Error-Correcting Codes in Projective Spaces Via Rank-Metric Codes and Ferrers Diagrams

Tuvi Etzion, *Fellow, IEEE*, and Natalia Silberstein

***Abstract*—Coding in the projective space has received recently a lot of attention due to its application in network coding. Reduced row echelon form of the linear subspaces and Ferrers diagram can play a key role for solving coding problems in the projective space. In this paper, we propose a method to design error-correcting codes in the projective space. We use a multilevel approach to design our codes. First, we select a constant-weight code. Each codeword defines a skeleton of a basis for a subspace in reduced row echelon form. This skeleton contains a Ferrers diagram on which we design a rank-metric code. Each such rank-metric code is lifted to a constant-dimension code. The union of these codes is our final constant-dimension code. In particular, the codes constructed recently by Koetter and Kschischang are a subset of our codes. The rank-metric codes used for this construction form a new class of rank-metric codes. We present a decoding algorithm to the constructed codes in the projective space. The efficiency of the decoding depends on the efficiency of the decoding for the constant-weight codes and the rank-metric codes. Finally, we use puncturing on our final constant-dimension codes to obtain large codes in the projective space which are not constant-dimension.**

***Index Terms*—Constant-dimension codes, constant-weight codes, Ferrers diagram, identifying vector, network coding, projective space codes, puncturing, rank-metric codes, reduced row echelon form.**

I. Introduction

THE *projective space* of order n over the finite field $\mathbb{F}_q$, denoted $\mathcal{P}_q(n)$, is the set of all subspaces of the vector space $\mathbb{F}_q^n$. Given a nonnegative integer $k \leq n$, the set of all subspaces of $\mathbb{F}_q^n$ that have dimension k is known as a *Grassmannian*, and usually denoted by $\mathcal{G}_q(n,k)$. Thus, $\mathcal{P}_q(n) = \bigcup_{0\leq k\leq n} \mathcal{G}_q(n,k)$. It turns out that the natural measure of distance in $\mathcal{P}_q(n)$ is given by

$$d_S(U,V) \stackrel{\text{def}}{=} \dim U + \dim V - 2\dim(U \cap V)$$

for all $U,V \in \mathcal{P}_q(n)$. It is well known (cf. [1], [2]) that the function above is a metric; thus, both $\mathcal{P}_q(n)$ and $\mathcal{G}_q(n,k)$ can be regarded as metric spaces. Given a metric space, one can define codes. We say that $\mathbb{C} \subseteq \mathcal{P}_q(n)$ is an $(n,M,d)_q$ *code in projective space* if $|\mathbb{C}| = M$ and $d_S(U,V) \geq d$ for all $U,V \in \mathbb{C}$. If an $(n,M,d)_q$ code $\mathbb{C}$ is contained in $\mathcal{G}_q(n,k)$ for some k, we say that $\mathbb{C}$ is an $(n,M,d,k)_q$ *constant-dimension code*. The $(n,M,d)_q$, respectively $(n,M,d,k)_q$, codes in projective space are akin to the familiar codes in the Hamming space, respectively (constant-weight) codes in the Johnson space, where the Hamming distance serves as the metric.

Koetter and Kschischang [2] showed that codes in $\mathcal{P}_q(n)$ are precisely what is needed for error-correction in random network coding: an $(n,M,d)_q$ code can correct any t packet errors (the packet can be overwritten), which is equivalent to t insertions and t deletions of dimensions in the transmitted subspace, and any ρ packet erasures introduced (adversarially) anywhere in the network as long as $4t + 2\rho < d$ (see [3] for more details). This is the motivation to explore error-correcting codes in $\mathcal{P}_q(n)$ [4]–[11]. Koetter and Kschischang [2] gave a Singleton-like upper bound on the size of such codes and a Reed–Solomon-like code which asymptotically attains this bound. Silva, Koetter, and Kschischang [3] showed how these codes can be described in terms of rank-metric codes [12], [13]. The related construction is our starting point in this paper. Our goal is to generalize this construction in the sense that the codes of Koetter and Kschischang will be subcodes of our codes and all our codes can be partitioned into subcodes, each one of them is a Koetter–Kschischang-like code. In the process, we describe some tools that can be useful to handle other coding problems in $\mathcal{P}_q(n)$. We also define a new type of rank-metric codes and construct optimal such codes. Our construction for constant-dimension codes and projective space codes uses a multilevel approach. This approach requires a few concepts which will be described in the following sections.

The rest of this paper is organized as follows. In Section II, we define the reduced row echelon form of a k-dimensional subspace and its Ferrers diagram. The reduced row echelon form is a standard way to describe a linear subspace. The Ferrers diagram is a standard way to describe a partition of a given positive integer into positive integers. It appears that the Ferrers diagrams can be used to partition the subspaces of $\mathcal{P}_q(n)$ into equivalence classes [14], [15]. In Section III, we present rank-metric codes which will be used for our multilevel construction. Our new method requires rank-metric codes in which some of the entries are forced to be zeros due to constraints given by the Ferrers diagram. We first present an upper bound on the size of such codes. We show how to construct some rank-metric codes which attain this bound. In Section IV, we describe in details the multilevel construction of the constant-dimension codes. We start by describing the connection of the rank-metric codes to constant-dimension codes. This connection was observed before in [2], [3], [6], [7]. We proceed to describe the multilevel construction. First, we select a binary constant-weight code $\boldsymbol{C}$. Each codeword of $\boldsymbol{C}$ defines a skeleton of a

Manuscript received July 30, 2008; revised February 02, 2009. Current version published June 24, 2009. This work was supported in part by the Israel Science Foundation (ISF), Jerusalem, Israel, under Grant 230/08. This work is part of N. Silberstein's Ph.D. dissertation performed at the Technion.

The authors are with the Department of Computer Science, Technion–Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: etzion@cs.technion.ac.il; natalys@cs.technion.ac.il).

Communicated by I. Dumer, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2009.2021376

basis for a subspace in reduced row echelon form. This skeleton contains a Ferrers diagram on which we design a rank-metric code. Each such rank-metric code is lifted to a constant-dimension code. The union of these codes is our final constant-dimension code. We discuss the parameters of these codes and also their decoding algorithms. In Section V, we generalize the well-known concept of a punctured code for a code in the projective space. Puncturing in the projective space is more complicated than its counterpart in the Hamming space. The punctured codes of our constant-dimension codes have larger size than the codes obtained by using the multilevel approach described in Section IV. We discuss the parameters of the punctured code and also its decoding algorithm. Finally, in Section VI, we summarize our results and present several problems for further research.

II. Reduced Echelon Form and Ferrers Diagram

In this section, we give the definitions for two structures which are useful in describing a subspace in $\mathcal{P}_q(n)$. The reduced row echelon form is a standard way to describe a linear subspace. The Ferrers diagram is a standard way to describe a partition of a given positive integer into positive integers.

A matrix is said to be in *row echelon form* if each nonzero row has more leading zeros than the previous row.

A $k \times n$ matrix with rank k is in *reduced row echelon form* if the following conditions are satisfied.

- 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.

A k-dimensional subspace X of $\mathbb{F}_q^n$ can be represented by a $k \times n$ *generator matrix* whose rows form a basis for X. We usually represent a codeword of a projective space code by such a matrix. There is exactly one such matrix in reduced row echelon form and it will be denoted by $E(X)$.

Example 1: We consider the three-dimensional subspace X of $\mathbb{F}_2^7$ with the following eight elements:

$$\begin{array}{ll}
1) & (0\ 0\ 0\ 0\ 0\ 0\ 0)\\
2) & (1\ 0\ 1\ 1\ 0\ 0\ 0)\\
3) & (1\ 0\ 0\ 1\ 1\ 0\ 1)\\
4) & (1\ 0\ 1\ 0\ 0\ 1\ 1)\\
5) & (0\ 0\ 1\ 0\ 1\ 0\ 1)\\
6) & (0\ 0\ 0\ 1\ 0\ 1\ 1)\\
7) & (0\ 0\ 1\ 1\ 1\ 1\ 0)\\
8) & (1\ 0\ 0\ 0\ 1\ 1\ 0).
\end{array}$$

The basis of X can be represented by a 3×7 matrix whose rows form a basis for the subspace. There are 168 different matrices for the 28 different basis. Many of these matrices are in row echelon form. One of them is

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Exactly one of these 168 matrices is in reduced row echelon form

$$E(X) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

A *Ferrers diagram* represents partitions as patterns of dots with the ith row having the same number of dots as the ith term in the partition [15]–[17]. 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 η we say that it is an $m \times \eta$ Ferrers diagram.

If we read the Ferrers diagram by columns we get another partition which is called the *conjugate* of the first one. If the partition forms an $m \times \eta$ Ferrers diagram then the conjugate partition forms an $\eta \times m$ Ferrers diagram.

Example 2: Assume we have the partition $6+5+5+3+2$ of 21. The 5×6 Ferrers diagram $\mathcal{F}$ of this partition is given by

$$\begin{array}{cccccc}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet\\
 & \bullet & \bullet & \bullet & \bullet & \bullet\\
 & \bullet & \bullet & \bullet & \bullet & \bullet\\
 & & & \bullet & \bullet & \bullet\\
 & & & & \bullet & \bullet.
\end{array}$$

The number of rows in $\mathcal{F}$ is five and the number of columns is six. The conjugate partition is the partition $5+5+4+3+3+1$ of 21 and its 6×5 Ferrers diagram is given by

$$\begin{array}{ccccc}
\bullet & \bullet & \bullet & \bullet & \bullet\\
\bullet & \bullet & \bullet & \bullet & \bullet\\
 & \bullet & \bullet & \bullet & \bullet\\
 & & \bullet & \bullet & \bullet\\
 & & \bullet & \bullet & \bullet\\
 & & & & \bullet.
\end{array}$$

Remark 1: Our definition of Ferrers diagram is slightly different from the usual definition [15]–[17], where the dots in each row are shifted to the left of the diagram.

Each k-dimensional subspace X of $\mathbb{F}_q^n$ has an *identifying vector* $v(X)$. $v(X)$ is a binary vector of length n and weight k, where the *ones* in $v(X)$ are in the positions (columns) where $E(X)$ has the leading *ones* (of the rows).

Example 3: Consider the three-dimensional subspace X of Example 1. Its identifying vector is $v(X) = 1011000$.

Remark 2: We can consider an identifying vector $v(X)$ for some k-dimensional subspace X as a characteristic vector of a k-subset. This coincides with the definition of rank- and order-preserving map ϕ from $\mathcal{G}_q(n,k)$ onto the lattice of subsets of an n-set, given by Knuth [14] and discussed by Milne [18].

The following lemma is easily observed.

Lemma 1: Let X be a k-dimensional linear subspace of $\mathbb{F}_q^n$, $v(X)$ its identifying vector, and $i_1, i_2, \ldots, i_k$ the positions in which $v(X)$ has *ones*. Then for each nonzero element $u \in X$, the leftmost *one* in u is in position i_j for some $1 \leq j \leq k$.

Proof: Clearly, for each $j, 1 \leq j \leq k$, there exists an element $u_j \in X$ whose leftmost *one* is in position i_j. Moreover, $u_1, u_2, \ldots, u_k$ are linearly independent. Assume the contrary, that there exists an element $u \in X$ whose leftmost *one* is in position $\ell \notin \{i_1, \ldots, i_k\}$. This implies that $u, u_1, u_2, \ldots, u_k$ are linearly independent and the dimension of X is at least $k+1$, a contradiction. □

The following result will play an important role in the proof that our constructions for error-correcting codes in the projective space have the desired minimum distance.

Lemma 2: If X and Y are two subspaces of $\mathcal{P}_q(n)$ with identifying vectors $v(X)$ and $v(Y)$, respectively, then $d_S(X,Y) \geq d_H(v(X), v(Y))$, where $d_H(u,v)$ denotes the Hamming distance between u and v.

Proof: Let $i_1, \ldots, i_r$ be the positions in which $v(X)$ has *ones* and $v(Y)$ has *zeros* and $j_1, \ldots, j_s$ be the positions in which $v(Y)$ has *ones* and $v(X)$ has *zeros*. Clearly, $r + s = d_H(v(X), v(Y))$. Therefore, by Lemma 1, X contains r linearly independent vectors $u_1, \ldots, u_r$ which are not contained in Y. Similarly, Y contains s linearly independent vectors which are not contained in X. Thus, $d_S(X,Y) \geq r + s = d_H(v(X), v(Y))$. □

The *echelon Ferrers form* of a vector v of length n and weight k, $EF(v)$, is the $k \times n$ matrix in reduced row echelon form with leading entries (of rows) in the columns indexed by the nonzero entries of v and "$\bullet$" in all entries which do not have terminals *zeros* or *ones*. A "$\bullet$" will be called in the sequel a *dot*. This notation is also given in [15], [17]. The dots of this matrix form the Ferrers diagram of $EF(v)$. If we substitute elements of $\mathbb{F}_q$ in the dots of $EF(v)$ we obtain a k-dimensional subspace X of $\mathcal{P}_q(n)$. $EF(v)$ will be called also the echelon Ferrers form of X.

Example 4: For the vector $v = 1001001$, the echelon Ferrers form $EF(v)$ is the following 3×7 matrix:

$$EF(v) = \begin{bmatrix} 1 & \bullet & \bullet & 0 & \bullet & \bullet & 0 \\ 0 & 0 & 0 & 1 & \bullet & \bullet & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

$EF(v)$ has the following 2×4 Ferrers diagram:

$$\mathcal{F} = \begin{matrix} \bullet & \bullet & \bullet & \bullet \\ & & \bullet & \bullet \end{matrix}.$$

Each binary word v of length n and weight k corresponds to a unique $k \times n$ matrix in an echelon Ferrers form. There are a total of $\binom{n}{k}$ binary vectors of length n and weight k and hence there are $\binom{n}{k}$ different $k \times n$ matrices in echelon Ferrers form.

III. Ferrers Diagram Rank-Metric Codes

In this section, we start by defining the rank-metric codes. These codes are strongly connected to constant-dimension codes by a lifting construction described by Silva, Kschischang, and Koetter [3]. We define a new concept which is a Ferrers diagram rank-metric code. Ferrers diagram rank-metric codes will be the main building blocks of our projective space codes. These codes present some questions which are of interest in themselves.

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

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

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 ϱ of $\mathbb{F}_q^{m \times \eta}$, and for each two distinct codewords A and B we have that $d_R(A,B) \geq \delta$. Rank-metric codes were well studied [12], [13], [19]. It was proved (see [13]) that for an $[m \times \eta, \varrho, \delta]$ rank-metric code $\mathcal{C}$ we have $\varrho \leq \min\{m(\eta - \delta + 1), \eta(m - \delta + 1)\}$. 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 are $m \times \eta$ matrices in which all entries not in $\mathcal{F}$ are *zeros*, it forms a rank-metric code with dimension ϱ, and minimum rank distance δ. Let $\dim(\mathcal{F}, \delta)$ be the largest possible dimension of an $[\mathcal{F}, \varrho, \delta]$ code.

Theorem 1: For a given $i, 0 \leq i \leq \delta - 1$, if ν_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 of $\dim(\mathcal{F}, \delta)$.

Proof: For a given $i, 0 \leq i \leq \delta - 1$, let $\mathcal{A}_i$ be the set of the ν_i positions of $\mathcal{F}$ which are not contained in the first i rows and are not contained in the rightmost $\delta - 1 - i$ columns. Assume the contrary that there exists an $[\mathcal{F}, \nu_i + 1, \delta]$ code $\mathcal{C}$. Let $\mathcal{B} = \{B_1, B_2, \ldots, B_{\nu_i + 1}\}$ be a set of $\nu_i + 1$ linearly independent codewords in $\mathcal{C}$. Since the number of linearly independent codewords is greater than the number of entries in $\mathcal{A}_i$, there exists a nontrivial linear combination $Y = \sum_{j=1}^{\nu_i+1} \alpha_j B_j$ for which the ν_i entries of $\mathcal{A}_i$ are equal *zeros*. Y is not the all-zeros codeword since the B_i's are linearly independent. $\mathcal{F}$ has outside $\mathcal{A}_i$ exactly i rows and $\delta - i - 1$ columns. These i rows can contribute at most i to the rank of Y and the $\delta - i - 1$ columns can contribute at most $\delta - i - 1$ to the rank of Y. Therefore, Y is a nonzero codeword with rank less than δ, a contradiction.

Hence, an upper bound on $\dim(\mathcal{F}, \delta)$ is ν_i for each $0 \leq i \leq \delta - 1$. Thus, an upper bound on the dimension $\dim(\mathcal{F}, \delta)$ is $\min_i\{\nu_i\}$. □

Conjecture 1: The upper bound of Theorem 1 is attainable for any given set of parameters $q, \mathcal{F}$, and δ.

If we use $i = 0$ or $i = \delta - 1$ in Theorem 1 we obtain the following result.

Corollary 1: An upper bound on $\dim(\mathcal{F}, \delta)$ is the minimum number of dots that can be removed from $\mathcal{F}$ such that the diagram remains with at most $\delta - 1$ rows of dots or at most $\delta - 1$ columns of dots.

Remark 3: $[m \times \eta, \varrho, \delta]$ MRD codes are one class of Ferrers diagram rank-metric codes which attain the bound of Corollary 1 with equality. In this case, the Ferrers diagram has $m \cdot \eta$ dots.

Example 5: Consider the following Ferrers diagram:

$$\mathcal{F} = \begin{array}{cccc} \bullet & \bullet & \bullet & \bullet \\ & & \bullet & \bullet \\ & & & \bullet \\ & & & \bullet \end{array}$$

and $\delta = 3$. By Corollary 1, we have an upper bound: $\dim(\mathcal{F}, 3) \leq 2$. But, if we use $i = 1$ in Theorem 1 then we have a better upper bound: $\dim(\mathcal{F}, 3) \leq 1$. This upper bound is attained with the following generator matrix of an $[\mathcal{F}, 1, 3]$ rank-metric code:

$$\begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 0 & 0 & \mathbf{1} & \mathbf{0} \\ 0 & 0 & 0 & \mathbf{0} \\ 0 & 0 & 0 & \mathbf{1} \end{pmatrix}.$$

When the bound of Theorem 1 is attained? We start with a construction of Ferrers diagram rank-metric codes which attain the bound of Corollary 1. Assume we have an $m \times \eta$, $m = \eta + \varepsilon$, $\varepsilon \geq 0$, Ferrers diagram $\mathcal{F}$ and that the minimum in the bound of Corollary 1 is obtained by removing all the dots from the $\eta - \delta + 1$ leftmost columns of $\mathcal{F}$. Hence, only the dots in the $\delta - 1$ rightmost columns will remain. We further assume that each of the $\delta - 1$ rightmost columns of $\mathcal{F}$ have m dots. The construction which follows is based on the construction of MRD q-cyclic rank-metric codes given by Gabidulin [12].

A code $\mathcal{C}$ of length m over $\mathbb{F}_{q^m}$ is called a *q-cyclic code* if $(c_0, c_1, \ldots, c_{m-1}) \in \mathcal{C}$ implies that $(c_{m-1}^q, c_0^q, \ldots, c_{m-2}^q) \in \mathcal{C}$.

For a construction of $[m \times m, \varrho, \delta]$ rank-metric codes, we use an isomorphism between the field with q^m elements, $\mathbb{F}_{q^m}$, and the set of all m-tuples over $\mathbb{F}_q$, $\mathbb{F}_q^m$. We use the obvious isomorphism by the representation of an element α in the extension field $\mathbb{F}_{q^m}$ as $\alpha = (\alpha_1, \ldots, \alpha_m)$, where α_i is an element in the ground field $\mathbb{F}_q$. Usually, we will leave to the reader to realize when the isomorphism is used as this will be easily verified from the context.

A codeword c in an $[m \times m, \varrho, \delta]$ rank-metric code $\mathcal{C}$, can be represented by a vector $c = (c_0, c_1, \ldots, c_{m-1})$, where $c_i \in \mathbb{F}_{q^m}$ and the generator matrix G of $\mathcal{C}$ is a $K \times m$ matrix, $\varrho = mK$. It was proved by Gabidulin [12] that if $\mathcal{C}$ is an MRD q-cyclic code then the generator polynomial of $\mathcal{C}$ is the linearized polynomial $G(x) = \sum_{i=0}^{m-K} g_i x^{q^i}$, where $g_i \in \mathbb{F}_{q^m}$, $g_{m-K} = 1$, $m = K + \delta - 1$, and its generator matrix G has the form

$$\begin{pmatrix} g_0 & g_1 & \cdots & g_{m-K-1} & 1 & 0 & \cdots & \cdots \\ 0 & g_0^q & g_1^q & \cdots & g_{m-K-1}^q & 1 & \cdots & \cdots \\ 0 & 0 & g_0^{q^2} & \cdots & \cdots & g_{m-K-1}^{q^2} & 1 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & g_{m-K-1}^{q^{K-1}} & 1 \end{pmatrix}.$$

Hence, a codeword $c \in \mathcal{C}$, $c \in (\mathbb{F}_{q^m})^m$, derived from the information word $(a_0, a_1, \ldots, a_{K-1})$, where $a_i \in \mathbb{F}_{q^m}$, i.e., $c = (a_0, a_1, \ldots, a_{K-1})G$, has the form

$$c = \left(a_0 g_0, a_0 g_1 + a_1 g_0^q, \ldots, a_{K-2} + a_{K-1} g_{m-K-1}^{q^{K-1}}, a_{K-1}\right).$$

We define an $[m \times \eta, m(\eta - \delta + 1), \delta]$ rank-metric code $\mathcal{C}'$, $m = \eta + \varepsilon$, derived from $\mathcal{C}$ as follows:

$$\mathcal{C}' = \{(c_0, c_1, \ldots, c_{\eta-1}) : (0, \ldots, 0, c_0, c_1, \ldots, c_{\eta-1}) \in \mathcal{C}\}.$$

Remark 4: $\mathcal{C}'$ is also an MRD code.

We construct an $[\mathcal{F}, \ell, \delta]$ Ferrers diagram rank-metric code $\mathcal{C}_{\mathcal{F}} \subseteq \mathcal{C}'$, where $\mathcal{F}$ is an $m \times \eta$ Ferrers diagram. Let γ_i, $1 \leq i \leq \eta$, be the number of dots in column i of $\mathcal{F}$, where the columns are indexed from left to right. A codeword of $\mathcal{C}_{\mathcal{F}}$ is derived from a codeword of $c \in \mathcal{C}$ by satisfying a set of m equations implied by

$$\left(a_0 g_0, a_0 g_1 + a_1 g_0^q, \ldots, a_{K-2} + a_{K-1} g_{m-K-1}^{q^{K-1}}, a_{K-1}\right) = \left(\overbrace{\begin{matrix} 0 & & 0 \\ \vdots & \cdots & \vdots \\ 0 & & 0 \end{matrix}}^{\varepsilon} \; f_1 \ldots f_{K-\varepsilon} \; \overbrace{\begin{matrix} \bullet & & \bullet \\ \vdots & \cdots & \vdots \\ \bullet & & \bullet \end{matrix}}^{\delta-1} \right) \quad (1)$$

where $f_i = (\underbrace{\bullet \cdots \bullet}_{\gamma_i} \underbrace{0 \cdots 0}_{m-\gamma_i})^T$ is a column vector of length m, $1 \leq i \leq K - \varepsilon$, and u^T denotes the transpose of the vector u. It is easy to verify that $\mathcal{C}_{\mathcal{F}}$ is a linear code.

By (1) we have a system of $m = K + \delta - 1$ equations with K variables, $a_0, a_1, \ldots, a_{K-1}$. The first ε equations imply that $a_i = 0$ for $0 \leq i \leq \varepsilon - 1$. The next $K - \varepsilon = \eta - \delta + 1$ equations determine the values of the a_i's, $\varepsilon \leq i \leq K - 1$, as follows. From the next equation

$$a_\varepsilon g_0^{q^\varepsilon} = (\underbrace{\bullet \cdots \bullet}_{\gamma_1} \underbrace{00 \ldots 0}_{m-\gamma_1})^T$$

(this is the next equation after we substitute $a_i = 0$ for $0 \leq i \leq \varepsilon - 1$), we have that a_ε has q^{γ_1} solutions in $\mathbb{F}_{q^m}$, where each element of $\mathbb{F}_{q^m}$ is represented as an m-tuple over $\mathbb{F}_q$. Given a solution of a_ε, the next equation

$$a_\varepsilon g_0^{q^\varepsilon} + a_{\varepsilon+1} g_1^{q^{\varepsilon+1}} = (\underbrace{\bullet \cdots \bullet}_{\gamma_2} \underbrace{00 \ldots 0}_{m-\gamma_2})^T$$

has q^{γ_2} solutions for $a_{\varepsilon+1}$. Therefore, we have that $a_0, a_1, \ldots, a_{K-1}$ have $q^{\sum_{i=1}^{K-\varepsilon} \gamma_i}$ solutions and hence the dimension of $\mathcal{C}_{\mathcal{F}}$ is $\sum_{i=1}^{K-\varepsilon} \gamma_i$ over $\mathbb{F}_q$. Note, that since each of the $\delta - 1$ rightmost columns of $\mathcal{F}$ have m dots, i.e., $\gamma_i = m$, $K - \varepsilon + 1 \leq i \leq \eta$ (no *zeros* in the related equations), it follows that any set of values for the a_i's cannot cause any contradiction in the last $\delta - 1$ equations. Also, since the values of the K variables $a_0, a_1, \ldots, a_{K-1}$ are determined for the last $\delta - 1$ equations, the values for the related $(\delta - 1)m$ dots are determined. Hence, they do not contribute to the number of solutions for the set of m equations. Thus, we have the following result.

Theorem 2: Let $\mathcal{F}$ be an $m \times \eta$, $m \geq \eta$, Ferrers diagram. Assume that each one of the rightmost $\delta - 1$ columns of $\mathcal{F}$ has m dots, and the ith column from the left of $\mathcal{F}$ has γ_i dots.

Then $\mathcal{C}_{\mathcal{F}}$ is an $[\mathcal{F}, \sum_{i=1}^{\eta-\delta+1} \gamma_i, \delta]$ code which attains the bound of Corollary 1.

Remark 5: For any solution of $a_0, a_1, \ldots, a_{K-1}$ we have that $(a_0, a_1, \ldots, a_{K-1})G = (0, \ldots, 0, c_0, c_1, \ldots, c_{\eta-1}) \in \mathcal{C}$ and $(c_0, c_1, \ldots, c_{\eta-1}) \in \mathcal{C}_{\mathcal{F}}$.

Remark 6: For any $[m \times \eta, m(\eta-\delta+1), \delta]$ rank-metric code $\mathcal{C}'$, the codewords which have *zeros* in all the entries which are not contained in $\mathcal{F}$ form an $[\mathcal{F}, \sum_{i=1}^{\eta-\delta+1} \gamma_i, \delta]$ code. Thus, we can use also any MRD codes, e.g., the codes described in [13], to obtain a proof for Theorem 2.

Remark 7: Since $\mathcal{C}_{\mathcal{F}}$ is a subcode of an MRD code then we can use the decoding algorithm of the MRD code for the decoding of our code. Also note, that if $\mathcal{F}$ is an $m \times \eta$, $m < \eta$, Ferrers diagram then we apply our construction for the $\eta \times m$ Ferrers diagram of the conjugate partition.

When $\delta = 1$, the bounds and the construction are trivial. If $\delta = 2$, then by definition the rightmost column and the top row of an $m \times \eta$ Ferrers diagram always has m dots and η dots, respectively. It implies that the bound of Theorem 1 is always attained with the construction if $\delta = 2$. This is the most interesting case since in this case the improvement of our constant-dimension codes compared to the codes in [2], [3] is the most impressive (see Section IV-C). If $\delta > 2$, the improvement is relatively small, but we will consider this case as it is of interest also from a theoretical point of view. Some constructions can be given based on the main construction and other basic constructions. We will give two simple examples for $\delta = 3$.

Example 6: Consider the following Ferrers diagram:

$$\mathcal{F} = \begin{array}{cccc} \bullet & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \\ & & \bullet & \bullet \\ & & & \bullet \end{array}.$$

The upper bound on $\dim(\mathcal{F}, 3)$ is 3. It is attained with the following basis with three 4×4 matrices.

$$\begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ 0 & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 0 & 0 & \mathbf{0} & \mathbf{0} \\ 0 & 0 & 0 & \mathbf{1} \end{pmatrix}, \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ 0 & 0 & \mathbf{1} & \mathbf{0} \\ 0 & 0 & 0 & \mathbf{0} \end{pmatrix}, \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ 0 & 0 & \mathbf{0} & \mathbf{1} \\ 0 & 0 & 0 & \mathbf{1} \end{pmatrix}.$$

Example 7: Consider the following Ferrers diagram

$$\mathcal{F} = \begin{array}{cccc} \bullet & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \\ & & & \bullet \end{array}.$$

The upper bound on $\dim(\mathcal{F}, 3)$ is 4. It is attained with the basis consisting of four 4×4 matrices, from which three are from Example 6 and the last one is

$$\begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 0 & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ 0 & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ 0 & 0 & 0 & \mathbf{0} \end{pmatrix}.$$

As for more constructions, some can be easily generated by the interested reader, but whether the upper bound of Theorem 1 can be attained for all parameters remains an open problem.

IV. Error-Correcting Constant-Dimension Codes

In this section, we will describe our multilevel construction. The construction will be applied to obtain error-correcting constant-dimension codes, but it can be adapted to construct error-correcting projective space codes without any modification. This will be discussed in the next section. We will also consider the parameters and decoding algorithms for our codes. Without loss of generality, we will assume that $k \leq n-k$. This assumption can be made as a consequence of the following lemma [4], [11].

Lemma 3: If $\mathbb{C}$ is an $(n, M, 2\delta, k)_q$ constant-dimension code then $\mathbb{C}^{\perp} = \{X^{\perp} : X \in \mathbb{C}\}$, where $X^{\perp}$ is the orthogonal subspace of X, is an $(n, M, 2\delta, n-k)_q$ constant-dimension code.

A. Lifted Codes

Koetter and Kschischang [2] gave a construction for constant-dimension Reed–Solomon-like codes. This construction can be presented more clearly in terms of rank-metric codes [3]. Given a $[k \times (n-k), \varrho, \delta]$ rank-metric code $\mathcal{C}$ we form an $(n, q^{\varrho}, 2\delta, k)_q$ constant-dimension code $\mathbb{C}$ by *lifting* $\mathcal{C}$, i.e., $\mathbb{C} = \{[I_k A] : A \in \mathcal{C}\}$, where I_k is the $k \times k$ identity matrix [3]. We will call the code $\mathbb{C}$ the *lifted code* of $\mathcal{C}$. Usually $\mathbb{C}$ is not maximal and it can be extended. This extension requires to design rank-metric codes, where the shape of a codeword is a Ferrers diagram rather than a $k \times (n-k)$ matrix. We would like to use the largest possible Ferrers diagram rank-metric codes. In the appropriate cases, e.g., when $\delta = 2$, we will use the codes constructed in Section III for this purpose.

Assume we are given an echelon Ferrers form $EF(v)$ of a binary vector v, of length n and weight k, with a Ferrers diagram $\mathcal{F}$ and a Ferrers diagram rank-metric code $\mathcal{C}_{\mathcal{F}}$. $\mathcal{C}_{\mathcal{F}}$ is lifted to a constant-dimension code $\mathbb{C}_v$ by substituting each codeword $A \in \mathcal{C}_{\mathcal{F}}$ in the columns of $EF(v)$ which correspond to the *zeros* of v. Note, that depending on $\mathcal{F}$ it might implies conjugating $\mathcal{F}$ first. Unless v starts with a *one* and ends with a *zero* (the cases in which $\mathcal{F}$ is a $k \times (n-k)$ Ferrers diagram) we also need to expand the matrices of the Ferrers diagram rank-metric code to $k \times (n-k)$ matrices (which will be lifted), where $\mathcal{F}$ is in their upper right corner (and the new entries are *zeros*). As an immediate consequence from [3] we have the following.

Lemma 4: If $\mathcal{C}_{\mathcal{F}}$ is an $[\mathcal{F}, \varrho, \delta]$ Ferrers diagram rank-metric code then its lifted code $\mathbb{C}_v$, related to an $k \times n$ echelon Ferrers form $EF(v)$, is an $(n, q^{\varrho}, 2\delta, k)_q$ constant-dimension code.

Example 8: For the word $v = 1110000$, its echelon Ferrers form

$$EF(v) = \begin{bmatrix} 1 & 0 & 0 & \bullet & \bullet & \bullet & \bullet \\ 0 & 1 & 0 & \bullet & \bullet & \bullet & \bullet \\ 0 & 0 & 1 & \bullet & \bullet & \bullet & \bullet \end{bmatrix}$$

the 3×4 matrix

$$\begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix}$$

is lifted to the three-dimensional subspace with the 3×7 generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 0 & 1 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ 0 & 0 & 1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}.$$

For the word $v = 1001001$, its echelon Ferrers form

$$EF(v) = \begin{bmatrix} 1 & \bullet & \bullet & 0 & \bullet & \bullet & 0 \\ 0 & 0 & 0 & 1 & \bullet & \bullet & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

the 2×4 matrix

$$\begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 0 & 0 & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

is lifted to the three-dimensional subspace with the 3×7 generator matrix

$$\begin{bmatrix} 1 & \mathbf{1} & \mathbf{0} & 0 & \mathbf{1} & \mathbf{0} & 0 \\ 0 & 0 & 0 & 1 & \mathbf{0} & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The code described in [3] is the same as the code described in Section III, where the identifying vector is $(1\ldots10\ldots0)$. If our lifted codes are the codes described in Section III then the same decoding algorithm can be applied. Therefore, the decoding in [3] for the corresponding constant-dimension code can be applied directly to each of our lifted constant-dimension codes in this case, e.g., it can always be applied when $\delta = 2$. It would be worthwhile to permute the coordinates in a way that the identity matrix I_k will appear in the first k columns, from the left, of the reduced row echelon form, and $\mathcal{F}$ will appear in the upper right corner of the $k \times n$ matrix. The reason is that the decoding of [3] is described on such matrices.

B. Multilevel Construction

Assume we want to construct an $(n, M, 2\delta, k)_q$ constant-dimension code $\mathbb{C}$.

The first step in the construction is to choose a binary constant-weight code $\boldsymbol{C}$ of length n, weight k, and minimum distance 2δ. This code will be called the *skeleton code*. Any constant-weight code can be chosen for this purpose, but different skeleton codes will result in different constant-dimension codes with usually different sizes. The best choice for the skeleton code $\boldsymbol{C}$ will be discussed in the next subsection. The next three steps are performed for each codeword $c \in \boldsymbol{C}$.

The second step is to construct the echelon Ferrers form $EF(c)$.

The third step is to construct an $[\mathcal{F}, \varrho, \delta]$ Ferrers diagram rank-metric code $\mathcal{C}_{\mathcal{F}}$ for the Ferrers diagram $\mathcal{F}$ of $EF(c)$. If possible we will construct a code as described in Section III.

The fourth step is to lift $\mathcal{C}_{\mathcal{F}}$ to a constant-dimension code $\mathbb{C}_c$, for which the echelon Ferrers form of $X \in \mathbb{C}_c$ is $EF(c)$.

Finally

$$\mathbb{C} = \bigcup_{c \in \boldsymbol{C}} \mathbb{C}_c.$$

As an immediate consequence of Lemmas 2 and 4, we have the following theorem.

Theorem 3: $\mathbb{C}$ is an $(n, M, 2\delta, k)_q$ constant-dimension code, where $M = \sum_{c \in \boldsymbol{C}} |\mathbb{C}_c|$.

Example 9: Let $n = 6, k = 3$, and

$$\boldsymbol{C} = \{111000, 100110, 010101, 001011\}$$

a constant-weight code of length 6, weight 3, and minimum Hamming distance 4. The echelon Ferrers forms of these four codewords are

$$EF(111000) = \begin{bmatrix} 1 & 0 & 0 & \bullet & \bullet & \bullet \\ 0 & 1 & 0 & \bullet & \bullet & \bullet \\ 0 & 0 & 1 & \bullet & \bullet & \bullet \end{bmatrix}$$
$$EF(100110) = \begin{bmatrix} 1 & \bullet & \bullet & 0 & 0 & \bullet \\ 0 & 0 & 0 & 1 & 0 & \bullet \\ 0 & 0 & 0 & 0 & 1 & \bullet \end{bmatrix}$$
$$EF(010101) = \begin{bmatrix} 0 & 1 & \bullet & 0 & \bullet & 0 \\ 0 & 0 & 0 & 1 & \bullet & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$
$$EF(001011) = \begin{bmatrix} 0 & 0 & 1 & \bullet & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

By Theorem 2, the Ferrers diagrams of these four echelon Ferrers forms yield Ferrers diagram rank-metric codes of sizes $64, 4, 2$, and 1, respectively. Hence, we obtain a $(6, 71, 4, 3)_2$ constant-dimension code $\mathbb{C}$.

Remark 8: A $(6, 74, 4, 3)_2$ code was obtained by computer search [8]. Similarly, we obtain a $(7, 289, 4, 3)_2$ code. A $(7, 304, 4, 3)_2$ code was obtained by computer search [8].

Example 10: Let $\boldsymbol{C}$ be the codewords of weight 4 in the $[8, 4, 4]$ extended Hamming code with the following parity-check matrix:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

$\boldsymbol{C}$ has 14 codewords with weight 4. Each one of these codewords is considered as an identifying vector for the echelon Ferrers forms from which we construct the final $(8, 4573, 4, 4)_2$ code $\mathbb{C}$. The 14 codewords of $\boldsymbol{C}$ and their contribution for the final code $\mathbb{C}$ are given in the following table. The codewords are taken in lexicographic order.

	$c \in \mathcal{C}$	size of $\mathbb{C}_c$
1	11110000	4096
2	11001100	256
3	11000011	16
4	10101010	64
5	10100101	16
6	10011001	16
7	10010110	16
8	01101001	32
9	01100110	16
10	01011010	16
11	01010101	8
12	00111100	16
13	00110011	4
14	00001111	1

C. Code Parameters

We now want to discuss the size of our constant-dimension code, the required choice for the skeleton code $\boldsymbol{C}$, and compare the size of our codes with the size of the codes constructed in [2], [3].

The size of the final constant-dimension code $\mathbb{C}$ depends on the choice of the skeleton code $\boldsymbol{C}$. The identifying vector with the largest size of corresponding rank-metric code is $\underbrace{1\cdots1}_{k}\underbrace{0\cdots0}_{n-k}$. The corresponding $[k \times (n-k), \ell, \delta]$ rank-metric code has dimension $\ell = (n-k)(k-\delta+1)$ and hence it contributes $q^{(n-k)(k-\delta+1)}$ k-dimensional subspaces to our final code $\mathbb{C}$. These subspaces form the codes in [2], [3]. The next identifying vector which contributes the most number of subspaces to $\mathbb{C}$ is

$$\underbrace{11\ldots1}_{k-\delta}\underbrace{0\cdots0}_{\delta}\underbrace{11\ldots1}_{\delta}\underbrace{000\ldots00}_{n-k-\delta}.$$

The number of subspaces it contributes depends on the bounds presented in Section III. The rest of the code $\mathbb{C}$ usually has fewer codewords than those contributed by these two. Therefore, the improvement in the size of the code compared to the code of [2] is not dramatic. But, for most parameters, our codes are larger than the best known codes. In some cases, e.g., when $\delta = k$, our codes are as good as the best known codes (see [4]) and suggest an alternative construction. When $k = 3$, $\delta = 4$, and reasonably small n, the cyclic codes constructed in [4], [8] are larger.

Two possible alternatives for the best choice for the skeleton code $\boldsymbol{C}$ might be of special interest. The first one is for $k = 4$ and n which is a power of two. We conjecture that the best skeleton code is constructed from the codewords with weight 4 of the extended Hamming code for which the columns of the parity-check matrix are given in lexicographic order. We generalize this choice of codewords from the Hamming code by choosing a constant-weight lexicode [20]. Such a code is constructed as follows. All vectors of length n and weight k are listed in lexicographic order. The code $\boldsymbol{C}$ is generated by adding to the code $\boldsymbol{C}$ one codeword at a time. At each stage, the first codeword of the list, that does not violate the distance constraint with the other codewords of $\boldsymbol{C}$, is joined to $\boldsymbol{C}$. Lexicodes are not necessarily the best constant-weight codes. For example, size of the largest constant-weight code of length 10 and weight 4 is 30, while the lexicode with the same parameters has size 18. But, the constant-dimension code derived from the lexicode is larger than any constant-dimension code derived from any related code of size 30.

The following table summarized the sizes of some of our codes compared to previous known codes. In all these codes we have started with a constant-weight lexicode in the first step of the construction.

q	$d_S(\mathbb{C})$	n	k	code size[2]	size of our code
2	4	9	4	2^{15}	2^{15}+4177
2	4	10	5	2^{20}	2^{20}+118751
2	4	12	4	2^{24}	2^{24}+2290845
2	6	10	5	2^{15}	2^{15}+73
2	6	13	4	2^{18}	2^{18}+4357
2	8	21	5	2^{32}	2^{32}+16844809
3	4	7	3	3^{8}	3^{8}+124
3	4	8	4	3^{12}	3^{12}+8137
4	4	7	3	4^{8}	4^{8}+345
4	4	8	4	4^{12}	4^{12}+72529

D. Decoding

The decoding of our codes is quite straightforward and it mainly consists of known decoding algorithms. As we used a multilevel coding we will also need a multilevel decoding. In the first step, we will use a decoding for our skeleton code and in the second step, we will use a decoding for the rank-metric codes.

Assume the received word was a k-dimensional subspace Y. We start by generating its reduced row echelon form $E(Y)$. Given $E(Y)$ it is straightforward to find the identifying vector $v(Y)$. Now, we use the decoding algorithm for the constant-weight code to find the identifying vector $v(X)$ of the submitted k-dimensional subspace X. If no more than $\delta-1$ errors occurred then we will find the correct identifying vector. This claim is an immediate consequence of Lemma 2.

In the second step of the decoding, we are given the received subspace Y, its identifying vector $v(Y)$, and the identifying vector $v(X)$ of the submitted subspace X. We consider the echelon Ferrers form $EF(v(X))$, its Ferrers diagram $\mathcal{F}$, and the $[\mathcal{F}, \varrho, \delta]$ Ferrers diagram rank-metric code associated with it. We can permute the columns of $EF(v(X))$, and use the same permutation on Y, in a way that the identity matrix I_k will be in the left side. Now, we can use the decoding of the specific rank-metric code. If our rank-metric codes are those constructed in Section III then we can use the decoding as described in [3]. It is clear now that the efficiency of our decoding depends on the efficiency of the decoding of our skeleton code and the efficiency of the decoding of our rank-metric codes. If the rank-metric codes are MRD codes then they can be decoded efficiently [12], [13]. The same is true if the Ferrers diagram metric codes are those constructed in Section III as they are subcodes of MRD codes and the decoding algorithm of the related MRD code applied to them as well.

There are some alternative ways for our decoding, some of which improve on the complexity of the decoding. For example, we can make use of the fact that most of the code is derived from two identifying vectors or that most of the rank-metric codes are of relatively small size. One such case can be when all the identity matrices of the echelon Ferrers forms are in consecutive columns of the codeword (see [10]). We will not discuss it as the related codes hardly improve on the codes in [2], [3].

Finally, if we allow to receive a word which is an ℓ-dimensional subspace Y, $k-\delta+1 \leq \ell \leq k+\delta-1$, then the same procedure will work as long as $d_S(X,Y) \leq \delta - 1$. This is a consequence of the fact that the decoding algorithm of [3] does not restrict the dimension of the received word.

V. Error-Correcting Projective Space Codes

In this section, our goal will be to construct large codes in $\mathcal{P}_q(n)$ which are not constant-dimension codes. We first note that the multilevel coding described in Section IV can be used to obtain a code in $\mathcal{P}_q(n)$. The only difference is that we should start in the first step with a general binary code of length n in the Hamming space as a skeleton code. The first question which will arise in this context is whether the method is as good as for constructing codes in $\mathcal{G}_q(n,k)$. The answer can be inferred from the following example.

Example 11: Let $n=7$ and $d=3$, and consider the $[7,4,3]$ Hamming code with the parity-check matrix

$$\begin{bmatrix} 0&0&0&1&1&1&1\\ 0&1&1&0&1&1&0\\ 1&0&1&1&0&1&0 \end{bmatrix}.$$

By using the multilevel coding with this Hamming code we obtain a code with minimum distance 3 and size 394 in $\mathcal{P}_2(7)$.

As we shall see in the sequel, this code is much smaller than a code that will be obtained by puncturing. We have also generated codes in the projective space based on the multilevel construction, where the skeleton code is a lexicode. The constructed codes appear to be much smaller than the codes obtained by puncturing. Puncturing of a code $\mathbb{C}$ (or union of codes with different dimensions and the required minimum distance) obtained in Section IV results in a projective space code $\mathbb{C}'$. If the minimum distance of $\mathbb{C}$ is 2δ then the minimum distance of $\mathbb{C}'$ is $2\delta-1$. $\mathbb{C}'$ has a similar structure to a code obtained by the multilevel construction (similar structure in the sense that the identifying vectors of the codewords can form a skeleton code). But the artificial "skeleton code" can be partitioned into pair of codewords with Hamming distance one, while the distance between two codewords from different pairs is at least $2\delta-1$. This property yields larger codes by puncturing, sometimes with double size, compared to codes obtained by the multilevel construction.

A. Punctured Codes

Puncturing and punctured codes are well known in the Hamming space. An (n,M,d) code in the Hamming space is a code of length n, minimum Hamming distance d, and M codewords. Let $\boldsymbol{C}$ be an (n,M,d) code in the Hamming space. Its punctured code $\boldsymbol{C}'$ is obtained by deleting one coordinate of $\boldsymbol{C}$. Hence, there are n punctured codes and each one is an $(n-1,M,d-1)$ code. In the projective space there is a very large number of punctured codes for a given code $\mathbb{C}$ and in contrary to the Hamming space the sizes of these codes are usually different.

Let X be an ℓ-dimensional subspace of $\mathbb{F}_q^n$ such that the unity vector with a *one* in the ith coordinate is not an element in X. The *i-coordinate puncturing* of X, $\Delta_i(X)$, is defined as the ℓ-dimensional subspace of $\mathbb{F}_q^{n-1}$ obtained from X by deleting coordinate i from each vector in X. This puncturing of a subspace is akin to puncturing a code $\boldsymbol{C}$ in the Hamming space by the ith coordinate.

Let $\mathbb{C}$ be a code in $\mathcal{P}_q(n)$ and let Q be an $(n-1)$-dimensional subspace of $\mathbb{F}_q^n$. Let $E(Q)$ be the $(n-1)\times n$ generator matrix of Q (in reduced row echelon form) and let τ be the position of the unique *zero* in $v(Q)$. Let $v \in \mathbb{F}_q^n$ be an element such that $v \notin Q$. We define the *punctured* code

$$\mathbb{C}'_{Q,v} = \mathbb{C}_Q \cup \mathbb{C}_{Q,v}$$

where

$$\mathbb{C}_Q = \{\Delta_\tau(X) : X \in \mathbb{C}, X \subseteq Q\})$$

and

$$\mathbb{C}_{Q,v} = \{\Delta_\tau(X \cap Q) : X \in \mathbb{C}, v \in X\}.$$

Remark 9: If $\mathbb{C}$ was constructed by the multilevel construction of Section IV then the codewords of $\mathbb{C}_Q$ and $\mathbb{C}_{Q,v}$ can be partitioned into related lifted codes of Ferrers diagram rank-metric codes. Some of these codes are cosets of the linear Ferrers diagram rank-metric codes.

The following theorem can be easily verified.

Theorem 4: The punctured code $\mathbb{C}'_{Q,v}$ of an $(n,M,d)_q$ code $\mathbb{C}$ is an $(n-1,M',d-1)_q$ code.

Remark 10: The code $\tilde{\mathbb{C}} = \{X : X \in \mathbb{C}, X \subseteq Q\}) \cup \{X \cap Q : X \in \mathbb{C}, v \in X\}$ is an $(n,M',d-1)_q$ code whose codewords are contained in Q. Since Q is an $(n-1)$-dimensional subspace it follows that there is an isomorphism φ such that $\varphi(Q) = \mathbb{F}_q^{n-1}$. The code $\varphi(\tilde{\mathbb{C}}) = \{\varphi(X) : X \in \tilde{\mathbb{C}}\}$ is an $(n-1,M',d-1)_q$ code. The code $\mathbb{C}'_{Q,v}$ was obtained from $\tilde{\mathbb{C}}$ by such isomorphism which uses the τ-coordinate puncturing on all the vectors of Q.

Example 12: Let $\mathbb{C}$ be the $(8,4573,4,4)_2$ code given in Example 10. Let Q be the seven-dimensional subspace whose 7×8 generator matrix is

$$\begin{pmatrix} 1&0&\dots&0&0\\ 0&1&\dots&0&0\\ \vdots&\vdots&\ddots&\vdots&\vdots\\ 0&0&\dots&1&0 \end{pmatrix}.$$

By using puncturing with Q and $v = 1000001$ we obtain a code $\mathbb{C}'_{Q,v}$ with minimum distance 3 and size 573. By adding to $\mathbb{C}'_{Q,v}$ two codewords, the null space $\{0\}$ and $\mathbb{F}_2^7$ we obtained a $(7,575,3)_2$ code in $\mathcal{P}_2(7)$. The following tables show the number of codewords which were obtained from each of the identifying vectors with weight 4 of Example 10 (see the top of the following page). The Ferrers diagram rank-metric codes in some of the entries must be chosen (if we want to construct the same code by a multilevel construction) in a clever way and not directly as given in Section III. We omit their description from lack of space and leave it to the interested reader.

The large difference between the sizes of the codes of Examples 11 and 12 shows the strength of puncturing when applied on codes in $\mathcal{P}_q(n)$.

$\mathbb{C}_Q$	
identifying vector	addition to $\mathbb{C}_Q$
11110000	256
11001100	16
10101010	8
10010110	2
01100110	4
01011010	2
00111100	1

$\mathbb{C}_{Q,v}$	$v = 10000001$
identifying vector	addition to $\mathbb{C}_{Q,v}$
11110000	256
11001100	16
11000011	1
10101010	4
10100101	2
10011001	4
10010110	1

B. Code Parameters

First we ask, what is the number of codes which can be defined in this way from $\mathbb{C}$? Q is an $(n-1)$-dimensional subspace of $\mathbb{F}_q^n$ and hence it can be chosen in $\frac{q^n-1}{q-1}$ different ways. There are $\frac{q^n-q^{n-1}}{q-1}=q^{n-1}$ distinct way to choose $v \notin Q$ after Q was chosen. Thus, we have that usually puncturing of a code $\mathbb{C}$ in $\mathcal{P}_q(n)$ will result in $\frac{q^{2n-1}-q^{n-1}}{q-1}$ different punctured codes.

Theorem 5: If $\mathbb{C}$ is an $(n,M,d,k)_q$ code then there exists an $(n-1,M',d-1)_q$ code $\mathbb{C}'_{Q,v}$ such that $M' \geq \frac{M(q^{n-k}+q^k-2)}{q^n-1}$.

Proof: As before, Q can be chosen in $\frac{q^n-1}{q-1}$ different ways. By using basic enumeration, it is easy to verify that each k-dimensional subspace of $\mathcal{P}_q(n)$ is contained in $\frac{q^{n-k}-1}{q-1}$ $(n-1)$-dimensional subspaces of $\mathcal{P}_q(n)$. Thus, by a simple averaging argument we have that there exists an $(n-1)$-dimensional subspace Q such that $|\mathbb{C}_Q| \geq M\frac{q^{n-k}-1}{q^n-1}$.

There are $M-|\mathbb{C}_Q|$ codewords in $\mathbb{C}$ which are not contained in Q. For each such codeword $X \in \mathbb{C}$ we have $\dim(X\cap Q) = k-1$. Therefore, X contains q^k-q^{k-1} vectors which do not belong to Q. In $\mathbb{F}_q^n$ there are q^n-q^{n-1} vectors which do not belong to Q. Thus, again by using simple averaging argument we have that there exist an $(n-1)$-dimensional subspace $Q \subset \mathbb{F}_q^n$ and $v \notin Q$ such that

$$|\mathbb{C}_{Q,v}| \geq \frac{(M-|\mathbb{C}_Q|)(q^k-q^{k-1})}{q^n-q^{n-1}} = \frac{M-|\mathbb{C}_Q|}{q^{n-k}}.$$

Therefore, there exists an $(n-1,M',d-1)_q$ code $\mathbb{C}'_{Q,v}$ such that

$$\begin{aligned} M' = |\mathbb{C}_Q|+|\mathbb{C}_{Q,v}| &\geq \frac{|\mathbb{C}_Q|q^{n-k}+M-|\mathbb{C}_Q|}{q^{n-k}} \\ &= \frac{(q^{n-k}-1)|\mathbb{C}_Q|+M}{q^{n-k}} \\ &\geq \frac{(q^{n-k}-1)M(q^{n-k}-1)+M(q^n-1)}{(q^n-1)q^{n-k}} \\ &= \frac{M(q^{n-k}+q^k-2)}{q^n-1}. \end{aligned}$$ □

Clearly, choosing the $(n-1)$-dimensional subspace Q and the element v in a way that $\mathbb{C}'_{Q,v}$ will be maximized is important in this context. Example 12 can be generalized in a very simple way. We start with a $(4k, q^{2k(k+1)}, 2k, 2k)_q$ code obtained from the codeword $\underbrace{1\cdots1}_{2k}\underbrace{0\cdots0}_{2k}$ in the multilevel approach. We apply puncturing with the $(n-1)$-dimensional subspace Q whose $(n-1)\times n$ generator matrix is

$$\begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

It is not difficult to show that in the $[(2k)\times(2k), 2k(k+1), k]$ rank-metric code $\mathcal{C}$ there are q^{2k^2} codewords with *zeros* in the last column and q^{2k^2} codewords with *zeros* in the first row. There is also a codeword whose first row ends with a *one*. If u is this first row which ends with a *one* there are q^{2k^2} codewords whose first row is u. We choose v to be $v = 1\underbrace{0\cdots0}_{2k-1}u$. By using puncturing with Q and v we have $|\mathbb{C}_Q| = q^{2k^2}$ and $|\mathbb{C}_{Q,v}| = q^{2k^2}$. Hence, $\mathbb{C}'_{Q,v}$ is a $(4k-1, 2q^{2k^2}, 2k-1)_q$ code in $\mathcal{P}_q(4k-1)$. By using more codewords from the constant-weight code in the multilevel approach and adding the null space and $\mathbb{F}_q^{4k-1}$ to the code we construct a slightly larger code with the same parameters.

C. Decoding

We assume that $\mathbb{C}$ is an $(n,M,d)_q$ code and that all the dimensions of the subspaces in $\mathbb{C}$ have the same parity which implies that $d = 2\delta$. This assumption makes sense as these are the interesting codes on which puncturing is applied, similarly to puncturing in the Hamming space. We further assume for simplicity that without loss of generality (w.l.o.g.) if $E(Q)$ is the $(n-1)\times n$ generator matrix of Q then the first $n-1$ columns are linearly independent, i.e., $E(Q) = [Iu]$, where I is an $(n-1)\times(n-1)$ unity matrix and u is a column vector of length $n-1$.

Assume that the received word from a codeword X' of $\mathbb{C}'_{Q,v}$ is an ℓ-dimensional subspace Y' of $\mathbb{F}_q^{n-1}$. The first step will be to find a subspace Z of $\mathbb{F}_q^n$ on which we can apply the decoding algorithm of $\mathbb{C}$. The result of this decoding will reduced to the $(n-1)$-dimensional subspace Q and punctured to obtain the codeword of $\mathbb{C}'_{Q,v}$. We start by generating from Y' an ℓ-dimensional subspace $Y \subset Q$ of $\mathbb{F}_q^n$. This is done by appending a symbol to the end of each vector in Y' by using the generator matrix $E(Q)$ of Q. If a generator matrix $E(Y')$ is given we can do this process only to the rows of $E(Y')$ to obtain the generator matrix $E(Y)$ of Y. We leave to the reader the verification that the generator matrix of Y is formed in its reduced row echelon form.

Remark 11: If the *zero* of $v(Q)$ is in coordinate τ then instead of appending a symbol to the end of the codeword we insert a symbol at position τ.

Let ℓ be the dimension of Y' and assume p is the parity of the dimension of any subspace in $\mathbb{C}$, where $p=0$ or $p=1$. Once we have Y we distinguish between two cases to form a new subspace Z of $\mathbb{F}_q^n$.

Case 1: δ is even.

- If $\ell \equiv p (\bmod 2)$ then $Z = Y \cup (v + Y)$.
- If $\ell \not\equiv p (\bmod 2)$ then $Z = Y$.

Case 2: δ is odd.

- If $\ell \equiv p (\bmod 2)$ then $Z = Y$.
- If $\ell \not\equiv p (\bmod 2)$ then $Z = Y \cup (v + Y)$.

Now we use the decoding algorithm of the code $\mathbb{C}$ with the word Z. The algorithm will produce as an output a codeword $\mathcal{X}$. Let $\tilde{X} = \mathcal{X} \cap Q$ and $\tilde{X}'$ be the subspace of $\mathbb{F}_q^{n-1}$ obtained from $\tilde{X}$ by deleting the last entry of $\tilde{X}$. We output $\tilde{X}'$ as the submitted codeword X' of $\mathbb{C}'_{Q,v}$. The correctness of the decoding algorithm is an immediate consequence of the following theorem.

Theorem 6: If $d_S(X', Y') \leq \delta - 1$ then $\tilde{X}' = X'$.

Proof: Assume that $d_S(X', Y') \leq \delta - 1$. Let $X \subseteq Q$ be the word obtained from X' by appending a symbol to the end of each vector in X' (this can be done by using the generator matrix $E(Q)$ of Q). If $u \in X' \cap Y'$ then we append the same symbol to u to obtain the element of X and to obtain the element of Y. Hence, $d_S(X, Y) = d_S(X', Y') \leq \delta - 1$. If $d_S(X, Y) \leq \delta - 2$ then $d_S(X, Z) \leq d_S(X, Y) + 1 \leq \delta - 1$. Now, note that if $\delta - 1$ is odd then Z does not have the same parity as the dimensions of the subspaces in $\mathbb{C}$ and if $\delta - 1$ is even then Z has the same parity as the dimensions of the subspaces in $\mathbb{C}$. Therefore, if $d_S(X, Y) = \delta - 1$ then by the definition of Z we have $Z = Y$ and hence $d_S(X, Z) = \delta - 1$. Therefore, the decoding algorithm of $\mathbb{C}$ will produce as an output the unique codeword $\mathcal{X}$ such that $d_S(\mathcal{X}, Z) \leq \delta - 1$, i.e., $X = \mathcal{X}$. X' is obtained by deleting the last entry is each vector of $X \cap Q$; $\tilde{X}'$ is obtained by deleting the last entry is each vector of $\mathcal{X} \cap Q$. Therefore, $\tilde{X}' = X'$. $\square$

The constant-dimension codes constructed in Section IV have the same dimension for all codewords. Hence, if $\mathbb{C}$ was constructed by our multilevel construction then its decoding algorithm can be applied on the punctured code $\mathbb{C}'_{Q,v}$.

VI. Conclusion and Open Problems

A multilevel coding approach to construct codes in the Grassmannian and the projective space was presented. The method makes usage of four tools, an appropriate constant-weight code, the reduced row echelon form of a linear subspace, the Ferrers diagram related to this echelon form, and rank-metric codes related to the Ferrers diagram. Some of these tools seem to be important and interesting in themselves in general and particularly in the connection of coding in the projective space. The constructed codes by our method are usually the best known today for most parameters. We have also defined the puncturing operation on codes in the projective space. We applied this operation to obtain punctured codes from our constant-dimension codes. These punctured codes are considerably larger than codes constructed by any other method. The motivation for considering these codes came from network coding [21]–[23] and error-correction in network coding [2], [24], [25]. It is worth mentioning that the actual dimensions of the error-correcting codes needed for network coding are much larger than the dimensions given in our examples. Clearly, our method works also on much higher dimensions as needed for the real application.

The research on coding in the projective space is only in its initial steps and many open problems and directions for further research are given in our references. We focus now only on problems which are directly related to our current research.

- Is there a specification for the best constant-weight code which should be taken for our multilevel approach? Our discussion on the Hamming code and lexicodes is a first step in this direction.
- Is the upper bound of Theorem 1 attained for all parameters? Our constructions for optimal Ferrers diagram rank-metric codes suggest that the answer is positive.
- How far are the codes constructed by our method from optimality? The upper bounds on the sizes of codes in the Grassmannian and the projective space are still relatively much larger than the sizes of our codes [4], [2], [11]. The construction of cyclic codes in [4] suggests that indeed there are codes which are relatively much larger than our codes. However, we believe that in general the known upper bounds on the sizes of codes in the projective space are usually much larger than the actual size of the largest codes. Indeed, solution for this question will imply new construction methods for error-correcting codes in the projective space.

Acknowledgment

The authors wish to thank Ron Roth and Alexander Vardy for many helpful discussions. They also thank the anonymous reviewers for their valuable comments.

References

[1] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, "On perfect codes and related concepts," *Des., Codes Cryptogr.*, vol. 22, pp. 221–237, 2001.

[2] 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.

[3] 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.

[4] T. Etzion and A. Vardy, "Error-correcting codes in projective space," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, ON, Canada, Jul. 2008, pp. 871–875.

[5] E. M. Gabidulin and M. Bossert, "Codes for network coding," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, ON, Canada, Jul. 2008, pp. 867–870.

[6] M. Gadouleau and Z. Yan, "On the Connection Between Optimal Constant-Rank Codes and Optimal Constant-Dimension Codes," arxiv.org/abs/0803.2262.

[7] M. Gadouleau and Z. Yan, "Constant-rank codes," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, ON, Canada, Jul. 2008, pp. 876–880.

[8] A. Kohnert and S. Kurz, "Construction of Large Constant Dimension Codes With a Prescribed Minimum Distance," arxiv.org/abs/0807.3212.

[9] F. Manganiello, E. Gorla, and J. Rosenthal, "Spread codes and spread decoding in network coding," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, ON, Canada, Jul. 2008, pp. 881–885.

[10] V. Skachek, "Recursive Code Construction for Random Network," arxiv.org/abs/0806.3650.

[11] S. T. Xia and F. W. Fu, "Johnson type bounds on constant dimension codes," *Des., Codes, Cryptogr.*, vol. 50, pp. 163–172, 2009.

[12] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inf. Transm.*, vol. 21, pp. 1–12, Jul. 1985.

[13] R. M. Roth, "Maximum-rank array codes and their application to criss-cross error correction," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 328–336, Mar. 1991.

[14] D. E. Knuth, "Subspaces, subsets. and partitions," *J. Combin. Theory*, vol. 10, pp. 178–180, 1971.
[15] J. H. van Lint and R. M. Wilson*, A Course in Combinatorics*. Cambridge, U.K.: Cambridge Univ. Press, 1992.
[16] G. E. Andrews and K. Eriksson*, Integer Partitions*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[17] R. P. Stanley*, Enumerative Combinatorics*. Monterey, CA: Wadsworth, 1986, vol. 1.
[18] S. Milne, "Mappings of subspaces into subsets," *J. Comb. Theory*, ser. A, vol. 33, pp. 36–47, 1982.
[19] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *J. Comb. Theory*, ser. A, vol. 25, pp. 226–241, 1978.
[20] J. H. Conway and N. J. A. Sloane, "Lexicographic codes: Error-correcting codes from game theory," *IEEE Trans. Inf. Theory*, vol. IT-32, no. 3, pp. 337–348, May 1986.
[21] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *Des., Codes, Cryptogr.*, vol. 46, pp. 1204–1216, July 2000.
[22] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.
[23] T. Ho, R. Koetter, M. Médard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in *Proc. IEEE Int. Symp. Information Theory*, Yokohoma, Japan, Jun./Jul. 2003, p. 442.
[24] N. Cai and R. W. Yeung, "Network error correction, part II: Lower bounds," *Commun. Inf. Systist.*, vol. 6, pp. 37–54, May 2006.
[25] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Commun. Inf. Systist.*, vol. 6, pp. 19–36, May 2006.

Tuvi Etzion (M'89–SM'99–F'04) was born in Tel-Aviv, Israel, in 1956. He received the B.A., M.Sc., and D.Sc. degrees from the Technion–Israel Institute of Technology, Haifa, Israel, in 1980, 1982, and 1984, respectively.

Since 1984, he has held a position in the Department of Computer Science at the Technion, where he is a Professor. During the years 1986–1987, he was Visiting Research Professor with the Department of Electrical Engineering–Systems at the University of Southern California, Los Angeles. During the summers of 1990 and 1991, he was visiting Bellcore, Morristown, NJ. During the years 1994–1996, he was a Visiting Research Fellow in the Computer Science Department at Royal Holloway College, Egham, U.K. He also had several visits to the Coordinated Science Laboratory at University of Illinois in Urbana-Champaign during the years 1995–1998, two visits to HP Bristol, Bristol, U.K., during the summers of 1996, 2000, a few visits to the Department of Electrical Engineering, University of California, San Diego, during the years 2000–2009, and several visits to the Mathematics Department at Royal Holloway College, Egham, U.K., during the years 2007–2008. His research interests include applications of discrete mathematics to problems in computer science and information theory, coding theory, and combinatorial designs.

Dr. Etzion was an Associate Editor for Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 2006 till 2009.

Natalia Silberstein was born in Russia in 1977. She received the B.A. and M.Sc. degrees from the Technion–Israel Institute of Technology, Haifa, Israel, in 2004 and 2007, respectively, from the Computer Science Department and the Applied Mathematics Department, respectively.

She is currently working toward the Ph.D. degree in the Computer Science Department at the Technion. Her research interests include algebraic error-correction coding, coding theory, and combinatorics.