# The Asymptotic Behavior of Grassmannian Codes

Simon R. Blackburn, *Member, IEEE*, and Tuvi Etzion, *Fellow, IEEE*

***Abstract*—The iterated Johnson bound is the best known upper bound on the size of an error-correcting code in the Grassmannian $\mathcal{G}_q(n,k)$. The iterated Schönheim bound is the best known lower bound on the size of a covering code in $\mathcal{G}_q(n,k)$. We prove that both bounds are asymptotically attained for fixed $k$ and fixed radius, as $n$ approaches infinity. Our methods rely on results from the theory of quasi-random hypergraphs which are proved using probabilistic techniques. We also determine the asymptotics of the size of the best Grassmannian codes and covering codes when $n-k$ and the radius are fixed, as $n$ approaches infinity.**

***Index Terms*—Constant dimension code, covering bound, Grassmannian, hypergraph, packing bound.**

## I. Introduction

Let $\mathbb{F}_q$ be the finite field of order $q$ and let $n$ and $k$ be integers such that $0 \le k \le n$. The *Grassmannian* $\mathcal{G}_q(n,k)$ is the set of all $k$-dimensional subspaces of $\mathbb{F}_q^n$. We have that

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

where $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the *$q$-ary Gaussian binomial coefficient*. A natural measure of distance in $\mathcal{G}_q(n,k)$ is the *subspace metric* [1], [17] given by

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

for $U,V \in \mathcal{G}_q(n,k)$. We say that $\mathbb{C} \subseteq \mathcal{G}_q(n,k)$ is an $(n,M,d,k)_q$ *code in the Grassmann space* if $|\mathbb{C}| = M$ and $d_S(U,V) \ge d$ for all distinct $U,V \in \mathbb{C}$. Such a code $\mathbb{C}$ is also called a constant dimension code. The subspaces in $\mathbb{C}$ are called *codewords*. (Note that the distance between any pair of elements of $\mathcal{G}_q(n,k)$ is even. Because of this, some authors define the distance between subspaces $U$ and $V$ as $\frac{1}{2}d_S(U,V)$.) An important observation is the following: a code $\mathbb{C}$ in the Grassmann space $\mathcal{G}_q(n,k)$ has minimum distance $2\delta+2$ or more if and only if each subspace in $\mathcal{G}(n,k-\delta)$ is contained in at most one codeword.

There is a "dual" notion to a Grassmannian code, known as a $q$-covering design: we say that $\mathbb{C} \subseteq \mathcal{G}_q(n,k)$ is a *$q$-covering design* $\mathbb{C}_q(n,k,r)$ if each element of $\mathcal{G}_q(n,r)$ is contained in at least one element of $\mathbb{C}$. If each element of $\mathcal{G}_q(n,r)$ is contained in exactly one element of $\mathbb{C}$, we have a *Steiner structure*, which is both an optimal Grassmannian code and an optimal $q$-covering design [12], [22]. Codes and designs in the Grassmannian have been studied extensively in the last five years due to the work by Koetter and Kschischang [17] in random network coding, who showed that an $(n,M,d,k)_q$ code can correct any $t$ packet insertions and any $s$ packet erasures, as long as $2t+2s < d$. Our goal in this paper is to examine cases in which we can determine the asymptotic behavior of codes and designs in the Grassmannian.

Let $\mathcal{A}_q(n,d,k)$ denote the maximum number of codewords in an $(n,M,d,k)_q$ code. The *packing bound* is the best known asymptotic upper bound for $\mathcal{A}_q(n,d,k)$. If we write $d = 2\delta+2$, we have

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

This bound is proved by noting that in an $(n,M,2\delta+2,k)_q$ code, each $(k-\delta)$-dimensional subspace can be contained in at most one codeword. Bounds on $\mathcal{A}_q(n,d,k)$ were given in many papers, e.g., [9]–[12], [17], [18], [25], [28], [29], In particular, the well-known Johnson bound for constant weight codes was adapted for constant dimension codes independently in [11], [12], and [29] to show that

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

By iterating this bound, using the observation that $\mathcal{A}_q(n,2\delta+2,k) = 1$ for all $k \le \delta$, we obtain the *iterated Johnson bound*

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

It is not difficult to see that the iterated Johnson bound is always stronger than the packing bound (indeed, the packing bound may be derived as a simple corollary of the iterated Johnson bound). However, the main goal of this paper is to prove that the packing bound (and so the iterated Johnson bound) is attained asymptotically for fixed $k$ and $\delta$, $k \ge \delta$, when $n$ tends to infinity. In other words, we will prove the following theorem, in which the term $A(n) \sim B(n)$ means that $\lim_{n\to\infty} A(n)/B(n) = 1$.

*Theorem 1:* Let $q$, $k$, and $\delta$ be fixed integers, with $0 \le \delta \le k$ and such that $q$ is a prime power. Then

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

as $n \to \infty$.

In fact, the proof of our theorem shows a little more than this: see the proof of the theorem and the comment in the last section

Manuscript received November 18, 2011; revised April 02, 2012; accepted June 06, 2012. Date of publication July 10, 2012; date of current version September 11, 2012. This work was supported in part by the Israeli Science Foundation, Jerusalem, Israel, under Grant 230/08.

S. R. Blackburn is with the Department of Mathematics, Royal Holloway, University of London, Egham, Surrey, TW20 0EX, U.K. (e-mail: s.blackburn@rhul.ac.uk).

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

Communicated by A. Ashikhmin, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2012.2207370

of this paper. Our proof of the lower bound relies on probabilistic results from the theory of quasi-random hypergraphs, and so does not produce explicit codes. We remark that the theory of quasi-random hypergraphs has been used previously in coding theory, to establish the existence of classes of error correcting codes that are larger than the Gilbert–Varshamov bound (see [16], [24], and [27]).

There are known explicit constructions that produce codes whose size is within a constant factor of the packing bound as $n \to \infty$. Currently, the best codes known are the codes of Etzion and Silberstein [9] that are obtained by extending the codes of Silva *et al.* [23] using a "multilevel construction." If $q = 2$ and $\delta = 2$, then the ratio between the size of the code and the packing bound is 0.6657, 0.6274, and 0.625 when $k = 4$, $k = 8$, and $k = 30$ respectively, as $n$ tends to infinity. When $k = 3$, the ratio of 0.7101 in [23] was improved in [10] to 0.7657. The Reed–Solomon-like codes of [17] represented as a lifting of codewords of maximum rank distance codes [23] approach the packing bound as $n \to \infty$ when one of $\delta$ or $q$ also tends to infinity [10, Lemma 19]. Theorem 1 shows that there exist codes approaching the packing bound as $n \to \infty$ even when $\delta$ and $q$ are fixed; of course, the challenge is now to construct such codes explicitly.

This paper also proves a similar result for $q$-covering designs. Let $\mathcal{C}_q(n,k,r)$ denote the minimum number of $k$-dimensional subspaces in a $q$-covering design $\mathbb{C}_q(n,k,r)$. Bounds on $\mathcal{C}_q(n,k,r)$ can be found in [8] and [13]. Setting $r = k-\delta$, the *covering bound* states that

$$\mathcal{C}_q(n,k,r) \geq \frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q}. \tag{3}$$

This bound may be proved by observing that in a $\mathbb{C}_q(n,k,k-\delta)$ covering design each $(k-\delta)$-dimensional subspace must be contained in at least one codeword. The *Schönheim bound* is an analogous result to the Johnson bound above

$$\mathcal{C}_q(n,k,r) \geq \frac{q^n-1}{q^k-1}\mathcal{C}_q(n-1,k-1,r-1).$$

This bound implies the iterated Schönheim bound [13]

$$\mathcal{C}_q(n,k,r) \geq \left\lceil \frac{q^n-1}{q^k-1} \left\lceil \frac{q^{n-1}-1}{q^{k-1}-1} \cdots \left\lceil \frac{q^{n-r+1}-1}{q^{k-r+1}-1} \right\rceil \cdots \right\rceil \right\rceil. \tag{4}$$

The iterated Schönheim bound is always at least as strong as the covering bound. But the following theorem shows that when $k$ and $\delta$ are fixed with $n \to \infty$ the covering bound (and so the iterated Schönheim bound) is attained asymptotically:

*Theorem 2:* Let $q$, $k$, and $\delta$ be fixed integers, with $0 \leq \delta \leq k$ and such that $q$ is a prime power. Then

$$\mathcal{C}_q(n,k,k-\delta) \sim \frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q}$$

as $n \to \infty$.

The proof of the theorem does not explicitly construct families of $q$-designs whose ratio with the covering bound approaches 1. The relationship between the best known $q$-covering designs and the covering bound is more complicated than in the case of Grassmannian codes, but it is usually the case that better ratios can be obtained by explicit constructions of $q$-covering designs when compared to the corresponding problem for Grassmannian codes. For example, a ratio of 1.05 can be obtained by explicit constructions [8] when $q = 2$, $k = 3$, and $\delta = 1$, as $n \to \infty$.

The asymptotics of $\mathcal{A}_q(n, 2\delta+2, k)$ when $n-k$ and $\delta$ are fixed, and of $\mathcal{C}_q(n,k,r)$ when $n-k$ and $r$ are fixed, are also determined in this paper. The result for $\mathcal{A}_q(n,2\delta+2,k)$ is a simple corollary of Theorem 1, whereas the result for $\mathcal{C}_q(n,k,r)$ follows from results in finite geometry.

The rest of this paper is organized as follows. In Section II, we will present the proofs for our main theorems. In Section III, we consider the case when $n-k$ is fixed as $n \to \infty$. Finally, in Section IV, we provide comments on our results, and state some open questions.

## II. Proofs of the Main Theorems

We begin by observing a simple relationship between the minimum size of a $q$-covering design and the maximum size of a Grassmannian code.

*Proposition 1:* We have that

$$\mathcal{C}_q(n,k,k-\delta) \leq \mathcal{A}_q(n,2\delta+2,k) + \begin{bmatrix} n \\ k-\delta \end{bmatrix}_q - \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q \mathcal{A}_q(n,2\delta+2,k)$$

and

$$\mathcal{A}_q(n,2\delta+2,k) \geq \mathcal{C}_q(n,k,k-\delta) + \begin{bmatrix} n \\ k-\delta \end{bmatrix}_q - \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q \mathcal{C}_q(n,k,k-\delta).$$

In particular, Theorems 1 and 2 are equivalent.

*Proof:* Let $\mathbb{C}$ be a Grassmannian code of size $\mathcal{A}_q(n,2\delta+2,k)$. There are exactly $\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q \mathcal{A}_q(n,2\delta+2,k)$ subspaces of dimension $k-\delta$ that lie in some element of $\mathbb{C}$, since no subspace of dimension $k-\delta$ is contained in more than one element of $\mathbb{C}$. Thus, there are $\Upsilon \overset{\text{def}}{=} \begin{bmatrix} n \\ k-\delta \end{bmatrix}_q - \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q \mathcal{A}_q(n,2\delta+2,k)$ uncovered subspaces of dimension $k-\delta$, and we may construct a $q$-covering design by adding $\Upsilon$ or fewer $k$-dimensional subspaces to $\mathbb{C}$. This establishes the first inequality of the proposition.

To establish the second inequality, let $\mathbb{C}$ be a $q-$ covering design of size $\mathcal{C}_q(n,k,k-\delta)$. There are $\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q \mathcal{C}_q(n,k,k-\delta)$ pairs $(U,V)$ such that $U \in \mathcal{G}_q(n,k-\delta)$, $V \in \mathbb{C}$ and $U \subseteq V$. Suppose we order these pairs in some way. Since every $(k-\delta)-$ dimensional subspace $U$ occurs at least once as the first element of a pair, there are $\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q \mathcal{C}_q(n,k,k-\delta) - \begin{bmatrix} n \\ k-\delta \end{bmatrix}_q$ pairs $(U,V)$ where a pair $(U,V')$ for some $V' \in \mathbb{C}$ occurs earlier in the ordering. Removing the corresponding subspaces $V$ from $\mathbb{C}$ produces a Grassmannian code of size at least $\mathcal{C}_q(n,k,k-\delta) + \begin{bmatrix} n \\ k-\delta \end{bmatrix}_q - \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q \mathcal{C}_q(n,k,k-\delta)$, and so the second inequality follows.

Suppose Theorem 1 holds. Let $q$ be a fixed prime power, and let $k$ and $\delta$ be fixed integers such that $0 \leq \delta \leq k$. Then (2) implies that $\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q - \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q \mathcal{A}_q(n, 2\delta+2, k) = o\left(\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q\right)$ and so the first inequality of the proposition implies that

$$\begin{aligned}\mathcal{C}_q(n,k,k-\delta) &\leq \mathcal{A}_q(n,2\delta+2,k) + o\left(\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q\right)\\ &\leq \frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q} + o\left(\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q\right) \quad \text{by (1)}\\ &\sim \frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q}.\end{aligned}$$

Theorem 2 now follows from this asymptotic inequality and the covering bound (3).

The proof that Theorem 1 follows from Theorem 2 is similar to the above, and is omitted. ■

We prove Theorem 1 by using a result in quasi-random hypergraphs. To state this result, we begin by recalling some terminology from hypergraph theory. A hypergraph $\Gamma$ is $\ell$-uniform if all its hyperedges have cardinality $\ell$. The *degree* $\deg(u)$ of a vertex $u \in \Gamma$ is the number of hyperedges containing $u$; if $\deg(u) = r$ for all $u \in \Gamma$, we say that $\Gamma$ is $r$*-regular*. The *codegree* $\operatorname{codeg}(u_1, u_2)$ of a pair of distinct vertices $u_1, u_2 \in \Gamma$ is the number of hyperedges containing both $u_1$ and $u_2$. A *matching* (or edge packing) in $\Gamma$ is a set of pairwise disjoint hyperedges of $\Gamma$. We write $\mathcal{U}(\Gamma)$ for the minimum number of vertices left uncovered by a matching in $\Gamma$. Thus the largest number of hyperedges in a matching of an $\ell$-uniform hypergraph $\Gamma$ on $v$ vertices is $(v - \mathcal{U}(\Gamma))/\ell$. The main theorem we use is due to [26, Th. 1.2.1]:

*Theorem 3:* Let $\ell$ be a fixed integer, where $\ell \geq 4$. Then, there exist constants $\alpha$ and $\beta$ with the following property. Let $\Gamma$ be an $\ell$-uniform $r$-regular hypergraph with $v$ vertices. Define $c = \max \operatorname{codeg}(u_1, u_2)$, where the maximum is taken over all distinct vertices $u_1, u_2 \in \Gamma$. Then

$$\mathcal{U}(\Gamma) \leq \alpha v (c/r)^{1/(\ell-1)} (\log r)^{\beta}.$$

The proof of Theorem 3 uses probabilistic methods, inspired by the techniques of Frankl and Rödl [15], [21]. See [2], [3], and [20] for related work.

*Proof of Theorem 1:* If $\delta = 0$, then the set of all subspaces in the Grassmannian is a code that achieves the packing bound; if $\delta = k$ then any single subspace of dimension $k$ achieves the packing bound. So we may assume that $0 < \delta < k$. Now suppose that $k = 2$, so $\delta = 1$. The theorem follows in this case since it is known [12] that $\mathcal{A}_q(n,4,2) = \frac{q^n-1}{q^2-1}$ if $n$ is even; and $\mathcal{A}_q(n,4,2) \geq \frac{q^n-1}{q^2-1} - \frac{q^2}{q+1}$ if $n$ is odd. Thus we may suppose that $k \geq 3$.

Define a hypergraph $\Gamma_n$ as follows. We identify the set of vertices of $\Gamma_n$ with $\mathcal{G}_q(n, k-\delta)$, and the set of hyperedges of $\Gamma_n$ with $\mathcal{G}_q(n,k)$. We define a hyperedge $V$ to contain a vertex $U$ if and only if $U \subseteq V$ (as subspaces). We note that $\mathcal{A}_q(n, 2\delta+2, k)$ is exactly the maximum size of a matching in $\Gamma_n$.

Now $\Gamma_n$ is an $\ell$-uniform hypergraph, where $\ell = \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q$. Note that $\ell \geq 4$, and $\ell$ does not depend on $n$. Every vertex of $\Gamma_n$ has degree $r(n) = \begin{bmatrix} n-(k-\delta) \\ \delta \end{bmatrix}_q$. Let $U_1$ and $U_2$ be distinct vertices, so $\dim(U_1 + U_2) = k - \delta + i$ for some positive integer $i$. Then, $\operatorname{codeg}(U_1, U_2)$ is the number of $k-$ dimensional subspaces containing $U_1 + U_2$, which is at most the number of $k$-dimensional subspaces containing a $(k-\delta+1)$-dimensional subspace of $U_1 + U_2$. So

$$\operatorname{codeg}(U_1, U_2) = \begin{bmatrix} n-(k-\delta+i) \\ \delta - i \end{bmatrix}_q \leq \begin{bmatrix} n-(k-\delta+1) \\ \delta - 1 \end{bmatrix}_q.$$

But

$$\begin{bmatrix} n-(k-\delta) \\ \delta \end{bmatrix}_q = \Theta(q^{n\delta}) \text{and}$$
$$\begin{bmatrix} n-(k-\delta+1) \\ \delta-1 \end{bmatrix}_q = \Theta(q^{n(\delta-1)})$$

and so $\max_{u_1,u_2 \in \Gamma_n} \operatorname{codeg}(u_1,u_2) = O(q^{-n} r(n))$. Theorem 3 now implies that there exists an integer $\beta$ such that

$$\mathcal{U}(\Gamma_n) = O\left(\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q q^{-n/(\ell-1)} (\log r(n))^{\beta}\right).$$

Thus, $\mathcal{U}(\Gamma_n) = o(\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q)$, and so the largest matching in $\Gamma_n$ contains at least $\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q (1-o(1))/\ell$ edges. The packing bound shows that the largest matching in $\Gamma_n$ has size at most $\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q/\ell$, and so $\mathcal{A}(n, 2\delta+2, k) \sim \begin{bmatrix} n \\ k-\delta \end{bmatrix}_q/\ell$, as required. ■

*Proof of Theorem 2:* Theorem 2 immediately follows from Proposition 1 and Theorem 1. ■

## III. Case of Large $k$

In the previous section, we assumed that $k$ is fixed (and therefore is small when compared to $n$). In this section, we consider the "dual" case, where $n-k$ is assumed to be fixed (and so $k$ is large).

It is proved in [12], [17], and [29] that $\mathcal{A}_q(n, 2\delta+2, k) = \mathcal{A}_q(n, 2\delta+2, n-k)$. (This holds because taking the duals of all subspaces in an $(n, M, d, k)_q$ code in the Grassmann space produces an $(n, M, d, n-k)_q$-code.) Thus, we have the following corollary of Theorem 1, which establishes the asymptotics of $\mathcal{A}_q(n, 2\delta+2, k)$ when $n-k$ and $\delta$ are fixed with $n \to \infty$.

*Corollary 1:* Let $q$, $t$, and $\delta$ be fixed integers such that $0 \leq \delta \leq t$, and such that $q$ is a prime power. Then

$$\mathcal{A}_q(n, 2\delta+2, n-t) \sim \frac{\begin{bmatrix} n \\ t-\delta \end{bmatrix}_q}{\begin{bmatrix} t \\ t-\delta \end{bmatrix}_q}$$

as $n \to \infty$.

Note that when $\delta > t$ we have that $\mathcal{A}_q(n, 2\delta + 2, n - t) = \mathcal{A}_q(n, 2\delta + 2, t) = 1$, so the restriction on $\delta$ in Corollary 1 is a natural one.

The same techniques do not establish a similar result for $q$-covering designs, since $\mathcal{C}_q(n, k, r)$ and $\mathcal{C}_q(n, n - k, r)$ are not equal in general. However, by translating some of the results known in finite geometry into our language, we can determine $\mathcal{C}_q(n, k, r)$ when $q$, $r$, and $n - k$ are fixed, as Theorem 6 shows.

For the proof of the theorem will need the notion of a $q$-Turán design. We say that $\mathbb{C} \subseteq \mathcal{G}_q(n, r)$ is a *$q$-Turán design* $\mathbb{T}_q(n, k, r)$ if each element of $\mathcal{G}_q(n, k)$ contains at least one element of $\mathbb{C}$. Let $\mathcal{T}_q(n, k, r)$ denote the minimum number of $r$-dimensional subspaces in a $q$-covering design $\mathbb{T}_q(n, k, r)$. The notions of $q$-covering designs and $q$-Turán designs are dual; the following result was proved in [13]:

*Theorem 4:* $\mathcal{C}_q(n, k, r) = \mathcal{T}_q(n, n - r, n - k)$ for all $1 \leq r \leq k \leq n$.

Using normal spreads [19] (also known as geometric spreads) Beutelspacher and Ueberberg [5] proved the following theorem using some of the theory of finite projective geometry.

*Theorem 5:* $\mathcal{T}_q(vm + \delta, vm - v + 1 + \delta, m) = \frac{q^{vm}-1}{q^m-1}$ for all $v \geq 2$ and $m \geq 2$.

We remark that Beutelspacher and Ueberberg show much more that there is essentially only one optimal construction for a $q$-Turán design with these parameters.

As a consequence from Theorems 1 and 5, we obtain the following result for $q$-covering designs.

*Corollary 2:* Let $r$ and $n$ be positive integers such that $r + 1$ divides $n$. Then

$$\mathcal{C}_q(n, n - n/(r + 1), r) = \frac{q^n - 1}{q^{n/(r+1)} - 1}.$$

*Proof:* Theorems 4 and 5 (in the case when $\delta = 0$) show that

$$\mathcal{C}_q(vm, vm - m, v - 1) = \frac{q^{vm} - 1}{q^m - 1}$$

for any integers $v \geq 2$ and $m \geq 2$. If we set $v = r + 1$ and $m = n/v$, the corollary follows except in the case when $n = 2$ and $r = 1$. But the corollary is true in this case also, as a $q$-covering design with these parameters must consist of all 1-D subspaces. ■

*Theorem 6:* Let integers $q$, $t$, and $r$ be fixed, where $q$ is a prime power. For all sufficiently large integers $n$

$$\mathcal{C}_q(n, n - t, r) = \frac{q^{(r+1)t} - 1}{q^t - 1}.$$

*Proof:* We first note that

$$\mathcal{C}_q(n + 1, n + 1 - t, r) \leq \mathcal{C}_q(n, n - t, r). \tag{5}$$

This is proved in [13]. To see why (5) holds, fix a 1-dimensional subspace $K$ of an $(n + 1)$-dimensional vector space $V$. Let $\mathbb{C}$ be a $q$-covering design $\mathbb{C}_q(n, n - t, r)$ contained in the $n$-dimensional space $V/K$. Then the set of subspaces $U$ such that $K \subseteq U \subseteq V$ and $U/K \in \mathbb{C}$ is a $q$-covering design $\mathbb{C}_q(n + 1, n + 1 - t, r)$ containing at most $\mathcal{C}_q(n, n - t, r)$ subspaces.

Inequality (5) implies that for any fixed $t$ and $r$, we have that $\mathbb{C}_q(n, n - t, r)$ is a nonincreasing sequence of positive integers as $n$ increases. So there exists a constant $c$ (depending only on $q$, $t$ and $r$) so that $\mathbb{C}_q(n, n - t, r) = c$ whenever $n$ is sufficiently large. It remains to show that $c = (q^{(r+1)t} - 1)/(q^t - 1)$.

Set $n' = t(r + 1)$, so $n' - t = n' - n'/(r + 1)$. Corollary 2 implies that

$$c \leq \mathcal{C}_q(n', n' - t, r) = \frac{q^{n'} - 1}{q^{n'/(r+1)} - 1} = \frac{q^{(r+1)t} - 1}{q^t - 1}.$$

Now $c$ is bounded below by the Schönheim bound (4). We give a simpler form for the Schönheim bound that holds for all sufficiently large $n$ as follows. When $n$ is sufficiently large, we find that

$$\left\lceil \frac{q^{n-r+1} - 1}{q^{k-r+1} - 1} \right\rceil = q^t + 1 = \frac{q^{2t} - 1}{q^t - 1}.$$

Moreover, for $i$ such that $0 \leq i \leq r - 2$

$$\left\lceil \frac{q^{n-i} - 1}{q^{k-i} - 1} \times \frac{q^{(r-i)t} - 1}{q^t - 1} \right\rceil = \frac{q^{(r-i+1)t} - 1}{q^t - 1}$$

provided that $n$ is sufficiently large. These equalities show that the right hand side of the Schönheim bound (4) is equal to $(q^{(r+1)t} - 1)/(q^t - 1)$ for all sufficiently large integers $n$. So $c \geq (q^{(r+1)t} - 1)/(q^t - 1)$, as required. ■

## IV. Optimal Codes and Research Directions

In this section, we comment on our results, we provide a little extra background, and we propose topics for further study.

We have proved that for a given $q$, if we fix $k$, and $\delta$, where $\delta < k$, the packing bound for Grassmannian codes is asymptotically attained when $n$ tends to infinity. We commented in Section I that the same is true when $q$ or $\delta$ grows. In Section III, we determined the asymptotics of $\mathcal{A}_q(n, 2\delta + 2, k)$ when $n - k$ and $\delta$ are fixed. These results do not address the cases when $q$ and $\delta$ are fixed, but $k$ and $n - k$ both grow (for example when $k = \lfloor \alpha n \rfloor$ for some fixed real number $\alpha \in (0, 1)$). Can similar results be obtained a wide range of these cases? When $k$ grows rather slowly when compared to $n$, it should be possible to use a result of Alon *et al.* [2] to show that $\mathcal{A}_q(n, 2\delta + 2, k)$ still approaches the packing bound.

The proof of Theorem 1 does not just give the leading term of $\mathcal{A}_q(n, 2\delta + 2, k)$: the order of the error term is also given. However, we do not see any reason why this error term is tight.

Similar questions can be asked about the relationship between the covering bound and $\mathcal{C}_q(n, k, r)$. It seems that small $q$-covering designs are easier to construct than large Grassmannian codes; certainly there are more construction methods currently known [8], [13].

As well as trivial cases, there are a few sets of parameters for which the exact (or almost the exact) values of $\mathcal{A}_q(n, d, k)$ and $\mathcal{C}_q(n, k, r)$ are known. Section III discusses a family of optimal $q$-covering designs. A family of optimal Grassmannian codes is known when $d = 2k$. *Spreads* (from projective geometry) give rise to optimal codes as well as $q$-covering designs when $k$

divides $n$. Known *partial spreads* of maximum size give rise to optimal codes in other cases [4], [6], [7], [14].

For small parameters, the best known codes are very often cyclic codes, which are defined as follows. Let $\alpha$ be a primitive element of $\mathrm{GF}(q^n)$. We say that a code $\mathbb{C} \subseteq \mathcal{G}_q(n,k)$ 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 subspace $V \in \mathbb{C}$ into the corresponding binary characteristic vector $x_V = (x_0, x_1, \ldots, x_{q^n-2})$ given by

$$x_i = 1, \text{ if } \alpha^i \in V \quad \text{and} \quad x_i = 0, \text{ if } \alpha^i \not\in V$$

then the set of all such characteristic vectors is closed under cyclic shifts. It would be very interesting to find out whether cyclic codes approach the packing bound and the covering bound asymptotically. Again, in this case, we would like to see proofs similar to the ones of Theorems 1 and 2. Of course, explicit families of asymptotically good cyclic codes would be even more worthwhile.

## Acknowledgment

The authors would like to thank Simeon Ball for introducing to them the concept of normal spreads.

## References

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

[2] N. Alon, B. Bollobas, J. H. Kim, and V. H. Vu, “Economical covers with geometric applications,” *Proc. London Math. Soc.*, vol. 86, pp. 273–301, 2003.

[3] N. Alon and J. H. Spencer, *The Probabilistic Method*, 3rd ed. Hoboken, NJ: Wiley, 2008.

[4] J. de Beule and K. Metsch, “The maximum size of a partial spread in $H(5, q^2)$ is $q^3 + 1$,” *J. Comb. Theory, Ser. A*, vol. 114, pp. 761–768, 2007.

[5] A. Beutelspacher and J. Ueberberg, “A characteristic property of geometric $t$-spreads in finite projective spaces,” *Eur. J. Comb.*, vol. 12, pp. 277–281, 1991.

[6] J. Eisfeld, L. Storme, and P. Sziklai, “On the spectrum of the sizes of maximal partial line spreads in $PG(2n, q)$, $n \geq 3$,” *Designs, Codes, Crypt.*, vol. 36, pp. 101–110, 2005.

[7] S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, and L. Spence, “The maximum size of a partial 3-spread in a finite vector space over $GF(2)$,” *Designs, Codes, Crypt.*, vol. 54, pp. 101–107, 2010.

[8] T. Etzion, Covering subspaces by subspaces [Online]. Available: arxiv.org/abs/1111.4319

[9] T. Etzion and N. Silberstein, “Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams,” *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 2909–2919, Jul. 2009.

[10] T. Etzion and N. Silberstein, Codes and designs related to lifted MRD codes arxiv.org/abs/1102.2593.

[11] T. Etzion and A. Vardy, “Error-correcting codes in projective space,” in *Proc. Int. Symp. Inf. Theory*, Jul. 2008, pp. 871–875.

[12] T. Etzion and A. Vardy, “Error-correcting codes in projective space,” *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1165–1173, Feb. 2011.

[13] T. Etzion and A. Vardy, “On $q$-analogs for Steiner systems and covering designs,” *Adv. Math. Commun.*, vol. 5, no. 2, pp. 161–176, 2011.

[14] A. Gács and T. Szonyi, “On maximal partial spreads in $PG(n, q)$,” *Designs Codes Crypt.*, vol. 29, pp. 123–129, 2003.

[15] P. Frankl and V. Rödl, “Near perfect coverings in graphs and hypergraphs,” *Eur. J. Combin.*, vol. 6, pp. 317–326, 1985.

[16] T. Jiang and A. Vardy, “Asymptotic improvement of the Gilbert–Varshamov bound on the size of binary codes,” *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1655–1664, Aug. 2004.

[17] 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.

[18] A. Kohnert and S. Kurz, “Construction of large constant-dimension codes with a prescribed minimum distance,” *Lecture Notes Comput. Sci.*, vol. 5393, pp. 31–42, Dec. 2008.

[19] G. Lunardon, “Normal spreads,” *Geometriae Dedicata*, vol. 75, pp. 245–261, 1999.

[20] N. Pippenger and J. Spencer, “Asymptotic behavior of the chromatic index for hypergraphs,” *J. Comb. Theory, Ser. A*, vol. 51, pp. 24–42, 1989.

[21] V. Rödl, “On a packing and covering problem,” *Eur. J. Comb.*, vol. 6, pp. 69–78, 1985.

[22] M. Schwartz and T. Etzion, “Codes and anticodes in the Grassman graph,” *J. Comb. Theory, Ser., A*, vol. 97, pp. 27–42, 2002.

[23] 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.

[24] L. M. G. M. Tolhuizen, “The generalized Gilbert–Varshamov bound is implied by Turan’s theorem,” *IEEE Trans. Inf. Theory*, vol. 43, no. 5, pp. 1605–1606, Sep. 1997.

[25] A.-L. Trautmann and J. Rosenthal, “New improvements on the Echelon-Ferrers construction,” in *Proc. Int. Symp. Math. Theory Netw. Syst.*, Jul. 2010, pp. 405–408.

[26] V. H. Vu, “New bounds on nearly perfect matchings in hypergraphs: Higher codegrees do help,” *Random Struct. Algorithms*, vol. 17, pp. 29–63, 2000.

[27] V. Vu and L. Wu, “Improving the Gilbert–Varshamov bound for $q$-ary codes,” *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3200–3208, Sep. 2005.

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

[29] S.-T. Xia and F.-W. Fu, “Johnson type bounds on constant dimension codes,” *Designs, Codes Crypt.*, vol. 50, pp. 163–172, 2009.

**Simon R. Blackburn** (M’12) was born in Beverley, Yorkshire, England in 1968. He received a BSc in Mathematics from Bristol in 1989, and a DPhil in Mathematics from Oxford in 1992.

He has worked in the Mathematics Department at Royal Holloway, University of London since 1992, and is currently a Professor of Pure Mathematics. His research interests include algebra, combinatorics and associated applications in cryptography and communication theory

**Tuvi Etzion** (M’89–SM’94–F’04) was born in Tel Aviv, Israel, in 1956. He received the B.A., M.Sc., and D.Sc. degrees in computer science from the Technion— Israel Institute of Technology, Haifa, Israel, in 1980, 1982, and 1984, respectively.

Since 1984 he held a position in the Department of Computer Science, Technion, where he currently has a Professor position. During 1986–1987, he was a Visiting Research Professor with the Department of Electrical Engineering—Systems, University of Southern California, Los Angeles. During summers 1990 and 1991, he was visiting Bellcore in Morristown, NJ. During 1994–1996, he was a Visiting Research Fellow in the Computer Science Department, Royal Holloway College, Egham, U.K. He also had several visits to the Coordinated Science Laboratory, University of Illinois in Urbana-Champaign, Urbana, during 1995–1998, two visits to HP Bristol during summers 1996 and 2000, a few visits to the Department of Electrical Engineering, University of California at San Diego during 2000–2010, and several visits to the Mathematics Department, Royal Holloway College, 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 until 2009