Error-Correcting Codes in Projective Space

Tuvi Etzion, *Fellow, IEEE*, and Alexander Vardy, *Fellow, IEEE*

Dedicated to the memory of Ralf Koetter (1963–2009)

***Abstract*—The projective space of order n over the finite field $\mathbb{F}_q$, denoted here as $\mathcal{P}_q(n)$, is the set of all subspaces of the vector space $\mathbb{F}_q^n$. The projective space can be endowed with the distance function $d(U,V) = \dim U + \dim V - 2\dim(U \cap V)$ which turns $\mathcal{P}_q(n)$ into a metric space. With this, *an* (n, M, d) *code* $\mathbb{C}$ *in projective space* is a subset of $\mathcal{P}_q(n)$ of size M such that the distance between any two codewords (subspaces) is at least d. Koetter and Kschischang recently showed that codes in projective space are precisely what is needed for error-correction in networks: an (n, M, d) code can correct t packet errors and ρ packet erasures introduced (adversarially) anywhere in the network as long as $2t + 2\rho < d$. This motivates our interest in such codes. In this paper, we investigate certain basic aspects of "coding theory in projective space." First, we present several new bounds on the size of codes in $\mathcal{P}_q(n)$, which may be thought of as counterparts of the classical bounds in coding theory due to Johnson, Delsarte, and Gilbert-Varshamov. Some of these are stronger than all the previously known bounds, at least for certain code parameters. We also present several specific constructions of codes and code families in $\mathcal{P}_q(n)$. Finally, we prove that nontrivial perfect codes in $\mathcal{P}_q(n)$ do not exist.**

***Index Terms*—Network coding, network error-correction, perfect codes, projective-space codes, subspace codes.**

I. Introduction

LET $\mathbb{F}_q$ be the finite field of order q, and let $\mathcal{W}$ be an arbitrary (fixed) vector space of dimension n over $\mathbb{F}_q$. Since $\mathcal{W}$ is isomorphic to $\mathbb{F}_q^n$, in what follows one can assume that $\mathcal{W}$ *is* in fact $\mathbb{F}_q^n$. The ***projective space***[1] of order n over $\mathbb{F}_q$, denoted herein by $\mathcal{P}_q(n)$, is the set of all the subspaces of $\mathcal{W}$, including $\{\mathbf{0}\}$ and $\mathcal{W}$ itself. Given a nonnegative integer $k \leqslant n$, the set of all subspaces of $\mathcal{W}$ that have dimension k is known as a ***Grassmannian***, and usually denoted by $\mathcal{G}_q(n,k)$. Thus $\mathcal{P}_q(n) = \cup_{0 \leqslant k \leqslant n} \mathcal{G}_q(n,k)$. It is well known that

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

where $\begin{bmatrix} n \\ k \end{bmatrix}$ is the *q-ary Gaussian coefficient*. It turns out that the natural measure of distance in $\mathcal{P}_q(n)$ is given by

$$d(U,V) \stackrel{\text{def}}{=} \dim U + \dim V - 2\dim(U \cap V) \qquad (1)$$

for all $U, V \in \mathcal{P}_q(n)$. It is well known (cf. [1], [20]) 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) ***code in projective space*** if $|\mathbb{C}| = M$ and $d(U,V) \geqslant d$ for all U, V in $\mathbb{C}$. If an (n, M, d) 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) code.

The (n, M, d), respectively (n, M, d, k), 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. There are, however, important differences. For all q, n and k, the metric space $\mathcal{G}_q(n,k)$ corresponds to a distance-regular graph, similar to the distance-regular graph resulting from the Johnson space. On the other hand, while the Hamming space $\mathbb{F}_q^n$ is always distance-regular (as a graph), the projective space $\mathcal{P}_q(n)$ is not. This implies that conventional geometric intuition does not always apply; for example, two spheres of the same radius in $\mathcal{P}_q(n)$ may have different sizes.

Codes in $\mathcal{G}_q(n,k)$ were studied, somewhat sparsely, over the past twenty years. For example, the nonexistence of perfect codes in $\mathcal{G}_q(n,k)$ was proved in [7] and again in [24]. In [1], it was shown that "Steiner structures" yield diameter-perfect codes in $\mathcal{G}_q(n,k)$; properties of these structures were studied in [26]. Related work on certain intersecting families and on byte-correcting codes can be found in [13] and in [6], [10], respectively. Another application of codes in $\mathcal{G}_q(n,k)$, to linear authentication schemes, was given in [35]. It appears that codes in the projective space $\mathcal{P}_q(n)$ were not studied at all, until recently [3], [11], [14], [15], [18]–[20], [23], [27]–[29].

Recently, Koetter and Kschischang [18]–[20] showed that codes in $\mathcal{P}_q(n)$ are precisely what is needed for error-correction in networks: an (n, M, d) code can correct any t packet errors and any ρ packet erasures introduced (adversarially) anywhere in the network as long as $2t + 2\rho < d$. This motivates our interest in such codes. In a sense, one would like to re-derive as much as possible of the classical coding theory, developed for the Hamming metric, in the context of $\mathcal{P}_q(n)$ and $\mathcal{G}_q(n,k)$.

Manuscript received May 01, 2010; revised August 25, 2010; accepted November 08, 2010. Date of current version January 19, 2011. This work was supported in part by the United States National Science Foundation and in part by the United States—Israel Binational Science Foundation (BSF), Jerusalem, Israel, under Grant 2006097. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Toronto, ON, Canada, July 2008.

This paper is part of the special issue on "Facets of Coding Theory: From Algorithms to Networks," dedicated to the scientific legacy of Ralf Koetter.

T. Etzion is with the Department of Computer Science, Technion, Haifa 32000, Israel (e-mail: etzion@cs.technion.ac.il).

A. Vardy is with the Department of Electrical and Computer Engineering, the Department of Computer Science and Engineering, and the Department of Mathematics, University of California San Diego, La Jolla, CA 92093-0407 USA (e-mail: avardy@ucsd.edu).

Communicated by F. R. Kschischang, Associate Editor for the special issue on "Facets of Coding Theory: From Algorithms to Networks."

Digital Object Identifier 10.1109/TIT.2010.2095232

[1]Many relevant papers refer to $\mathcal{P}_q(n)$ as the *projective geometry* of $\mathcal{W}$. The terms "projective geometry" and "projective space" seem to be equally well-established in the literature. We feel that "projective space" is the more fortunate terminology, since $\mathcal{P}_q(n)$ is the ambient *space* for the codes at hand.

Some of this work has been already carried out by Koetter and Kschischang [20], and others [4], [14]–[17], [21], [25], [28]. In particular, Koetter and Kschischang derived in [20] the counterparts of the classical sphere-packing, Singleton, and Gilbert-Varshamov bounds, and gave a construction of Reed-Solomon-like codes. However, most of these results pertain to codes in $\mathcal{G}_q(n,k)$ and do not extend to the more general case of $\mathcal{P}_q(n)$.

Our goal herein is to continue the work of [20] by studying certain key aspects of "coding theory in projective space." We begin in the following section with bounds on the size of codes in $\mathcal{G}_q(n,k)$, by deriving the counterparts of the classical bounds due to Delsarte and Johnson. These turn out to be always stronger than the best bound of [20]. We also provide two bounds on the size of codes in $\mathcal{P}_q(n)$ that are akin to the classical Gilbert-Varshamov and linear-programming bounds (despite the fact that $\mathcal{P}_q(n)$ is not distance-regular). In Section III, we present several constructions of specific codes and code families in $\mathcal{G}_q(n,k)$ and $\mathcal{P}_q(n)$. These are based upon Steiner structures [1], [23], [26], perfect byte-correcting codes [10], computer search for *cyclic* codes in $\mathcal{P}_q(n)$, and other ideas. A natural question is whether one can construct *perfect codes* in projective space. In Section IV, we prove that nontrivial perfect codes in $\mathcal{P}_q(n)$ do not exist. We conclude the paper with a brief discussion and a list of open problems in Section V.

II. Bounds on the Size of Codes in Projective Space

Let $\mathcal{A}_q(n,d)$, respectively $\mathcal{A}_q(n,d,k)$, denote the maximum number of codewords in an (n,M,d) code in $\mathcal{P}_q(n)$, respectively (n,M,d,k) code in $\mathcal{G}_q(n,k)$ (we use calligraphic letters to distinguish these from the well-known quantities $A_q(n,d)$ and $A_q(n,d,w)$ defined for the Hamming metric). Note that the distance between any two elements of $\mathcal{G}_q(n,k)$ is always even; thus it suffices to consider $\mathcal{A}_q(n,d,k)$ for even $d=2\delta$.

Let $t=\lfloor(\delta-1)/2\rfloor$. Koetter and Kschischang [20] established the following bound:

$$\mathcal{A}_q(n,2\delta,k)\leqslant\frac{|\mathcal{G}_q(n,k)|}{|\mathcal{S}_{n,k}(t)|}=\frac{\begin{bmatrix}n\\k\end{bmatrix}}{\sum_{m=0}^{t}\begin{bmatrix}k\\m\end{bmatrix}\begin{bmatrix}n-k\\m\end{bmatrix}q^{m^2}}. \tag{2}$$

Here, $|\mathcal{S}_{n,k}(t)|$ is the volume of a sphere of radius t in $\mathcal{G}_(n,k)$, which is well-defined since $\mathcal{G}_q(n,k)$ is distance-regular. Thus, (2) is the counterpart of the well-known *sphere-packing bound* in Hamming space. Koetter-Kschischang [20] also proved that

$$\mathcal{A}_q(n,2\delta,k)\leqslant\begin{bmatrix}n-\delta+1\\k-\delta+1\end{bmatrix} \tag{3}$$

which may be regarded as a counterpart of the classical *Singleton bound* [22, p.33]. They have further observed that (3) is usually stronger than the sphere-packing bound (2).

Herein, we observe that the sphere is the wrong structure to consider in the case of $\mathcal{G}_q(n,k)$. The sphere-packing bound is a special case of the *anticode bound* which was proved by Delsarte [8] for arbitrary association schemes. An anticode $\mathscr{A}(t)$ of diameter t in $\mathcal{G}_q(n,k)$ is any subset of $\mathcal{G}_q(n,k)$ such that $d(U,V)\leqslant 2t$ for all $U,V\in\mathscr{A}(t)$. Delsarte's theorem [8, p.32] implies that $\mathcal{A}_q(n,2\delta,k)\leqslant|\mathcal{G}_q(n,k)|/|\mathscr{A}(\delta-1)|$, for *any* anticode of diameter $\delta-1$. The sphere $\mathcal{S}_{n,k}(t)$ is clearly an example of such an anticode. But, in contrast to the binary Hamming space, where spheres are the largest anticodes, $\mathcal{S}_{n,k}(t)$ is but a small anticode in $\mathcal{G}_q(n,k)$. The optimal (largest) anticodes in $\mathcal{G}_q(n,k)$ were found by Frankl and Wilson in [13]. Combining the results of [13] with the foregoing discussion, we immediately obtain the following bound.

Theorem 1:

$$\mathcal{A}_q(n,2\delta+2,k)\leqslant\frac{\begin{bmatrix}n\\k\end{bmatrix}}{\begin{bmatrix}n-k+\delta\\\delta\end{bmatrix}} \tag{4}$$

Proof: It is shown in [13] that the size of the largest anticode of diameter δ in $\mathcal{G}_q(n,k)$ is given by $\begin{bmatrix}n-k+\delta\\\delta\end{bmatrix}$. ∎

An altogether different way to improve upon (2) is based upon a standard covering argument.

Theorem 2:

$$\mathcal{A}_q(n,2\delta+2,k)\leqslant\frac{\begin{bmatrix}n\\k-\delta\end{bmatrix}}{\begin{bmatrix}k\\k-\delta\end{bmatrix}} \tag{5}$$

Proof: Let $\mathbb{C}$ be an $(n,M,2\delta+2,k)$ code. Then each codeword of $\mathbb{C}$ contains (or "covers") exactly $\begin{bmatrix}k\\k-\delta\end{bmatrix}$ subspaces of dimension $k-\delta$. On the other hand, a given subspace of $\mathbb{F}_q^n$ of dimension $k-\delta$ cannot be contained in two distinct codewords U, V of $\mathbb{C}$, since otherwise

$$d(U,V)=2k-2\dim(U\cap V)\leqslant 2k-2(k-\delta)=2\delta.$$

Since the total number of $(k-\delta)$-dimensional subspaces of $\mathbb{F}_q^n$ is $\begin{bmatrix}n\\k-\delta\end{bmatrix}$, we see that M cannot exceed $\begin{bmatrix}n\\k-\delta\end{bmatrix}/\begin{bmatrix}k\\k-\delta\end{bmatrix}$. ∎

Theorem 2 was proved in [35, Theorem 5.2] in the context of linear authentication codes. It is clear from its proof herein that if $\mathbb{C}$ attains the bound of (5) with equality, then every $(k-\delta)$-dimensional subspace of $\mathbb{F}_q^n$ must be contained in exactly one codeword of $\mathbb{C}$. Such codes are known as *Steiner structures* [1], [26] and will be discussed again in the next section, where necessary conditions for their existence are given. It follows that for those parameters n,k,δ which do not satisfy these conditions, Theorem 2 can be further improved.

The following theorem results by iteratively applying one of the Johnson bounds, established later in this section.

Theorem 3:

$$\mathcal{A}_q(n,2\delta,k)\leqslant\prod_{i=0}^{k-\delta}\frac{q^{n-i}-1}{q^{k-i}-1} \tag{6}$$

Proof: Apply Theorem 4 iteratively $k-\delta+1$ times, stopping with the trivial equality $\mathcal{A}_q(n-k+\delta-1,2\delta,\delta-1)=1$. ∎

Theorems 1, 2, and 3 are proved using completely different methods. It is therefore remarkable that the corresponding bounds coincide. Namely

$$\frac{\begin{bmatrix} n \\ k \end{bmatrix}}{\begin{bmatrix} n-k+\delta \\ \delta \end{bmatrix}} = \frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}} = \prod_{i=0}^{k-\delta-1} \frac{q^{n-i}-1}{q^{k-i}-1}. \tag{7}$$

as can be verified directly from the definition of Gaussian coefficients. It is noteworthy that, in contrast to (2), these bounds are *always stronger* than the Singleton bound (3), as shown in [36]. It is proved in [20, p. 3588] that the Singleton bound (3) differs from the true value of $\mathcal{A}_q(n, 2\delta, k)$ by a factor of at most 4. This immediately implies that all the bounds in (7) have the same property. However, these bounds can be further improved, albeit slightly, as we shall see in what follows.

The next two theorems are the counterparts in $\mathcal{G}_q(n,k)$ of the two classical Johnson bounds for constant-weight codes.

Theorem 4:

$$\mathcal{A}_q(n, 2\delta, k) \leqslant \frac{q^n-1}{q^k-1}\,\mathcal{A}_q(n-1, 2\delta, k-1)$$

Proof: Let $\mathbb{C}$ be an $(n, M, 2\delta, k)$ code in $\mathcal{G}_q(n,k)$, and suppose that $M = \mathcal{A}_q(n, 2\delta, k)$. Then each codeword of $\mathbb{C}$ contains $(q^k-1)/(q-1)$ one-dimensional subspaces of $\mathbb{F}_q^n$. Since the total number of such subspaces is $(q^n-1)/(q-1)$, there is a one-dimensional subspace $\mathcal{X} \in \mathcal{G}_q(n,1)$ that is contained in at least $M(q^k-1)/(q^n-1)$ codewords of $\mathbb{C}$. Assume $\mathcal{X} = \langle x \rangle$, where $x \in \mathbb{F}_q^n$ and $\langle \cdot \rangle$ stands for the linear span. Write $\mathbb{F}_q^n$ as $\mathcal{X} \oplus \mathcal{W}$, where $\mathcal{W} \in \mathcal{G}_q(n, n-1)$. For example, find a basis $\{x, e_1, e_2, \ldots, e_{n-1}\}$ for $\mathbb{F}_q^n$, and set $\mathcal{W} = \langle e_1, e_2, \ldots, e_{n-1} \rangle$. Next, define

$$\mathbb{C}' \stackrel{\text{def}}{=} \big\{ V \cap \mathcal{W} \,:\, V \in \mathbb{C} \text{ and } \mathcal{X} \subset V \big\}.$$

It is easy to see that all the codewords of $\mathbb{C}'$ are contained in $\mathcal{W}$ and have dimension $k-1$. Thus, $\mathbb{C}'$ can be regarded as an $(n-1, M', 2\delta', k-1)$ code, where $M' \geqslant M(q^k-1)/(q^n-1)$ by our choice of $\mathcal{X}$. It remains to show that $\delta' = \delta$, for this would imply that

$$\mathcal{A}_q(n-1, 2\delta, k-1) \geqslant M' \geqslant \frac{q^k-1}{q^n-1}\,\mathcal{A}_q(n, 2\delta, k).$$

To this end, consider two arbitrary codewords U' and V' of $\mathbb{C}'$ such that $U' = U \cap \mathcal{W}$ and $V' = V \cap \mathcal{W}$, where U and V are the corresponding codewords of $\mathbb{C}$ (with $\mathcal{X} \subset U$ and $\mathcal{X} \subset V$). Note that $U' \cap V' = (U \cap \mathcal{W}) \cap (V \cap \mathcal{W}) = (U \cap V) \cap \mathcal{W}$. This implies that

$$\begin{aligned} &\dim(U' \cap V') \\ &\quad = \dim(U \cap V) + \dim \mathcal{W} - \dim\big((U \cap V) + \mathcal{W}\big) \\ &\quad = \dim(U \cap V) + (n-1) - n \end{aligned}$$

where the second equality follows from the fact that $U \cap V$ contains $\mathcal{X}$. Hence $\dim(U' \cap V') = \dim(U \cap V) - 1$, from which $\delta' = \delta$ follows immediately by (1). ■

Observe that Theorem 4 is proved in a manner similar to the proof of the analogous Johnson bound in [22, p. 527]. In fact, a proof along these lines was given independently by Xia and Fu [36]. Notably, while we have two different proofs[2] of the next result, neither of them has anything in common with the proof of the analogous Johnson bound [22, p. 528].

Theorem 5:

$$\mathcal{A}_q(n, 2\delta, k) \leqslant \frac{q^n-1}{q^{n-k}-1}\,\mathcal{A}_q(n-1, 2\delta, k)$$

Proof: Let $\mathbb{C}$ be an $(n, M, 2\delta, k)$ code in $\mathcal{G}_q(n,k)$, and suppose $M = \mathcal{A}_q(n, 2\delta, k)$. For each $\mathcal{W} \in \mathcal{G}_q(n, n-1)$, define

$$\mathbb{C}_{\mathcal{W}} \stackrel{\text{def}}{=} \big\{ V \,:\, V \in \mathbb{C} \text{ and } V \subset \mathcal{W} \big\}.$$

Then $\mathbb{C}_{\mathcal{W}}$ is an $(n-1, M_{\mathcal{W}}, 2\delta', k)$ code with $\delta' \geqslant \delta$, for each $\mathcal{W} \in \mathcal{G}_q(n, n-1)$. It is known (see e.g., [34, p.551]) that any given k-dimensional subspace of $\mathbb{F}_q^n$ is contained in precisely $(q^{n-k}-1)/(q-1)$ elements of $\mathcal{G}_q(n, n-1)$. Thus, each codeword of $\mathbb{C}$ belongs to $(q^{n-k}-1)/(q-1)$ different codes $\mathbb{C}_{\mathcal{W}}$, and therefore

$$\sum_{\mathcal{W}} |\mathbb{C}_{\mathcal{W}}| \;=\; M\frac{q^{n-k}-1}{q-1}$$

where the sum is over all the $(q^n-1)/(q-1)$ elements of $\mathcal{G}_q(n, n-1)$. Hence, there exists at least one $\mathcal{W} \in \mathcal{G}_q(n, n-1)$ such that $|\mathbb{C}_{\mathcal{W}}| \geqslant M(q^{n-k}-1)/(q^n-1)$. Since it is obvious that $\mathcal{A}_q(n-1, 2\delta, k) \geqslant |\mathbb{C}_{\mathcal{W}}|$ for all $\mathcal{W}$, the theorem follows. ■

Theorems 4 and 5 can be now iterated to obtain a bound on $\mathcal{A}_q(n, 2\delta, k)$ for any specific values of n, k, and δ. In which order they should be iterated to produce the *best* bound is not at all clear. In fact, this problem is still open even for the conventional Johnson space—see [22, Research Problem 17.1]. However, one can, of course, simply iterate Theorem 4 with itself. In conjunction with the observation that $\mathcal{A}_q(n, 2\delta, k) = 1$ for all $k < \delta$, this produces the following bound.

Theorem 6:

$$\mathcal{A}_q(n, 2\delta, k) \leqslant \left\lfloor \frac{q^n-1}{q^k-1} \left\lfloor \frac{q^{n-1}-1}{q^{k-1}-1} \cdots \left\lfloor \frac{q^{n-k+\delta}-1}{q^\delta-1} \right\rfloor \cdots \right\rfloor \right\rfloor$$

Theorem 6 was also proved by Xia and Fu [36]. Notice that if one ignores all the floors in Theorem 6, one recovers precisely the upper bound of Theorem 3. Hence, Theorem 6 is always at least as strong (and usually stronger) as Theorems 1, 2, and 3.

We conclude this section with upper and lower bounds on $\mathcal{A}_q(n,d)$. The counterpart of the well-known Gilbert-Varshamov bound for codes in $\mathcal{G}_q(n,k)$ was proved by Koetter and Kschischang [20]. Generalizing this bound to codes in $\mathcal{P}_q(n)$ is nontrivial, since spheres of the same radius in $\mathcal{P}_q(n)$ have different sizes. We begin with the following lemma.

Lemma 7: Define a sphere of radius r about a point $X \in \mathcal{P}_q(n)$ in the usual way

$$\mathcal{S}_r(X) \stackrel{\text{def}}{=} \big\{ Y \in \mathcal{P}_q(n) \,:\, d(X,Y) \leqslant r \big\}.$$

[2]An alternative proof of Theorem 5 will be given in Section III.

Let $c(j,k,r)$ denote the number of subspaces of dimension j in a sphere of radius r about a k-dimensional subspace of $\mathbb{F}_q^n$. That is, $c(j,k,r) = |\mathcal{S}_r(X) \cap \mathcal{G}_q(n,j)|$ for all $X \in \mathcal{G}_q(n,k)$. Then

$$c(j,k,r) = \sum_{i=\lceil \frac{k+j-r}{2} \rceil}^{\min\{j,k\}} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{(j-i)(k-i)}. \tag{8}$$

Proof: Given X in $\mathcal{G}_q(n,k)$, there are $\begin{bmatrix} k \\ i \end{bmatrix}$ ways to choose an i-dimensional subspace Z of X. For a fixed Z, assuming $i \leqslant j$, the number of subspaces $Y \in \mathcal{G}_q(n,j)$ such that $X \cap Y = Z$ is

$$\frac{(q^n - q^k)(q^n - q^{k+1}) \cdots (q^n - q^{k+j-i-1})}{(q^j - q^i)(q^j - q^{i+1}) \cdots (q^j - q^{j-1})} = \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{(j-i)(k-i)}.$$

Finally, $d(X,Y) \leqslant r$ if and only if $2i \geqslant k+j-r$, and the lemma immediately follows. ∎

Using (8), we can compute the size of the sphere of radius r about a point $X \in \mathcal{G}_q(n,k)$. Note that this is different from the size of the sphere computed by Koetter and Kschischang [20], since the latter is restricted to a Grassmannian. In fact, what is computed in [20, Theorem 6] is $|\mathcal{S}_r(X) \cap \mathcal{G}_q(n,k)| = c(k,k,r)$ (or $|S(V,\ell,t)| = c(\ell,\ell,2t)$, if we use their notation). In what follows, we set $\begin{bmatrix} k \\ i \end{bmatrix} = 0$ by convention, for $i \notin \{0,1,\ldots,k\}$.

Lemma 8: For all $X \in \mathcal{P}_q(n)$ with $\dim X = k$, we have

$$|\mathcal{S}_r(X)| = \mathcal{S}_{k,r} \stackrel{\text{def}}{=} \sum_{j=0}^{r} \sum_{i=0}^{j} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{i(j-i)}. \tag{9}$$

Proof: Since $|\mathcal{S}_r(X)| = \sum_{j=0}^{n} c(j,k,r)$, the lemma follows from (8) by substituting $j := j+k-2i$ and then $i := k-i$. ∎

We are now ready to prove the counterpart of the Gilbert-Varshamov bound in projective space.

Theorem 9:

$$\mathcal{A}_q(n,d) \geqslant \frac{\sum_{k=0}^{n} \sum_{j=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} n \\ j \end{bmatrix}}{\sum_{k=0}^{n} \sum_{j=0}^{d-1} \sum_{i=0}^{j} \begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{i(j-i)}}.$$

Proof: The main tool we use is the work of Tolhuizen [33], which extends the Gilbert-Varshamov bound to graphs that are not necessarily distance-regular. Specifically, [33] establishes the following intuitive, but not obvious, result: if $\overline{\mathcal{S}}_r$ is the *average size* of a sphere of radius r in a graph $G = (V,E)$, then there exists a code $\mathcal{C}$ in G with minimum (graph) distance d and $|\mathcal{C}| \geqslant |V| / \overline{\mathcal{S}}_{d-1}$. In the case of $\mathcal{P}_q(n)$, we have

$$\overline{\mathcal{S}}_{d-1} = \frac{\sum_{X \in \mathcal{P}_q(n)} |\mathcal{S}_{d-1}(X)|}{|\mathcal{P}_q(n)|} = \frac{1}{|\mathcal{P}_q(n)|} \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} \mathcal{S}_{k,d-1}$$

as the average size of a sphere of radius $d-1$ in the relevant graph. The theorem now follows immediately from (9). ∎

Our next result employs linear programming to establish an upper bound on $\mathcal{A}_q(n,d)$. Given a code $\mathbb{C}$ in $\mathcal{P}_q(n)$, we let $D_0, D_1, \ldots, D_n$ denote its *dimension distribution*. Specifically, $D_k = |\mathbb{C} \cap \mathcal{G}_q(n,k)|$ for $k = 0,1,\ldots,n$. Set $D_k = 0$ by convention, for $k \notin \{0,1,\ldots,n\}$.

Theorem 10: Let $f^* = \max \sum_{k=0}^{n} D_k$, subject to the $2n+2$ linear constraints

$$D_k \leqslant \mathcal{A}_q(n, 2e+2, k) \quad \text{for } k = 0,1,\ldots,n \tag{10}$$

$$\sum_{i=-e}^{e} c(k,k+i,e) D_{k+i} \leqslant \begin{bmatrix} n \\ k \end{bmatrix} \quad \text{for } k = 0,1,\ldots,n \tag{11}$$

where the coefficients $c(k,k+i,e)$ in (11) are as defined in (8). Then f^* is an upper bound on $\mathcal{A}_q(n,2e+1)$.

Proof: Both (10) and (11) are constraints on the dimension distribution of an $(n, M, 2e+1)$ code $\mathbb{C}$ in $\mathcal{P}_q(n)$. Constraint (10) is obvious. To prove (11), note that spheres of radius e about the codewords of $\mathbb{C}$ are disjoint. Thus (11) counts the number of points of $\mathcal{G}_q(n,k)$ contained in such spheres. ∎

A bound analogous to Theorem 10 in the Hamming space is well known. However, there are several differences. For example, Theorem 10 applies in both binary and nonbinary projective space, whereas for the Hamming space, the corresponding bounds differ: codes in $\mathcal{G}_q(n,k)$ have even distance for all q, while in the Hamming space this is true only for $q = 2$. In the binary Hamming space, we can invoke the analogue of Theorem 10 also in the case of even distance, via the well-known relation $A_2(n,2e+2) = A_2(n-1,2e+1)$. However, this is not possible in projective space, since the analogous relation does not hold. For example, $\mathcal{A}_2(6,4) \geqslant 77$ as shown in [21], but $\mathcal{A}_2(5,3) = 18$ as we shall see in the next section.

III. Constructions of Codes

It is well known that optimal codes in the Johnson space can be constructed from Steiner systems. We observe that a completely analogous construction can be carried out in projective space. A ***Steiner structure*** $\mathcal{S}_q(t,k,n)$ is a set $\mathcal{S}$ of k-dimensional subspaces of $\mathbb{F}_q^n$ such that each t-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly one element of $\mathcal{S}$. It can be easily shown that any Steiner structure $\mathcal{S}_q(t,k,n)$ is an (n,M,d,k) code in $\mathcal{G}_q(n,k)$ with $M = \begin{bmatrix} n \\ t \end{bmatrix} / \begin{bmatrix} k \\ t \end{bmatrix}$ and $d = 2(k-t+1)$. Furthermore, any such code attains the upper bound of Theorem 2.

Steiner structures were introduced and studied in [26], [31], [32], where it is proved that they exist only if $\begin{bmatrix} k-i \\ t-i \end{bmatrix}$ divides $\begin{bmatrix} n-i \\ t-i \end{bmatrix}$ for all $i = 0,1,\ldots,t$. For $t = 1$, this reduces to the simple condition that k divides n and the Steiner structure $\mathcal{S}_q(1,k,n)$ is known as a *spread*. Such spreads were studied in many papers [6], [10], [26], [31]. In particular, Schwartz and Etzion [26] construct a Steiner structure $\mathcal{S}_q(1,k,n)$, for all q, whenever k divides n. In view of the foregoing discussion, this immediately implies

$$\mathcal{A}_q(n,2k,k) = \frac{q^n - 1}{q^k - 1} \quad \text{whenever } k \mid n. \tag{12}$$

Herein, we extend the results of [6], [10], and [26] to the case where k does *not* divide n. Our construction is summarized in the following theorem, which includes (12) as a special case.

Theorem 11: Let $n \equiv r \pmod{k}$. Then, for all q, we have

$$\mathcal{A}_q(n, 2k, k) \geqslant \frac{q^n - q^k(q^r - 1) - 1}{q^k - 1}. \tag{13}$$

Proof: Let r be the remainder obtained when k is divided into n, and define $m = k + r$. Henceforth, we will represent the vectors in $\mathbb{F}_q^n$ as follows:

$$\mathbb{F}_q^n = \left\{(x, y) \,:\, x \in \mathrm{GF}(q^{n-m}), y \in \mathrm{GF}(q^m)\right\}$$

Let α be a primitive element of $\mathrm{GF}(q^{n-m})$, and let β be a primitive element of $\mathrm{GF}(q^m)$. Further, let

$$W = \left\langle (0, \beta^0), (0, \beta^1), \ldots, (0, \beta^{k-1}) \right\rangle. \tag{14}$$

Since $\beta^0, \beta^1, \ldots, \beta^{m-1}$ are independent over $\mathbb{F}_q$ and $m \geqslant k$, we see that $\dim W = k$. Next, define $t = (q^{n-m} - 1)/(q^k - 1)$, which is an integer since k divides $n - m$ by our choice of m. Let $\gamma = \alpha^t$. Then the multiplicative order of γ in $\mathrm{GF}(q^{n-m})$ is $q^k - 1$, and therefore γ is a primitive element of $\mathrm{GF}(q^k)$, as a subfield of $\mathrm{GF}(q^{n-m})$. This implies that $1, \gamma, \gamma^2, \ldots, \gamma^{k-1}$ form a basis for $\mathrm{GF}(q^k)$ over $\mathbb{F}_q$, and hence are linearly independent over $\mathbb{F}_q$. Now, consider the $t + t(q^m - 1)$ subspaces of $\mathbb{F}_q^n$ that are given by

$$U_i = \left\langle (\alpha^i, 0), (\alpha^i\gamma, 0), \ldots, (\alpha^i\gamma^{k-1}, 0) \right\rangle \tag{15}$$

$$V_{i,j} = \left\langle (\alpha^i, \beta^j), (\alpha^i\gamma, \beta^{j+1}), \ldots, (\alpha^i\gamma^{k-1}, \beta^{j+k-1}) \right\rangle \tag{16}$$

where i ranges over $\{0, 1, \ldots, t-1\}$ and, for each i, j ranges over $\{0, 1, \ldots, q^m - 2\}$. Since $1, \gamma, \gamma^2, \ldots, \gamma^{k-1}$ are independent over $\mathbb{F}_q$, it is easy to see that $\dim U_i = \dim V_{i,j} = k$ for all i and j. We construct the code $\mathbb{C}$ as follows:

$$\mathbb{C} = \left(\bigcup_i U_i\right) \cup \left(\bigcup_{i,j} V_{i,j}\right) \cup W.$$

Observe that $\mathbb{C}$ has the requisite number of codewords, since $t + t(q^m - 1) + 1$ evaluates to the right-hand side of (13) for our choice of m and t. Hence, in order to complete the proof, it remains to show that the minimum distance of $\mathbb{C}$ is $2k$. Since $\mathbb{C} \subset \mathcal{G}_q(n, k)$, this means we must show that for all distinct $X, Y \in \mathbb{C}$, we have $X \cap Y = \{\mathbf{0}\}$. First, observe that for any nonzero vector (x, y) in $\mathbb{F}_q^n$, we have

$$\begin{aligned} (x, y) \in W &\;\Rightarrow\; x = \mathbf{0}, y \neq \mathbf{0} \\ (x, y) \in U_i &\;\Rightarrow\; x \neq \mathbf{0}, y = \mathbf{0} \\ (x, y) \in V_{i,j} &\;\Rightarrow\; x \neq \mathbf{0}, y \neq \mathbf{0} \end{aligned}$$

since both $\alpha^i, \alpha^i\gamma, \ldots, \alpha^i\gamma^{k-1}$ and $\beta^j, \beta^{j+1}, \ldots, \beta^{j+k-1}$ are linearly independent over $\mathbb{F}_q$, for all i and j. It follows that

$$W \cap U_i = W \cap V_{i,j} = U_i \cap V_{i,j} = \{\mathbf{0}\} \quad \text{for all } i, j.$$

Next, observe that the t vector spaces $U_0, U_1, \ldots, U_{t-1}$ form a spread in $\mathbb{F}_q^{n-m}$. This fact is well-known, see [6], [26] for a detailed proof. Therefore, $U_{i_1} \cap U_{i_2} = \{\mathbf{0}\}$ for all $i_1 \neq i_2$. For the same reason, $V_{i_1,j_1} \cap V_{i_2,j_2} = \{\mathbf{0}\}$ for all j_1 and j_2, whenever $i_1 \neq i_2$. It remains to prove that $V_{i,j_1} \cap V_{i,j_2} = \{\mathbf{0}\}$ for every fixed i and all $j_1 \neq j_2$. Assume to the contrary that (x, y) is a nonzero vector in $V_{i,j_1} \cap V_{i,j_2}$, and consider the corresponding linear combinations of the basis vectors in (16), namely

$$\begin{aligned} x &= a_0\alpha^i + a_1\alpha^i\gamma + \cdots + a_{k-1}\alpha^i\gamma^{k-1} \\ &= b_0\alpha^i + b_1\alpha^i\gamma + \cdots + b_{k-1}\alpha^i\gamma^{k-1} \end{aligned} \tag{17}$$

$$\begin{aligned} y &= a_0\beta^{j_1} + a_1\beta^{j_1+1} + \cdots + a_{k-1}\beta^{j_1+k-1} \\ &= b_0\beta^{j_2} + b_1\beta^{j_2+1} + \cdots + b_{k-1}\beta^{j_2+k-1}. \end{aligned} \tag{18}$$

Since $1, \gamma, \gamma^2, \ldots, \gamma^{k-1}$ are linearly independent over $\mathbb{F}_q$, (17) implies that $b_\ell = a_\ell$ for all ℓ. Hence, we can rewrite (18) as follows:

$$(\beta^{j_1} - \beta^{j_2})(a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{k-1}\beta^{k-1}) = 0.$$

But since $1, \beta, \beta^2, \ldots, \beta^{k-1}$ are also independent over $\mathbb{F}_q$, this implies that $\beta^{j_1} = \beta^{j_2}$, and hence $j_1 = j_2$, a contradiction. ∎

For a code $\mathbb{C}$ in $\mathcal{P}_q(n)$, the *orthogonal complement* of $\mathbb{C}$ can be defined as follows: $\mathbb{C}^\perp = \{V^\perp : V \in \mathbb{C}\}$. Such orthogonal complements were first considered in [20] and [36] in the context of codes in $\mathcal{G}_q(n, k)$. Here, we extend these results to $\mathcal{P}_q(n)$ and provide formal proofs, which were not given in [20] and [36].

Lemma 12: Let U, V be two arbitrary elements of $\mathcal{P}_q(n)$. Then

$$\dim(U^\perp \cap V^\perp) \;=\; n - \dim U - \dim V + \dim(U \cap V).$$

Proof: We claim that $U^\perp \cap V^\perp = (U + V)^\perp$. Indeed, suppose that $x \in U^\perp \cap V^\perp$, that is $\langle x, u\rangle = 0$ for all $u \in U$ and $\langle x, v\rangle = 0$ for all $v \in V$. Then $\langle x, \alpha u + \beta v\rangle = 0$ for all scalars $\alpha, \beta \in \mathbb{F}_q$, and therefore x is orthogonal to $U + V$. In the other direction, if x is orthogonal to $U + V$ then it is also orthogonal to U and to V, since U, V are subspaces of $U + V$. The lemma now follows from the claim along with the fact that $\dim(U + V)^\perp = n - \dim(U + V)$. ∎

Lemma 13: If $\mathbb{C}$ is an (n, M, d) code in $\mathcal{P}_q(n)$, then its orthogonal complement $\mathbb{C}^\perp$ is also an (n, M, d) code.

Proof: Let U and V be two arbitrary elements of $\mathbb{C}$, with $\dim U = i$ and $\dim V = j$. Further let $U^\perp, V^\perp$ be the corresponding elements of $\mathbb{C}^\perp$. Then, by Lemma 12, we have

$$\begin{aligned} &d\big(U^\perp, V^\perp\big) \\ &\quad= \dim U^\perp + \dim V^\perp - 2\dim(U^\perp \cap V^\perp) \\ &\quad= (n - i) + (n - j) - 2(n - i - j + \dim(U \cap V)) \\ &\quad= i + j - 2\dim(U \cap V) = d(U, V). \end{aligned}$$

Consequently, $\mathbb{C}$ and $\mathbb{C}^\perp$ have the same distance distribution and, in particular, the same minimum distance. ∎

Lemma 13 readily leads to an alternative proof of Theorem 5 of the previous section. Indeed, it follows from Lemma 13 that $\mathcal{A}_q(n, 2\delta, k) = \mathcal{A}_q(n, 2\delta, n - k)$, and by Theorem 4 we have

$$\mathcal{A}_q(n, 2\delta, n - k) \leqslant \frac{q^n - 1}{q^{n-k} - 1}\mathcal{A}_q(n - 1, 2\delta, n - k - 1).$$

But $\mathcal{A}_q(n-1, 2\delta, n-k-1) = \mathcal{A}_q(n-1, 2\delta, k)$, again by Lemma 13, and Theorem 5 follows.

In the remainder of this section, we present several specific examples of codes in $\mathcal{P}_q(n)$. All these codes are either optimal

or close to optimal. First, consider the code $\mathbb{C} \subset \mathcal{P}_2(5)$ which consists of the column spaces of the following 18 matrices:

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

It can be verified by inspection that the minimum distance of $\mathbb{C}$ is 3. Thus $\mathbb{C}$ is a $(5, 18, 3)$ binary projective-space code. The following theorem shows that $\mathbb{C}$ is optimal.

Theorem 14: $\mathcal{A}_2(5, 3) = 18$.

Proof: Let $\mathbb{C}$ be a $(5, M, 3)$ projective-space code over $\mathbb{F}_2$ with dimension distribution $D_0, D_1, \ldots, D_5$. It follows from Lemma 15 (proved, independently, in Section IV) that $D_2 \leqslant 9$, and it is obvious that $D_4 \leqslant 1$. Hence, $D_2 + D_4 \leqslant 10$. We will prove next that, in fact, $D_2 + D_4 \leqslant 9$. Assume to the contrary that $\mathbb{C} \cap \mathcal{G}_2(5, 4) = \{X\}$ and

$$\mathbb{C}_2 \stackrel{\text{def}}{=} \mathbb{C} \cap \mathcal{G}_2(5, 2) = \{V_1, V_2, \ldots, V_9\}.$$

Let $U = V_1 \cup V_2 \cup \cdots \cup V_9$. Since the minimum distance of $\mathbb{C}_2$ is 4, we must have $V_i \cap V_j = \{\mathbf{0}\}$ for all $V_i, V_j \in \mathbb{C}_2$. Hence $|U| = 1 + 9{\cdot}3 = 28$. Now, let us count the number of vectors in $U \cap X$. Since the minimum distance of $\mathbb{C}$ is 3, we have $\dim(V_i \cap X) = 1$ for all $V_i \in \mathbb{C}_2$. Thus $|U \cap X| = 1{+}9 = 10$. It follows that $28 - 10 = 18$ different vectors in U lie outside of X. This is a contradiction since $|\mathbb{F}_2^5 \setminus X| = 16$.

The fact that $D_2 + D_4 \leqslant 9$ in conjunction with Lemma 13 implies that $D_3 + D_1 \leqslant 9$. Adding these two constraints to the equation system of Theorem 10, we find that $\mathcal{A}_2(5, 3) \leqslant 18$. ■

Let α be a primitive element of $\mathrm{GF}(2^n)$. We say that a code $\mathbb{C} \subseteq \mathcal{P}_2(n)$ is ***cyclic*** if it has the following property: whenever $\{\mathbf{0}, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_m}\}$ is a codeword of $\mathbb{C}$, so is its cyclic shift $\{\mathbf{0}, \alpha^{i_1+1}, \alpha^{i_2+1}, \ldots, \alpha^{i_m+1}\}$. In other words, if we map each vector space $V \in \mathbb{C}$ into the corresponding binary characteristic vector $x_V = (x_0, x_1, \ldots, x_{2^n-2})$ given by

$$x_i = 1 \text{ if } \alpha^i \in V \quad \text{and} \quad x_i = 0 \text{ if } \alpha^i \notin V$$

then the set of all such characteristic vectors is closed under cyclic shifts. Note that the property of being cyclic does *not* depend on the choice of a primitive element α in $\mathrm{GF}(2^n)$. Moreover, cyclic codes have a number of useful properties. Using these properties, we have developed computational methods to search for cyclic codes in projective space. Several examples of interesting codes found in this manner follow.

Example 1: Let α be a root of $x^6{+}x{+}1$, and use this primitive polynomial to generate $\mathrm{GF}(2^6)$. Consider the code $\mathbb{C}$ in $\mathcal{G}_2(6, 3)$ which consists of all the cyclic shifts of

$$\{\alpha^0, \alpha^1, \alpha^4, \alpha^6, \alpha^{16}, \alpha^{24}, \alpha^{33}\}.$$

Note that here, and hereafter, we omit the $\mathbf{0}$ vector when specifying codewords of cyclic projective-space codes. It can be verified that $\mathbb{C}$ is a $(6, 63, 4, 3)$ code; therefore $\mathcal{A}_2(6, 4, 3) \geqslant 63$. On the other hand, it follows from Lemma 15 along with Theorems 4 and 5 that $\mathcal{A}_2(6, 4, 3) \leqslant 81$. Adjoining the codewords $\mathbb{F}_2^{63}$ and $\{\alpha^0, \alpha^{21}, \alpha^{42}\}$, along with all its cyclic shifts, to $\mathbb{C}$, we obtain a $(6, 85, 3)$ cyclic code $\mathbb{C}'$ in $\mathcal{P}_2(6)$. On the other hand, $\mathcal{A}_2(6, 3) \leqslant 123$ by Theorem 10.

We note that both $\mathbb{C}$ and $\mathbb{C}'$ are optimal among cyclic codes: there is no cyclic code in $\mathcal{G}_2(6, 3)$, respectively $\mathcal{P}_2(6)$, of distance ≥ 3 and size greater than 63, respectively 85.

Example 2: Let α be a root of $x^8 + x^7 + x^2 + x + 1$, and use this primitive polynomial to construct $\mathrm{GF}(2^8)$. Consider the code $\mathbb{C} \subset \mathcal{G}_2(8, 3)$ which consists of all the cyclic shifts of

$$\{\alpha^0, \alpha^1, \alpha^{18}, \alpha^{33}, \alpha^{69}, \alpha^{99}, \alpha^{109}\}$$
$$\{\alpha^0, \alpha^2, \alpha^{58}, \alpha^{135}, \alpha^{163}, \alpha^{198}, \alpha^{246}\}$$
$$\{\alpha^0, \alpha^3, \alpha^{22}, \alpha^{82}, \alpha^{134}, \alpha^{205}, \alpha^{250}\}$$
$$\{\alpha^0, \alpha^4, \alpha^{24}, \alpha^{97}, \alpha^{104}, \alpha^{110}, \alpha^{141}\}$$
$$\{\alpha^0, \alpha^{12}, \alpha^{41}, \alpha^{55}, \alpha^{102}, \alpha^{125}, \alpha^{221}\}.$$

It can be verified that $\mathbb{C}$ is an $(8, 1275, 4, 3)$ code, and therefore $\mathcal{A}_2(8, 4, 3) \geqslant 1275$. On the other hand, in view of Lemma 15 and Theorem 4, we have $\mathcal{A}_2(8, 4, 3) \leqslant 1493$. We note that $\mathbb{C}$ is optimal among cyclic codes.

Example 3: Let α be a root of $x^9 + x^4 + 1$, and use this primitive polynomial to construct $\mathrm{GF}(2^9)$. Consider the code $\mathbb{C}$ in $\mathcal{G}_2(9, 3)$ which consists of all the cyclic shifts of

$$\{\alpha^0, \alpha^1, \alpha^{27}, \alpha^{130}, \alpha^{142}, \alpha^{185}, \alpha^{277}\}$$
$$\{\alpha^0, \alpha^2, \alpha^{207}, \alpha^{228}, \alpha^{260}, \alpha^{300}, \alpha^{432}\}$$
$$\{\alpha^0, \alpha^3, \alpha^{99}, \alpha^{157}, \alpha^{220}, \alpha^{244}, \alpha^{420}\}$$
$$\{\alpha^0, \alpha^4, \alpha^9, \alpha^{51}, \alpha^{110}, \alpha^{305}, \alpha^{454}\}$$
$$\{\alpha^0, \alpha^6, \alpha^{60}, \alpha^{131}, \alpha^{290}, \alpha^{329}, \alpha^{504}\}$$
$$\{\alpha^0, \alpha^8, \alpha^{18}, \alpha^{170}, \alpha^{187}, \alpha^{255}, \alpha^{320}\}$$
$$\{\alpha^0, \alpha^{11}, \alpha^{139}, \alpha^{177}, \alpha^{299}, \alpha^{333}, \alpha^{470}\}$$
$$\{\alpha^0, \alpha^{14}, \alpha^{98}, \alpha^{114}, \alpha^{134}, \alpha^{216}, \alpha^{238}\}$$
$$\{\alpha^0, \alpha^{15}, \alpha^{48}, \alpha^{77}, \alpha^{126}, \alpha^{196}, \alpha^{476}\}$$
$$\{\alpha^0, \alpha^{19}, \alpha^{155}, \alpha^{192}, \alpha^{278}, \alpha^{308}, \alpha^{421}\}$$
$$\{\alpha^0, \alpha^{23}, \alpha^{69}, \alpha^{97}, \alpha^{186}, \alpha^{262}, \alpha^{337}\}$$
$$\{\alpha^0, \alpha^{73}, \alpha^{146}, \alpha^{219}, \alpha^{292}, \alpha^{365}, \alpha^{438}\}.$$

It can be verified that $\mathbb{C}$ is a $(9, 5694, 4, 3)$ code, and therefore $\mathcal{A}_2(9, 4, 3) \geqslant 5694$. On the other hand, $\mathcal{A}_2(9, 4, 3) \leqslant 6205$ by Theorem 1. We note that $\mathbb{C}$ is optimal among cyclic codes.

IV. Nonexistence of Nontrivial Perfect Codes

The study of perfect codes is one of the most fascinating topics of research in coding theory. Given any metric space $\mathcal{S}$, a code $\mathbb{C} \subseteq \mathcal{S}$ is said to be *e-perfect* if (closed) spheres of radius e centered at the codewords both pack and cover $\mathcal{S}$; in other words, every element of $\mathcal{S}$ is contained in one and only one such sphere. A finite metric space $\mathcal{S}$ always admits two trivial perfect codes: the whole space is 0-perfect, and any single element $x \in \mathcal{S}$ is n-perfect, where $n = \max_{y \in \mathcal{S}} d(x,y)$. The binary Hamming space, the Johnson space $\mathcal{J}(2n,n)$, and the projective space $\mathcal{P}_q(n)$, but not the Grassmannians, also admit a third type of a trivial perfect code when $n = 2e+1$ is odd. In the case of $\mathcal{P}_q(n)$, it consists of the null-space $\{\mathbf{0}\}$ and $\mathbb{F}_q^n$.

It is well known [7], [24] that for all q, n, and k, there are no nontrivial perfect codes in the Grassmannian $\mathcal{G}_q(n,k)$. But this does not rule out perfect codes in $\mathcal{P}_q(n)$, just like the (conjectured) nonexistence of nontrivial perfect codes in the Johnson space does not rule out nontrivial perfect codes in the Hamming space. Our main result in this section is a self-contained proof of the *nonexistence of nontrivial perfect codes in* $\mathcal{P}_q(n)$. Note that since $\mathcal{P}_q(n)$ is not distance-regular, standard methods (based upon association schemes) do not apply, and our proof employs completely different techniques. We will first need the following lemma (note that related results in [9] and [10] are weaker, and do not imply this lemma).

Lemma 15:

$$\mathcal{A}_q(n,2k,k) \leqslant \left\lfloor \frac{q^n-1}{q^k-1} \right\rfloor - 1 \quad \text{if } n \not\equiv 0 \pmod{k}$$

Proof: Divide k into n to write $n = mk + r$, where the remainder r is nonzero by assumption. It is easy to verify that

$$q^n - 1 = q^r \left(q^{(m-1)k} + \cdots + q^k + 1 \right) (q^k - 1) + (q^r - 1). \quad (19)$$

Now assume to the contrary that there exists an $(n, M, 2k, k)$ code $\mathbb{C}$ in $\mathcal{G}_q(n,k)$ with $M = \lfloor (q^n-1)/(q^k-1) \rfloor$. Further, let $V_1, V_2, \ldots, V_M$ denote the codewords of $\mathbb{C}$, and observe that $V_i \cap V_j = \{\mathbf{0}\}$ for all $i \neq j$. Hence, we can partition $\mathbb{F}_q^n \setminus \{\mathbf{0}\}$ into $M+1$ disjoint sets as follows:

$$\mathbb{F}_q^n \setminus \{\mathbf{0}\} \;=\; V_1^* \cup V_2^* \cup \cdots \cup V_M^* \cup X \quad (20)$$

where $V_i^* = V_i \setminus \{\mathbf{0}\}$ for all i, and X denotes the set of all vectors in $\mathbb{F}_q^n$ that are not contained in any codeword of $\mathbb{C}$. Thus

$$|X| = (q^n - 1) - M(q^k - 1) = q^r - 1$$

in view of (19) and (20). Given a fixed nonzero vector $u \in \mathbb{F}_q^n$ and a set $\mathcal{S} \subseteq \mathbb{F}_q^n$, let $\eta_u(\mathcal{S})$ denote the number of vectors in $\mathcal{S}$ that are *not* orthogonal to u, that is

$$\eta_u(\mathcal{S}) \stackrel{\text{def}}{=} \left| \{ x \in \mathcal{S} : \langle x, u \rangle \neq 0 \} \right|$$

where the inner product is over $\mathbb{F}_q$. Note that $\eta_u(V_i^*) = \eta_u(V_i)$ is either 0 or $(q-1)q^{k-1}$ for all i, since V_i is a vector space of dimension k. Also note that $\eta_u(\mathbb{F}_q^n) = (q-1)q^{n-1}$. Hence

$$\eta_u(X) = \eta_u \left(\mathbb{F}_q^n \setminus \{\mathbf{0}\} \right) - \sum_{i=1}^{M} \eta_u(V_i^*) \quad (21)$$

is divisible by q^{k-1}. But $|X| = q^r - 1 < q^{k-1}$, which implies that $\eta_u(X) = 0$. Since this is true for *all* nonzero $u \in \mathbb{F}_q^n$, the set X cannot contain any nonzero vectors, a contradiction. ∎

Theorem 16: For all q and n, there are no nontrivial perfect codes in the projective space $\mathcal{P}_q(n)$.

Proof: Let us assume to the contrary that $\mathbb{C}$ is an e-perfect code in $\mathcal{P}_q(n)$. Let $d = 2e+1$, and define $\mathbb{C}_k \stackrel{\text{def}}{=} \mathbb{C} \cap \mathcal{G}_q(n,k)$ for all $k = 0, 1, \ldots, n$. We distinguish between two cases.

Case 1. $\{\mathbf{0}\} \in \mathbb{C}$

Here, we have $\mathbb{C}_1 = \mathbb{C}_2 = \cdots = \mathbb{C}_{2e} = \varnothing$, and all the points in $\mathcal{G}_q(n, e+1)$ must be covered by the codewords of $\mathbb{C}_d$. This implies that $\mathbb{C}_d$ is a Steiner structure $\mathcal{S}_q(e+1, d, n)$ and hence $|\mathbb{C}_d| = \begin{bmatrix} n \\ e+1 \end{bmatrix} / \begin{bmatrix} d \\ e+1 \end{bmatrix}$. Each subspace of $\mathbb{C}_d$ covers $\begin{bmatrix} d \\ e+2 \end{bmatrix}$ points in $\mathcal{G}_q(n, e+2)$. This leaves $\begin{bmatrix} n \\ e+2 \end{bmatrix} - |\mathbb{C}_d| \begin{bmatrix} d \\ e+2 \end{bmatrix}$ points in $\mathcal{G}_q(n, e+2)$ uncovered, and each of them must be covered by a codeword of $\mathbb{C}_{d+1}$. Furthermore, each codeword of $\mathbb{C}_{d+1}$ covers exactly $\begin{bmatrix} d+1 \\ e+2 \end{bmatrix}$ points in $\mathcal{G}_q(n, e+2)$. Putting all this together, we see that

$$|\mathbb{C}_{d+1}| = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-e}-1)}{(q^{d+1}-1)(q^d-1)\cdots(q^{e+1}-1)} (q^{n-e-1} - q^e).$$

Observe that $\mathcal{A}_q(n, d+1, d+1) \geqslant |\mathbb{C}_{d+1}|$. Starting with this, and applying Theorem 4 iteratively $e+1$ times, we obtain

$$\mathcal{A}_q(m, 2k, k) \geqslant \frac{q^m - q^{k-1}}{q^k - 1} \quad (22)$$

for $m = n - (e+1)$ and $k = e+1$. Moreover, the fact that $\mathbb{C}_d$ is a Steiner structure $\mathcal{S}_q(e+1, d, n)$ implies that $e+1$ divides $n - e = m + 1$. This further implies that

$$\frac{q^m - q^{k-1}}{q^k - 1} = q^{m-k} + q^{m-2k} + \cdots + q^{k-1} = \left\lfloor \frac{q^m - 1}{q^k - 1} \right\rfloor$$

Also, since $k = e+1$ divides $m+1$, it cannot divide m. This finally establishes a contradiction between (22) and Lemma 15.

Case 2. $\{\mathbf{0}\} \notin \mathbb{C}$

Our proof for this case is based upon constructing a certain partition of $\mathbb{F}_q^n$, and then applying a counting argument to this partition in order to arrive at a contradiction. For the counting argument, let us introduce a function η from subsets of $\mathbb{F}_q^n$ to the natural numbers, defined as follows: given a set $\mathcal{S} \subseteq \mathbb{F}_q^n$, let $\eta(\mathcal{S})$ denote the number of vectors $(x_1, x_2, \ldots, x_n)$ in $\mathcal{S}$ such that $x_1 = 1$. Note that if $\mathcal{S}$ is a vector space of dimension i and $\eta(\mathcal{S}) \neq 0$, then $\eta(\mathcal{S}) = q^{i-1}$. Now let $X \in \mathbb{C}$ be a vector space of the smallest dimension among all the vector spaces in $\mathbb{C}$. Since $X \neq \{\mathbf{0}\}$, we can assume w.l.o.g. that $\eta(X) \neq 0$ (otherwise, permute the coordinates of the ambient space $\mathbb{F}_q^n$ so that X is not entirely zero on the first position). The partition of $\mathbb{F}_q^n$ is constructed as follows. Let $k = \dim X$. Since X must cover the null-space $\{\mathbf{0}\}$, we have $k \leqslant e$. Find a vector space V in $\mathcal{P}_q(n)$ which satisfies the following conditions:

$$\dim V = e - k, \quad X \cap V = \{\mathbf{0}\}, \quad \eta(V) = 0. \quad (23)$$

It is easy to see that such a vector space V always exists. Next, define $W = X \oplus V$. In view of (23), we have $\dim W = e$, and

since $\eta(X) \neq 0$ this implies that $\eta(W) = q^{e-1}$. Finally, define a subcode $\mathbb{C}'$ of $\mathbb{C}$ as follows:

$$\mathbb{C}' \stackrel{\text{def}}{=} \big\{Y \in \mathbb{C} : V \subset Y \text{ and } \dim Y = d-k\big\}. \tag{24}$$

Suppose that $\mathbb{C}'$ contains M codewords $Y_1, Y_2, \ldots, Y_M$ (we shall see later on that $M = q^k(q^{n-e}-1)/(q^{e+1}-1)$, although this is not required for the proof). For all $i = 1, 2, \ldots, M$, let $Y_i^* = Y_i \setminus V$. The partition of $\mathbb{F}_q^n$ we have in mind is as follows:

$$\mathbb{F}_q^n \;=\; Y_1^* \cup Y_2^* \cup \cdots \cup Y_M^* \cup W. \tag{25}$$

Assuming that (25) is, indeed, a partition of $\mathbb{F}_q^n$, we easily arrive at a contradiction. Since $\dim Y_i = d-k$ and $\eta(V) = 0$, we find that $\eta(Y_i^*) = \eta(Y_i)$ is either 0 or $q^{d-k-1} = q^{2e-k}$ for all i. Also $\eta(\mathbb{F}_q^n) = q^{n-1}$ and therefore

$$\eta(W) = \eta\left(\mathbb{F}_q^n\right) - \sum_{i=1}^{M} \eta(Y_i^*) \tag{26}$$

must be divisible by q^{2e-k}. This is a contradiction, since we have already shown that $\eta(W) = q^{e-1}$, but $e-1 < 2e-k$ for all $k \leqslant e$. To complete the proof, it remains to establish (25).

Claim 1: Let u be a vector of $\mathbb{F}_q^n$ that lies outside of W. Then there exists a $Y_i \in \mathbb{C}'$ such that $u \in Y_i$.

Proof: Let $U = V \oplus \{\mathbf{0}, u\}$. Then U is a vector space of dimension $e-k+1$ that must be covered by some codeword Y of $\mathbb{C}$. This codeword is not X since $U \cap X = \{\mathbf{0}\}$, and so

$$d(X,U) = \dim X + \dim U = k + (e-k+1) = e+1.$$

Since X and Y are (distinct) codewords of $\mathbb{C}$, we must have $d(X,Y) \geqslant d$ which implies that $\dim Y \geqslant d-k$. Now, from the fact that Y covers U, we obtain

$$d(U,Y) \;=\; \dim U + \dim Y - 2\dim(U \cap Y) \;\leqslant\; e. \tag{27}$$

Since $\dim Y \geqslant d-k$, the only way in which (27) can be satisfied is when $\dim Y = d-k$ and

$$\dim(U \cap Y) \;=\; \dim U \;=\; e-k+1. \tag{28}$$

But (28) implies that $V \subset U \subset Y$, and therefore $Y \in \mathbb{C}'$. Finally, $U \subset Y$ also implies that $u \in Y$, and we are done. □

If u lies outside of $W = X \oplus V$ and $u \in Y_i$, then clearly u must belong to $Y_i^* = Y_i \setminus V$. Hence, Claim 1 shows that the set union $Y_1^* \cup Y_2^* \cup \cdots \cup Y_M^* \cup W$ indeed contains all of $\mathbb{F}_q^n$.

Claim 2: The sets $Y_1^*, Y_2^*, \ldots, Y_M^*$ and W are disjoint.

Proof: Given any two codewords Y_i and Y_j in $\mathbb{C}'$, we have $d(Y_i, Y_j) = 2(d-k) - 2\dim(Y_i \cap Y_j) \geqslant d$. This implies that $\dim(Y_i \cap Y_j) \leqslant e-k = \dim V$ and therefore $Y_i \cap Y_j = V$. Consequently, the sets $Y_1^*, Y_2^*, \ldots, Y_M^*$ are disjoint.

Now assume to the contrary that there exists a nonzero vector y in the intersection $Y_i^* \cap W$ for some i. Then $y \in Y_i$, and $y = x + v$ for some nonzero $x \in X$ and some $v \in V$. But Y_i is a vector space which contains V as a subspace. Therefore Y_i also contains the vector $y - v = x$, and so $\dim(X \cap Y_i) \geqslant 1$. But this clearly contradicts the minimum distance of $\mathbb{C}$, since then $d(X, Y_i) = k + (d-k) - 2\dim(X \cap Y_i) \leqslant d-2$. □

Claim 2 completes the proof that (25) is, indeed, a partition of $\mathbb{F}_q^n$. This, in turn, completes our proof of the theorem. ■

V. Conclusions and Open Problems

We have considered several basic questions that arise in the framework of "coding theory in projective space." Many more questions remain unanswered. In particular, our work leads to a multitude of open problems in this area. We briefly mention below five specific problems that are directly related to the results compiled in this paper.

- Although Theorem 10 employs linear programming to establish a bound on $\mathcal{A}_q(n,d)$, this theorem is not related to Delsarte's inequalities [8] and the resulting linear-programming bounds in the Hamming and Johnson spaces. Unfortunately, direct extension of Delsarte's methods to $\mathcal{P}_q(n)$ is not possible, since $\mathcal{P}_q(n)$ is *not* an association scheme. Nevertheless, we ask whether a linear-programming bound stronger than Theorem 10 can be developed. In particular, can Delsarte's theory be extended to include the projective space? Some results along these lines have been reported by Bachoc [2]. Alternatively, can one add nontrivial constraints to the system of inequalities in (11)?
- We wonder whether the construction presented in Theorem 11 is, in fact, optimal. The problem is to either prove this or find $n \equiv r \pmod{k}$ and q, such that

$$\mathcal{A}_q(n, 2k, k) > \frac{q^n - q^k(q^r-1) - 1}{q^k - 1}$$

- While the cyclic codes constructed in Section III are optimal, our constructions make use of computational methods. They are thus limited to small values of n. Are there purely algebraic constructions of large cyclic codes, either in $\mathcal{G}(n,k)$ or in $\mathcal{P}_q(n)$? In particular, can useful bounds on the parameters of a cyclic code in $\mathcal{G}_2(n,k)$ be determined by analyzing relevant cyclotomic cosets?
- Although no (known) nontrivial perfect codes exist in the Johnson space and the Grassmann space, both spaces admit *diameter-perfect* codes [1]. All such diameter-perfect codes are optimal for their parameters. Unfortunately, the definition of diameter-perfect codes does not extend to the projective space $\mathcal{P}_q(n)$, since the size of a sphere in $\mathcal{P}_q(n)$ depends on its center. Can one define another type of perfect codes in projective space, so that certain optimal codes become "perfect" under this definition?
- In addition to perfect codes, equidistant codes are often of special interest. In other words, we ask: what is the largest code $\mathbb{C}$ in $\mathcal{G}_q(n,k)$ such that $\dim(X \cap Y) = k - \delta$ for all distinct X, Y in $\mathbb{C}$? Preliminary results on this can be obtained from our discussion in Section III, but the general answer seems to be related to extremal combinatorics.

Another interesting topic is the investigation of the fundamental concepts of "linear codes" and "complements" in the context of $\mathcal{P}_q(n)$. These turn out to be considerably more involved than their classical counterparts. For more on this, see [5], [11]. Finally, our work herein naturally leads to questions regarding the projective-space analogues of covering designs and Turán systems. Our results on this topic are presented in [12].

ACKNOWLEDGMENT

We acknowledge stimulating discussions on the subject matter of this paper with Ralf Koetter and Frank Kschischang.

REFERENCES

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

[2] C. Bachoc, "Semidefinite programming, harmonic analysis, and coding theory," Lecture Notes CIMPA Summer School on Semidefinite Programming in Algebraic Combinatorics pp. 1–47, Jul. 2009.

[3] H. Bahramgiri and F. Lahouti, "Block network error control codes and syndrome-based maximum likelihood decoding," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, ON, Canada, Jul. 2008.

[4] I. Bocharova, B. Kudryashov, M. Bossert, and V. Sidorenko, "Convolutional rank codes," *IEEE Trans. Inf. Theory*, submitted for publication.

[5] M. Braun, T. Etzion, and A. Vardy, "Linearity and complements in projective space," Aug. 2010, preprint.

[6] T. Bu, "Partitions of a vector space," *Discrete Math.*, vol. 31, pp. 79–83, Jan. 1980.

[7] L. Chihara, "On the zeros of the Askey-Wilson polynomials, with applications to coding theory," *SIAM J. Math. Anal.*, vol. 18, pp. 191–207, 1987.

[8] Ph. Delsarte, "An algebraic approach to association schemes of coding theory," *Philips J. Res.*, vol. 10, pp. 1–97, 1973.

[9] S. I. El-Zanati, G. F. Seelinger, P. A. Sissokho, L. E. Spence, and C. V. Eynden, "Partitions of finite vector spaces into subspaces," *J. Combin. Designs*, vol. 16, pp. 329–341, July 2007.

[10] T. Etzion, "Perfect byte-correcting codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 3140–3146, Nov. 1998.

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

[12] T. Etzion and A. Vardy, "On q-analogs of Steiner systems and covering designs," *Adv. Math. Commun.*, 2011, to appear.

[13] P. Frankl and R. M. Wilson, "The Erdös-Ko-Rado theorem for vector spaces," *J. Combin. Theory, Series A*, vol. 43, pp. 228–236, 1986.

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

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

[16] M. Gadouleau and Z. Yan, "Constant-rank codes and their connection to constant-dimension codes," *IEEE Trans. Inf. Theory*, submitted for publication.

[17] M. Gadouleau and Z. Yan, "Packing and covering properties of subspace codes for error control in random linear network coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2097–2108, May 2010.

[18] R. Kötter and F. R. Kschischang, "Error correction in random network coding," presented at the 2nd Annual Workshop on Information Theory and Applications, La Jolla, CA, Jan. 2007.

[19] R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, Jun. 2007.

[20] R. Kötter 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.

[21] A. Kohnert and S. Kurz, "Construction of large constant-dimension codes with a prescribed minimum distance," *Lecture Notes in Computer Science*, vol. 5393, pp. 31–42, Dec. 2008.

[22] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[23] 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.

[24] W. J. Martin and X. J. Zhu, "Anticodes for the Grassmann and bilinear forms graphs,," *Designs, Codes, Crypto.*, vol. 6, pp. 73–79, 1995.

[25] A. Montanari and R. Urbanke, "Iterative coding for network coding," *IEEE Trans. Inf. Theory*, submitted for publication.

[26] M. Schwartz and T. Etzion, "Codes and anticodes in the Grassmann graph," *J. Combin. Theory*, ser. A, vol. 97, pp. 27–42, 2002.

[27] M. J. Siavoshani, C. Fragouli, and S. Diggavi, "Noncoherent multisource network coding," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, ON, Canada, Jul. 2008.

[28] D. Silva, F. R. Kschischang, and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.

[29] D. Silva and F. R. Kschischang, "Security for wiretap networks via rank-metric codes," in *Proc. IEEE Intern. Symp. Information Theory*, Toronto, ON, Canada, Jul. 2008.

[30] B. S. Rajan and P. Krishnan, "Convolutional codes for network-error correction: Instantaneous networks," *IEEE Trans. Inf. Theory*, submitted for publication.

[31] S. Thomas, "Designs over finite fields," *Geometriae Dedicata*, vol. 21, pp. 237–242, 1987.

[32] S. Thomas, "Designs and partial geometries over finite fields," *Geometriae Dedicata*, vol. 63, pp. 247–253, 1996.

[33] L. M. G. Tolhuizen, "The generalized Gilbert-Varshamov bound is implied by Turán theorem," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1605–1606, Sep. 1997.

[34] A. Vardy and Y. Be'ery, "Maximum-likelihood soft decision decoding of BCH codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 546–554, Mar. 1994.

[35] H. Wang, C. Xing, and R. M. Safavi-Naini, "Linear authentication codes: Bounds and constructions," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 866–872, Apr. 2003.

[36] S.-T. Xia and F.-W. Fu, "Johnson type bounds on constant dimension codes," *Designs, Codes, Crypto.*, vol. 50, pp. 163–172, Feb. 2009.

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, in 1980, 1982, and 1984, respectively.

Since 1984, he has been with the Department of Computer Science, Technion, where he is currently a Professor. During 1986–1987, he was a Visiting Research Professor with the Department of Electrical Engineering—Systems, University of Southern California, Los Angeles. During the summers of 1990 and 1991, he visited Bellcore, Morristown, NJ. During 1994–1996, he was a Visiting Research Fellow in the Computer Science Department, Royal Holloway, University of London, London, U.K. He also had several visits to the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, during 1995–1998; two visits to HP Bristol during the summers of 1996 and 2000; several visits to the Department of Electrical Engineering, University of California at San Diego, during 2000–2009; and several visits to the Mathematics Department, Royal Holloway, University of London, during 2007–2009. 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.

Alexander Vardy (S'88–M'91–SM'94–F'98) was born in Moscow, U.S.S.R., in 1963. He earned the B.Sc. degree (*summa cum laude*) from the Technion, Israel, in 1985, and the Ph.D. degree from Tel Aviv University in 1991.

During 1985–1990 he was with the Israeli Air Force, where he worked on electronic counter measures systems and algorithms. During 1992–1993 he was a Visiting Scientist at the IBM Almaden Research Center, San Jose, CA. From 1993 to 1998, he was with the University of Illinois at Urbana-Champaign, first as an Assistant Professor then as an Associate Professor. He is now a Professor in the Department of Electrical Engineering, the Department of Computer Science, and the Department of Mathematics, all at the University of California, San Diego (UCSD). While on sabbatical from UCSD, he has held long-term visiting appointments with CNRS, France, the EPFL, Switzerland, and the Technion, Israel. His research interests include error-correcting codes, algebraic and iterative decoding algorithms, lattices and sphere packings, coding for digital media, cryptography and computational complexity theory, and fun math problems.

Prof. Vardy received an IBM Invention Achievement Award in 1993, and NSF Research Initiation and CAREER awards in 1994 and 1995. In 1996, he was appointed Fellow in the Center for Advanced Study at the University of Illinois, and received the Xerox Award for faculty research. In the same year, he became a Fellow of the Packard Foundation. He received the IEEE Information Theory Society Paper Award (jointly with Ralf Koetter) for the year 2004. In 2005, he received the Fulbright Senior Scholar Fellowship, and the Best Paper Award at the IEEE Symposium on Foundations of Computer Science (FOCS). During 1995–1998, he was an Associate Editor for Coding Theory and during 1998–2001, he was the Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY. He was also an Editor for the *SIAM Journal on Discrete Mathematics*. He has been a member of the Board of Governors of the IEEE Information Theory Society from 1998 to 2006, and again starting in 2011.