes, say the first codewords in each sub-code. This approach will speed up the process of the code generation.

A construction of constant dimension lexicodes based on the Ferrers tableaux form ordering of the Grassmannian was mentioned in [15]. Note that in this construction we order the identifying vectors by the sizes of corresponding Ferrers diagrams. The motivation is that usually a larger diagram contributes more codewords than a smaller one.

**Example 3.** Table 1 shows the identifying vectors and the sizes of corresponding sub-codes in the $(8, 4605, 4, 4)_2$ lexicode, $\mathbb{C}^{lex}$ (see [15]), and the $(8, 4573, 4, 4)_2$ code, $\mathbb{C}^{ML}$, obtained by the ML construction [4].

TABLE 1. $\mathbb{C}^{lex}$ vs. $\mathbb{C}^{ML}$ in $\mathcal{G}_2(8, 4)$ with $d_S = 4$

| $i$ | id.vector $v_i$ | size of $\mathbb{C}_i^{lex}$ | size of $\mathbb{C}_i^{ML}$ |
|---|---|---|---|
| 1 | 11110000 | 4096 | 4096 |
| 2 | 11001100 | 256 | 256 |
| 3 | 10101010 | 64 | 64 |
| 4 | 10011010 | 16 | – |
| 5 | 10100110 | 16 | – |
| 6 | 00111100 | 16 | 16 |
| 7 | 01011010 | 16 | 16 |
| 8 | 01100110 | 16 | 16 |
| 9 | 10010110 | 16 | 16 |
| 10 | 01101001 | 32 | 32 |
| 11 | 10011001 | 16 | 16 |
| 12 | 10100101 | 16 | 16 |
| 13 | 11000011 | 16 | 16 |
| 14 | 01010101 | 8 | 8 |
| 15 | 00110011 | 4 | 4 |
| 16 | 00001111 | 1 | 1 |

We can see that these two codes have the same identifying vectors, except for two vectors 10011010 and 10100110 in the lexicode $\mathbb{C}^{lex}$ which form the difference in the size of these two codes. In addition, there are several sub-codes of $\mathbb{C}^{lex}$ for which the corresponding unlifted codes are nonlinear: $\mathbb{C}_4^{lex}$, $\mathbb{C}_5^{lex}$, $\mathbb{C}_7^{lex}$, $\mathbb{C}_8^{lex}$, $\mathbb{C}_{11}^{lex}$, and $\mathbb{C}_{12}^{lex}$. However, all these unlifted codes are cosets of linear codes.

In general, not all unlifted codes of lexicodes based on the Ferrers tableaux form representation are linear or cosets of some linear codes. However, if we construct a binary constant dimension lexicode with only one identifying vector, the unlifted code is always linear. This phenomenon can be explained as an immediate consequence from the main theorem in [19]. However, it does not explain why some of unlifted codes in Example 3 are cosets of linear codes, and why $\mathbb{C}_9^{lex}$ is linear ($d_H(v_5, v_9) < 4$)?

Based on Theorem 2.1, Lemmas 3.4, and 3.5, we suggest an improved search of a constant dimension $(n, M, d, k)_q$ code, which will be called a *lexicode with a seed*.

In the first step we construct a maximal sub-code $\mathbb{C}_1$ which corresponds to the identifying vector $\underbrace{11\ldots1}_{k}\underbrace{00\ldots0}_{n-k}$. This sub-code corresponds to the largest Ferrers diagram. In this step we can take any known $[k \times (n-k), (n-k)(k - \frac{d}{2} + 1), \frac{d}{2}]$ MRD code (e.g. [8]) and consider its codewords as the unlifted codewords (Ferrers tableaux forms) of $\mathbb{C}_1$.

In the second step we construct a sub-code $\mathbb{C}_2$ which corresponds to the identifying vector $\underbrace{11\ldots1}_{k-\delta}\underbrace{00\ldots0}_{\delta}\underbrace{11\ldots1}_{\delta}\underbrace{00\ldots0}_{n-k-\delta}$. According to Lemma 3.4, we cannot use identifying vectors with larger Ferrers diagrams (except for the identifying vector

$\underbrace{11\ldots1}_{k}\underbrace{00\ldots0}_{n-k}$ already used). If there exists an MRD (Ferrers diagram) code with the corresponding parameters, we can take any known construction of such code (see in [4]) and build from it the corresponding sub-code. If a code which attains the bound of Theorem 3.1 is not known, we take the largest known Ferrers diagram rank-metric code with the required parameters.

In the third step we construct the other sub-codes, according to the lexicographic order based on the Ferrers tableaux form representation. We first calculate the Hamming distance between the identifying vectors and examine the subspace distance only of subspaces which are not pruned out by Lemmas 3.4 and 3.5.

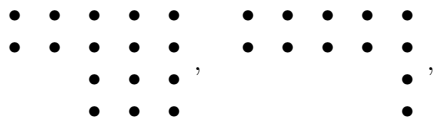
**Example 4.** Let $n = 10$, $k = 5$, $d = 6$, and $q = 2$. By the construction of a lexicode with a seed we obtain a constant dimension code of size 32890. (A code of size 32841 was obtained by the ML construction [4]).

**Example 5.** Let $n = 7$, $k = 3$, $d = 4$, and $q = 3$. By the construction a lexicode with a seed we obtain a constant dimension code of size 6691. (A code of size 6685 was obtained by the ML construction [4]).

We introduce now a variant of the construction of a lexicode with a seed. As a seed we take a constant dimension code obtained by the ML construction [4] and try to add some more codewords using the lexicode construction. Similarly, we can take as a seed any subset of codewords obtained by any given construction and to continue by applying the lexicode with a seed construction.

**Example 6.** Let $n = 8$, $k = d = 4$, and $q = 2$. We take the $(8, 4573, 4, 4)_2$ code obtained by the ML construction (see Table 1) and then continue with the lexicode construction. The size of the resulting code is 4589 (compared to $\mathbb{C}^{lex}$ of size 4605 in Table 1), where there are two additional sub-codes of size 8 which correspond to identifying vectors 10011010 and 10100110.

**Example 7.** Let $n = 9$, $k = d = 4$, and $q = 2$. Let $\mathbb{C}$ be a $(9, 2^{15} + 2^{11} + 2^7, 4, 4)_2$ code obtained as follows. We take three codes of sizes $2^{15}$, $2^{11}$, and $2^7$, corresponding to identifying vectors 111100000, 110011000, and 110000110, respectively, and then continue by applying the lexicode with a seed construction. For the identifying vector 111100000 we can take as the unlifted code, any code which attains the bound of Theorem 3.1. To generate the codes for the last two identifying vectors with the corresponding unlifted codes (which attains the bound of Theorem 3.1), we permute the order of entries in the Ferrers diagrams and apply the lexicode construction. The Ferrers diagrams which correspond to the identifying vector 110011000 and 110000110 are



respectively. The coordinates' order of their entries (defined in the Introduction) is:

$$\begin{array}{ccccc} 15 & 13 & 9 & 5 & 1 \\ 16 & 14 & 10 & 6 & 2 \\ & & 11 & 7 & 3 \\ & & 12 & 8 & 4 \end{array}, \qquad \begin{array}{ccccc} 11 & 9 & 7 & 5 & 1 \\ 12 & 10 & 8 & 6 & 2 \\ & & & & 3 \\ & & & & 4 \end{array},$$

respectively. The order of the coordinates that we use to form an MRD code (lexicode) is

$$\begin{array}{ccccc} 11 & 7 & 5 & 3 & 1 \\ 15 & 12 & 8 & 2 & 4 \\ & & 13 & 9 & 6 \\ & & 16 & 14 & 10 \end{array}, \quad \begin{array}{ccccc} 9 & 7 & 5 & 3 & 1 \\ 11 & 10 & 8 & 2 & 4 \\ & & & & 6 \\ & & & & 12 \end{array}.$$

As a result, we obtain a code of size 37649 which is the largest known constant dimension code with these parameters.

**Remark 2.** One of the most interesting questions, at least from a mathematical point of view, is the existence of a $(7, 381, 4, 3)_2$ code $\mathbb{C}$ [6]. If such code exists one can verify that it contains 128 codewords with the identifying vector 1110000 which is half the size of the corresponding MRD code. It suggests that the unlifted Ferrers diagram rank-metric code of the largest Ferrers diagram is not necessarily an MRD code, in the largest constant dimension code with given parameters $n$, $k$, and $d$.

**Remark 3.** The decoding of a code $\mathbb{C}$ constructed by the search method depends on the nature of the seed code ($\mathbb{C}_s$) and the size of rest of the code ($\mathbb{C}_r = \mathbb{C} \setminus \mathbb{C}_s$) produced by the greedy search. For example, if the identifying vectors of $\mathbb{C}_s$ form a constant weight code with minimum distance $d$, the related rank-metric codes have an efficient decoding algorithm, and $\mathbb{C}_r$ is relatively of small size then we can use the decoding algorithm mentioned in [4] to decode $\mathbb{C}_s$. For the decoding of the small code $\mathbb{C}_r$ we will use a look-up table.

**Remark 4.** It should be noted that the improvements yielded by the search method are not dramatic. Nevertheless, it is interesting to realize that simple greedy algorithm can be effective in enlarging a code obtained by a mathematical method. Furthermore, we used small parameters in our examples to make it possible for an interested reader to reconstruct the codes relatively easily; and also to save some space. But, the search method will work also on larger parameters as well. If the parameters will be too large then we might need to make a partial search for $\mathbb{C}_r$ to make the search feasible.

## 5. Conclusion and open problems

We have described a search method for constant dimension codes based on their multilevel structure. Some of the codes obtained by this search are the largest known constant dimension codes with their parameters. We described several ideas to make this search more efficient. In this context a new formula for computation of the subspace distance between two subspaces of $\mathbb{F}_q^n$ is given. It is reasonable to believe that the same ideas will enable to improve the sizes of the codes with parameters not considered in our examples. We hope that a general mathematical technique to generate related codes with larger size can be developed based on our discussion. Our discussion raises several more questions for future research:

1. Is the upper bound of Theorem 3.1 on the size of Ferrers diagram rank-metric code is attainable for all parameters?
2. What is the best choice of identifying vectors for constant dimension lexicode in general, and for the the ML construction in particular?
3. Can every MRD Ferrers diagram code be generated as a lexicode by using a proper permutation on the coordinates (see Example 7)?

4. Is there an optimal combination of linear Ferrers diagram rank-metric codes and cosets of linear Ferrers diagram rank-metric codes to form a large constant dimension code?
5. For which $n$ and $k$ there exists an order of all identifying vectors such that all the unlifted codes (of the lexicode) will be either linear or cosets of linear codes (see Example 3).

## REFERENCES


[1] G. E. Andrews and K. Eriksson, "Integer Partitions," Cambridge University Press, 2004.
[2] J. H. Conway and N. J. A. Sloane, *Lexicographic codes: error-correcting codes from game theory*, IEEE Trans. Inform. Theory, **32** (1986), 337–348.
[3] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, J. Combin. Theory Ser. A, **25** (1978), 226–241.
[4] T. Etzion and N. Silberstein, *Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams*, IEEE Trans. Inform. Theory, **55** (2009), 2909–2919.
[5] T. Etzion and A. Vardy, *Error-correcting codes in projective space*, in "Proceedings of International Symposium on Information Theory," (2008), 871–875.
[6] T. Etzion and A. Vardy, *On q-analogs for Steiner systems and covering designs*, Adv. Math. Commun., **5** (2011), 161–176.
[7] W. Fulton, "Young Tableaux," Cambridge University Press, 1997.
[8] E. M. Gabidulin, *Theory of codes with maximal rank distance*, Probl. Inform. Transm., **21** (1985), 1–12.
[9] M. Gadouleau and Z. Yan, *Constant-rank codes and their connection to constant-dimension codes*, IEEE Trans. Inform. Theory, **56** (2010), 3207–3216.
[10] R. Koetter and F. R. Kschischang, *Coding for errors and erasures in random network coding*, IEEE Trans. Inform. Theory, **54** (2008), 3579–3591.
[11] A. Kohnert and S. Kurz, *Construction of large constant dimension codes with a prescribed minimum distance*, Lecture Notes Comp. Sci., **5393** (2008), 31–42.
[12] V. L. Levenshtein, *A class of systematic codes*, Soviet Math. Dokl., **1** (1960), 368–371.
[13] J. H. van Lint and R. M. Wilson, "A Course in Combinatorics," $2^{nd}$ edition, Cambridge University Press, 2001.
[14] R. M. Roth, *Maximum-rank array codes and their application to crisscross error correction*, IEEE Trans. Inform. Theory, **37** (1991), 328–336.
[15] N. Silberstein and T. Etzion, *Enumerative coding for Grassmannian space*, IEEE Trans. Inform. Theory, **57** (2011), 365–374.
[16] D. Silva, F. R. Kschischang and R. Koetter, *A rank-metric approach to error control in random network coding*, IEEE Trans. Inform. Theory, **54** (2008), 3951–3967.
[17] V. Skachek, *Recursive code construction for random networks*, IEEE Trans. Inform. Theory, **56** (2010), 1378–1382.
[18] R. P. Stanley, "Enumerative Combinatorics," Wadsworth, 1986.
[19] A. J. Van Zanten, *Lexicographic order and linearity*, Des. Codes Crypt., **10** (1997), 85–97.


Received March 2010; revised September 2010.

*E-mail address:* natalys@cs.technion.ac.il
*E-mail address:* etzion@cs.technion.ac.il