Asymptotic Improvement of the Gilbert-Varshamov Bound on the Size of Binary Codes

TAO JIANG and ALEXANDER VARDY

arXiv:math/0404325v1 [math.CO] 19 Apr 2004

Abstract—**Given positive integers n and d, let $A_2(n,d)$ denote the maximum size of a binary code of length n and minimum distance d. The well-known Gilbert-Varshamov bound asserts that $A_2(n,d) \geqslant 2^n/V(n,d-1)$, where $V(n,d)=\sum_{i=0}^{d}\binom{n}{i}$ is the volume of a Hamming sphere of radius d. We show that, in fact, there exists a positive constant c such that**

$$A_2(n,d) \;\geqslant\; c\,\frac{2^n}{V(n,d-1)}\,\log_2 V(n,d-1)$$

whenever $d/n \leqslant 0.499$. The result follows by recasting the Gilbert-Varshamov bound into a graph-theoretic framework and using the fact that the corresponding graph is locally sparse. Generalizations and extensions of this result are briefly discussed.

Keywords— **Ajtai-Komlós-Szemerédi bound, asymptotic constructions, binary codes, constant-weight codes, Gilbert-Varshamov bound, locally sparse graphs, nonlinear codes, q-ary codes.**

I. INTRODUCTION

Let $A_q(n,d)$ denote the maximum number of codewords in a code of length n and minimum distance d over an alphabet with q letters. The Gilbert-Varshamov bound, which asserts that

$$A_q(n,d) \;\geqslant\; \frac{q^n}{\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i} \tag{1}$$

is one of the most well-known and fundamental results in coding theory. In this paper, we focus on binary codes (although an extension of our results to codes over an arbitrary alphabet is discussed in Section V). Thus we let

$$V(n,d) \;\stackrel{\text{def}}{=}\; \sum_{i=0}^{d}\binom{n}{i}$$

denote the volume of a Hamming sphere of radius d in $\mathbb{F}_2^n$, and consider the binary version of (1), namely

$$A_2(n,d) \;\geqslant\; f_{\mathrm{GV}}(n,d) \;\stackrel{\text{def}}{=}\; \frac{2^n}{V(n,d-1)} \tag{2}$$

This inequality was first proved by Gilbert [18] in 1952. It was subsequently improved upon by Varshamov [42]. However, following the established terminology, we will refer to (1) and (2) as the Gilbert-Varshamov bound. This bound is used extensively in the coding theory literature [31], [37], and has been generalized to numerous contexts [9], [29], [20], [32], [38].

Improving upon the Gilbert-Varshamov bound asymptotically is a notoriously difficult task [37], [39]. The breakthrough work of Tsfasman-Vlăduţ-Zink [40] led to an asymptotic improvement of (1), but only for alphabets of size $q \geqslant 49$ (see also the recent papers [16], [45]). For $q < 46$, no asymptotic improvements upon (1) are currently known [48]. In fact, a well-known conjecture (cf. Goppa [19]) asserts that the binary version (2) of the Gilbert-Varshamov bound is asymptotically exact.

Nevertheless, for small n and d, the size of best known binary codes [37, Chapter 5] often exceeds $f_{\mathrm{GV}}(n,d)$ by a large factor. Thus it is natural to ask whether the bound (2) can be strengthened. Indeed, various improvements upon the binary Gilbert-Varshamov bound were presented (in chronological order) by Varshamov [42], Hashim [21], Elia [15], Tolhuizen [38], Barg-Guritman-Simonis [5], and Fabris [17]. We review these improvements in detail in the next section. One of our main results herein is the following theorem, which strengthens the Gilbert-Varshamov bound using a technique quite different from those of [5], [15], [17], [21], [38], and [42].

Theorem 1. *For $x \in \mathbb{R}$, let $\lceil x \rceil^+$ denote the smallest nonnegative integer m with $m \geqslant x$. Given positive integers n and d, with $d \leqslant n$, let $e(n,d)$ denote the following quantity*

$$e(n,d) \;\stackrel{\text{def}}{=}\; \frac{1}{6}\sum_{w=1}^{d}\binom{n}{w}\left(\sum_{i=1}^{d}\;\sum_{j=\lceil\frac{w+i-d}{2}\rceil^+}^{\min\{w,i\}}\binom{w}{j}\binom{n-w}{i-j}-1\right)$$

Then

$$A_2(n,d) \;\geqslant\; \frac{2^n}{V(n,d-1)}\cdot\frac{\log_2 V(n,d-1) \;-\; \log_2\sqrt{e(n,d-1)}}{10} \tag{3}$$

What distinguishes Theorem 1 from prior improvements of the Gilbert-Varshamov bound is the asymptotic behavior of (3). All the previously known explicit lower bounds on $A_2(n,d)$ that we are aware of, including those of [5], [15], [17], [21], [38], and [42], have the following property: if we write the bound as $A_2(n,d) \geqslant f(n,d)$, then

$$f(n,d) \;=\; O\Big(f_{\mathrm{GV}}(n,d)\Big) \tag{4}$$

In fact, as we shall see in the next section, for some of these bounds $f(n,d) \;=\; f_{\mathrm{GV}}(n,d)\,\big(1+o(1)\big)$, where $o(1)$ tends to zero exponentially fast with n. In contrast, the asymptotic behavior of (3) is given by the following theorem.

Manuscript submitted August 12, 2003, and revised March 28, 2004. This work was supported in part by the David and Lucile Packard Foundation, by the National Science Foundation, and by the Miami University Summer Faculty Research Grant. The material in this paper was presented in part at the 41-st Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, October 2003.

Tao Jiang is with the Department of Mathematics and Statistics, Miami University, Oxford, OH 45056, U.S.A. (e-mail: `jiangt@muohio.edu`).

Alexander 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, U.S.A. (e-mail: `vardy@kilimanjaro.ucsd.edu`.)

Communicated by Ralf Koetter, Associate Editor for Coding Theory.

Theorem 2. *Let n and d be positive integers, with $d/n \leqslant 0.499$. Then there exists a positive constant c such that*

$$A_2(n,d) \;\geqslant\; c\,\frac{2^n}{V(n,d-1)}\,\log_2 V(n,d-1) \tag{5}$$

Remark. The constant in Theorem 2, the way it is stated above, may depend on the ratio d/n. However, if we only wish to claim that (5) is true for all sufficiently large n, then c becomes an absolute constant, independent of both n and d. For more on this, see (38). Also note that while the bound in (5) holds for any n and d with $d/n \leqslant 0.499$, it is useful only when the ratio d/n is constant. If we allow $d/n \to 0$ as $n \to \infty$, then better bounds on $A_2(n,d)$ are known [6], [31], [39].

So, how does Theorem 2 relate to the conjecture that the Gilbert-Varshamov bound is asymptotically exact for $q = 2$? This depends on the interpretation. If one views the conjecture as dealing with the asymptotics of $A_2(n,d)$ itself, namely the <u>size</u> of the best binary codes, then it corresponds to the assertion that for all positive $\delta < 0.5$, we have

$$\lim_{n\to\infty} \frac{A_2(n,\delta n)}{f_{\mathrm{GV}}(n,\delta n)} \;=\; \text{const} \tag{6}$$

where the constant might be a function of δ. Theorem 2 clearly shows that this is false: the limit $\lim_{n\to\infty} A_2(n,\delta n)/f_{\mathrm{GV}}(n,\delta n)$ does not exist for any δ. Indeed, the theorem implies that

$$\log_2 A_2(n,d) \;\geqslant\; \log_2 f_{\mathrm{GV}}(n,d) \;+\; \log(n) \;+\; \text{const} \;+\; o(1) \tag{7}$$

On the other hand, it is more common to interpret the conjecture as dealing with the asymptotics of the best possible <u>rate</u> of a binary code, namely the function $R(n,d) = \log_2 A_2(n,d)/n$. In this case, the conjecture could still be true, since the term $\log(n)/n$ will vanish for $n \to \infty$.

The rest of this paper is organized as follows. In the next section, we review the previously known improvements of the Gilbert-Varshamov bound, with the aim of establishing (4). In Section III, we recast the problem of estimating $A_2(n,d)$ into a graph-theoretic framework, and express $A_2(n,d)$ as the independence number of a certain graph (Lemma 3). We then recover the Gilbert-Varshamov bound as a straightforward consequence of a simple bound on the independence number of a graph (Proposition 4). The key idea in the proof of Theorems 1 and 2 is surprisingly simple: the bound on the independence number used in Proposition 4 can be improved upon, providing the graph at hand is locally sparse (Theorem 7). In Section IV, we show that this is, indeed, the case. Specifically, we derive a simple closed-form expression for the number of edges in the relevant graph (Proposition 9), and then prove that this graph is sparse for all sufficiently large n whenever $d/n \leqslant 0.4994$ (Proposition 12). This completes the proof of Theorems 1 and 2. In Section V, we briefly discuss various extensions and generalizations of our results. In particular, we show that just like the bounds of Gilbert [18] and Varshamov [42], our bound can be proved "constructively." That is, there is an (exponential-time) algorithm [22] that actually constructs codes satisfying (5). We also generalize Theorem 1 to arbitrary alphabets (Theorem 14) and to constant-weight codes. Finally, we point out a number of intriguing open problems related to the results of this paper.

II. Comparison with Prior Work

In this section, we briefly review previously known (to us) improvements of the Gilbert-Varshamov bound (2), roughly in chronological order, and establish the claim of (4).

The first improvement on (2) is due to Varshamov himself. Varshamov showed in [42] that $A_2(n,d) \geqslant f_{\mathrm{V}}(n,d)$, where[1]

$$f_{\mathrm{V}}(n,d) \;\stackrel{\text{def}}{=}\; \frac{2^{n-1}}{2^{\lfloor \log_2 V(n-1,d-2)\rfloor}} \tag{8}$$

and, moreover, there exist linear codes that attain this bound. We now show that the ratio $f_{\mathrm{V}}(n,d)/f_{\mathrm{GV}}(n,d)$ is upper bounded by a constant. Indeed, we have

$$\frac{f_{\mathrm{V}}(n,d)}{f_{\mathrm{GV}}(n,d)} \;\leqslant\; \frac{V(n,d-1)}{V(n-1,d-2)} \;=\; 1 \;+\; \frac{V(n-1,d-1)}{V(n-1,d-2)}$$

where the equality above follows from the fact that $V(n,d-1) = V(n-1,d-1) + V(n-1,d-2)$. Expressing $V(n,d)$ as the sum $\sum_{i=0}^{d}\binom{n}{i}$, we further obtain

$$\begin{aligned}
\frac{V(n-1,d-1)}{V(n-1,d-2)} \;&=\; 1 + \frac{\binom{n-1}{d-1}}{V(n-1,d-2)} && (9)\\
&=\; 1 + \frac{1}{\sum_{i=0}^{d-2}\frac{(d-1)!\,(n-d)!}{i!\,(n-i-1)!}} && (10)\\
&\leqslant\; 1 + \frac{n-(d-1)}{d-1} && (11)
\end{aligned}$$

where the inequality in (11) follows by retaining a single term in the sum of (10), namely the term corresponding to $i = d-2$. Thus $f_{\mathrm{V}}(n,d)/f_{\mathrm{GV}}(n,d) \leqslant (\delta+1)/\delta$, where $\delta = (d-1)/n$.

Another improvement of (2) was proposed by Hashim in 1978. Hashim [21, eq. (7)] proved the following. Let $t = \lceil (d-1)/2 \rceil$ and let $A(w;n,k,d)$ denote the minimum number of codewords of weight w in an (n,k,d) binary linear code. Then [21] shows that $A_2(n,d) \geqslant 2^k$, where k is the largest integer satisfying

$$V(n-1,d') \;-\; \sum_{w=d}^{d'+t}\;\sum_{i=w-d'}^{t}\binom{w}{i} A(w;n,k,d) \;<\; 2^{n-k} \tag{12}$$

where $d' = d-2$. Unfortunately, the bound (12) is non-explicit. Hashim [21] writes that "this improved bound requires the determination of the lowest possible value of $A(w;n,k,d)$, where $w = d, d+1, \ldots, d-2+t$, in terms of the code parameters n, k, and d." While various estimates of $A(w;n,k,d)$ are known [4], [23], [25], [26], we are not aware of any results that can be used in conjunction with (12) to produce an explicit lower bound on $A_2(n,d)$, at least not without a substantial research effort.

In 1983, Elia [15] has extended the Varshamov bound (8) in a different way. Specifically, it is shown in [15, Corollary 2] that $A_2(n,d) \geqslant f_{\mathrm{E}}(n,d)$, where

[1] Usually, $f_{\mathrm{V}}(n,d)$ is defined as 2^k, where k is the largest integer satisfying $2^k < 2^n/V(n-1,d-2)$. The explicit form (8) is equivalent to this definition.

$$f_{\mathrm{E}}(n,d) \stackrel{\mathrm{def}}{=} \frac{2^{n-2}}{\max\left\{2^{\lfloor \log_2 V(n-3,d-2)\rfloor},\ 2^{\lfloor \log_2 V(n-2,d-3)\rfloor}\right\}}$$

It is not difficult to see that, again, the ratio $f_{\mathrm{E}}(n,d)/f_{\mathrm{GV}}(n,d)$ is upper bounded by a constant. Indeed, writing $2^{\lfloor \log_2 V(n,d)\rfloor}$ as $V(n,d)/2^{\{\log_2 V(n,d)\}}$, where $\{x\}$ denotes the fractional part of $x \in \mathbb{R}$, we have

$$f_{\mathrm{E}}(n,d) \leqslant \frac{2^{n-2}2^{\{\log_2 V(n-3,d-2)\}}}{V(n-3,d-2)} \leqslant \frac{2^{n-1}}{V(n-3,d-2)}$$

This, in turn, leads to the following bound

$$\frac{f_{\mathrm{E}}(n,d)}{f_{\mathrm{GV}}(n,d)} \leqslant \frac{V(n,d-1)}{2V(n-3,d-2)} \leqslant \frac{8V(n-3,d-1)}{2V(n-3,d-2)} \qquad (13)$$

We know from (11) that $V(n-3,d-1)/V(n-3,d-2) \leqslant 1/\delta$, where $\delta = (d-1)/n$. In conjunction with (13), this implies that $f_{\mathrm{E}}(n,d)/f_{\mathrm{GV}}(n,d) \leqslant 4/\delta$.

Tolhuizen [38] established yet another slight improvement of (2) using Turán's theorem [41, Chapter 4]. Specifically, Tolhuizen [38, p. 1605] shows that $A_2(n,d) \geqslant f_{\mathrm{T}}(n,d)+1$, where $f_{\mathrm{T}}(n,d)$ is the largest integer satisfying

$$\frac{2^n}{f_{\mathrm{T}}(n,d)} + \frac{r(f_{\mathrm{T}}(n,d)-r)}{2^n f_{\mathrm{T}}(n,d)} > V(n,d-1) \qquad (14)$$

with r being the remainder when 2^n is divided by $f_{\mathrm{T}}(n,d)$. If we ignore the second term on the left-hand side of (14), then this is precisely the Gilbert-Varshamov bound (2). Otherwise, it is easy to see that

$$\begin{aligned} f_{\mathrm{T}}(n,d) &\leqslant \frac{2^n}{V(n,d-1)-2^{-(n+2)}} \\ &\leqslant \frac{2^n}{V(n,d-1)} \cdot \frac{2^{n+2}}{2^{n+2}-1} = f_{\mathrm{GV}}(n,d)\big(1+o(1)\big) \end{aligned}$$

The latest improvement on (2) is due to Fabris [17]. In fact, Fabris [17] proves two new bounds on $A_2(n,d)$. The first bound is given by $A_2(n,d) \geqslant f_{\mathrm{F}_1}(n,d)$, where

$$f_{\mathrm{F}_1}(n,d) \stackrel{\mathrm{def}}{=} \frac{2^n - \mathcal{I}(n,d-1)}{V(n,d-1)-\mathcal{I}(n,d-1)} \qquad (15)$$

and $\mathcal{I}(n,d-w)$ is the volume of the intersection between two Hamming spheres of radius $d-w$, whose centers are distance d apart. The second bound is $A_2(n,d) \geqslant f_{\mathrm{F}_2}(n,d)$, where

$$f_{\mathrm{F}_2}(n,d) \stackrel{\mathrm{def}}{=} \frac{2^n}{V(n,d-1)}\left(\frac{V(n,d-1)+\mathcal{I}(n,d-2)}{V(n,d-2)}\right) \qquad (16)$$

Obviously $\mathcal{I}(n,d-2) \leqslant V(n,d-2)$. Thus it follows straightforwardly from (16), (11) that $f_{\mathrm{F}_2}(n,d)/f_{\mathrm{GV}}(n,d) \leqslant (\delta+1)/\delta$. It is not difficult to see (cf. Lemma 8) that

$$\mathcal{I}(n,d-w) = \sum_{i=w}^{d-w} \sum_{j=\lceil \frac{w+i}{2} \rceil}^{i} \binom{w}{j}\binom{n-w}{i-j}$$

In Section IV herein, we will show (in a different context) that $\lim_{n\to\infty} \mathcal{I}(n,d-1)/V(n,d-1) = 0$. In conjunction with (15), this immediately implies that $f_{\mathrm{F}_1}(n,d) = f_{\mathrm{GV}}(n,d)\big(1+o(1)\big)$.

Finally, the recent work of Barg, Guritman and Simonis [5] contains various extensions and generalizations of the Varshamov bound (8) as well as related prior work by Hashim [21], Elia [15], and Edel [14]. However, just as the Hashim bound, most of the results of [5] are non-explicit — they provide methods for constructing codes, but a substantial research effort would be required to convert them into an explicit lower bound on $A_2(n,d)$. On the other hand, [5] does contain the following generalization of Elia's bound: for all $b = 0,1,\ldots,d-1$, if $2^{b-1}V(n-b,d-b-1) < 2^{n-k}$ and there exists an $(n-b,k-1,d)$ code, then $A_2(n,d) \geqslant 2^k$. If we use the Varshamov bound (8) to guarantee the existence of the $(n-b,k-1,d)$ code, then this reduces to $A_2(n,d) \geqslant f_{\mathrm{BGS}}(n,d)$, where

$$f_{\mathrm{BGS}}(n,d) \stackrel{\mathrm{def}}{=} \frac{2^n}{2^b \max\left\{2^{\lfloor \log_2 V(n-b-1,d-2)\rfloor},\ 2^{\lfloor \log_2 V(n-b,d-b-1)\rfloor}\right\}}$$

with b serving as an optimization parameter (note that for $b=1$, we recover the Varshamov bound (8), while for $b=2$ this is precisely the Elia bound). Proceeding as in (11) and (13) while taking into account that $V(n,d-1) \leqslant 2^{b+1}V(n-b-1,d-1)$, it is easy to see that $f_{\mathrm{BGS}}(n,d)/f_{\mathrm{GV}}(n,d) \leqslant 4/\delta$.

III. Gilbert-Varshamov Bound and Locally Sparse Graphs

We first recall some elementary terminology from graph theory. A *graph* G consists of a set of *vertices* $V(G)$ and a set $E(G)$ of pairs of vertices, whose elements are called *edges*. We henceforth assume that both $V(G)$ and $E(G)$ are finite sets. We use $n(G)$ and $e(G)$ to denote, respectively, the number of vertices and the number of edges in G. Two vertices $u,v \in V(G)$ are *adjacent* or *neighbors* in G iff $\{u,v\} \in E(G)$. The set of all neighbors of a vertex v is denoted $N(v)$ and called the *neighborhood* of v. The *degree* of a vertex $v \in V(G)$, denoted $\deg(v)$, is defined as $\deg(v) = |N(v)|$. A graph G is said to be Δ-*regular* if $\deg(v) = \Delta$ for all $v \in V(G)$. A set $K \subseteq V(G)$ is a *clique* if every vertex in K is adjacent to all other vertices in K. A clique consisting of 3 vertices is a *triangle*. A set $\mathcal{I} \subseteq V(G)$ such that no two vertices in $\mathcal{I}$ are adjacent is an *independent set*. A *proper* c-*coloring* of G is a partition of $V(G)$ into c independent sets. The maximum number of vertices in an independent set is called the *independence number* of G, and denoted $\alpha(G)$.

The n-dimensional hypercube $\mathcal{H}_n$ is defined as a graph whose vertex set $V(\mathcal{H}_n)$ is the set of all binary vectors of length n, with $u,v \in V(\mathcal{H}_n)$ being adjacent iff $d(u,v) = 1$, where $d(\cdot,\cdot)$ is the Hamming distance. Note that the graph distance in $\mathcal{H}_n$ is equal to the Hamming distance. Given a minimum distance d, we define the *Gilbert graph* as $\mathcal{H}_n$ to the power $(d-1)$.

Definition. *Let n and $d \leqslant n$ be positive integers. The corresponding* Gilbert graph $\mathcal{G}_{\mathrm{G}}$ *is defined as follows: $V(\mathcal{G}_{\mathrm{G}}) = \mathbb{F}_2^n$ and $\{u,v\} \in E(\mathcal{G}_{\mathrm{G}})$ if and only if $1 \leqslant d(u,v) \leqslant d-1$.*

Clearly, a binary code of length n and minimum distance d is an independent set in the Gilbert graph $\mathcal{G}_{\mathrm{G}}$. Conversely, any independent set in $\mathcal{G}_{\mathrm{G}}$ is a binary code of length n and minimum distance at least d. This proves the following.

Lemma 3.

$$A_2(n,d) \;=\; \alpha(\mathcal{G}_{\rm G}) \tag{17}$$

Lemma 3 makes it possible to recover the Gilbert-Varshamov bound (2) as a straightforward corollary to a simple bound on the independence number of a graph. Since numerous distinct proofs of the GV bound (e.g. using Turán's theorem [5], [38]) abound in the literature, it is somewhat surprising that the simple proof below seems to have not been previously published.

Proposition 4.

$$\alpha(\mathcal{G}_{\rm G}) \;\geqslant\; \frac{2^n}{V(n,d{-}1)} \tag{18}$$

Proof. By definition, the Gilbert graph $\mathcal{G}_{\rm G}$ is Δ-regular with $\Delta = V(n,d{-}1)-1$. Let $\mathcal{I}$ be a *maximal* independent set in $\mathcal{G}_{\rm G}$, and let $\mathcal{E} \subset E(\mathcal{G}_{\rm G})$ be the set of edges with one endpoint in $\mathcal{I}$ and the other in $V(\mathcal{G}_{\rm G}) - \mathcal{I}$. Since $\mathcal{I}$ is an independet set, we have $|\mathcal{E}| = \Delta|\mathcal{I}|$. Since $\mathcal{I}$ is maximal, every vertex of $V(\mathcal{G}_{\rm G}){-}\mathcal{I}$ is adjacent to at least one vertex of $\mathcal{I}$, and so $|\mathcal{E}| \geqslant n(\mathcal{G}_{\rm G}) - |\mathcal{I}|$. Therefore $\alpha(\mathcal{G}_{\rm G}) \geqslant |\mathcal{I}| \geqslant n(\mathcal{G}_{\rm G})/(\Delta{+}1) = 2^n/V(n,d{-}1)$. ∎

Remark. The trivial bound $\alpha(\mathcal{G}_{\rm G}) \geqslant n(\mathcal{G}_{\rm G})/(\Delta{+}1)$ proved in Proposition 4 is well known in graph theory. This bound can be strengthened somewhat using Brooks' theorem [8], [41, p. 20]: since $\mathcal{G}_{\rm G}$ is obviously neither a complete graph nor an odd cycle, it must be Δ-colorable. The largest color class in a proper Δ-coloring of $\mathcal{G}_{\rm G}$ has to contain at least $n(\mathcal{G}_{\rm G})/\Delta$ vertices.

Note that the proof of (18) requires very little information about $\mathcal{G}_{\rm G}$. Thus we can easily improve upon (18) using the fact that the neighborhood $N(v)$ of every vertex v in $\mathcal{G}_{\rm G}$ is fairly sparse. First, we need a couple of well-known results about locally sparse graphs. We say that G is a graph with maximum degree at most Δ if $\deg(v) \leqslant \Delta$ for all $v \in V(G)$.

Lemma 5. *Let G be a graph with maximum degree at most Δ, and suppose that there are no triangles in G. Then*

$$\alpha(G) \;\geqslant\; \frac{n(G)}{8\Delta}\,\log_2\Delta \tag{19}$$

Lemma 5 was first proved by Ajtai, Komlós, and Szemerédi [1] (but see [3, p. 272] for a much shorter proof of the same result). Subsequently, the bound in (19) has been extended from graphs without triangles to graphs with relatively few triangles. In particular, a proof of the following lemma can be found, for example, in Bollobás [7, Lemma 15, p. 296].

Lemma 6. *Let G be a graph with maximum degree at most Δ and suppose that G contains no more than T triangles. Then*

$$\alpha(G) \;\geqslant\; \frac{n(G)}{10\Delta}\left(\log_2\Delta \;-\; {}^1\!/_2\,\log_2\!\left(\frac{T}{n(G)}\right)\right)$$

Observe that a graph has no triangles iff the neighborhood of every vertex is an independent set. If the neighborhood of every vertex is sparse, then the graph will have few triangles. This simple observation is made precise in the following theorem.

Theorem 7. *Let G be a graph with maximum degree at most Δ, and suppose that for all $v \in V(G)$, the subgraph of G induced by the neighborhood of v has at most t edges. Then*

$$\alpha(G) \;\geqslant\; \frac{n(G)}{10\Delta}\left(\log_2\Delta \;-\; {}^1\!/_2\,\log_2\!\left(\frac{t}{3}\right)\right)$$

Proof. The number of triangles containing a given vertex $v \in V(G)$ is equal to the number of edges in the subgraph of G induced by $N(v)$. Thus, for every $v \in V(G)$, there are at most t triangles containing v. Summing the number of triangles containing v over all $v \in V(G)$, we count each triangle in G exactly three times. Hence, the total number of triangles in G is at most $n(G)\,t/3$. The theorem now follows from Lemma 6. ∎

Thus if we can show that $\mathcal{G}_{\rm G}$ is locally sparse (that is, it satisfies the conditions of Theorem 7 for a relatively small value of t), then we can improve upon the Gilbert-Varshamov bound of Proposition 4 by a factor of about $\log_2 V(n,d{-}1)/10$.

IV. How Sparse Is the Sphere Graph?

In this section, we consider the Hamming sphere graph $\mathcal{G}_{\mathcal{S}}$, which is the subgraph of the Gilbert graph $\mathcal{G}_{\rm G}$ induced by the neighborhood $N(\mathbf{0})$ of the vertex $\mathbf{0} \in V(\mathcal{G}_{\rm G})$. Clearly, the subgraph induced in the Gilbert graph by the neighborhood $N(v)$ of any other vertex $v \in V(\mathcal{G}_{\rm G})$ is isomorphic to $\mathcal{G}_{\mathcal{S}}$. Our goal here is to determine how sparse $\mathcal{G}_{\mathcal{S}}$ is. Namely, we would like to compute $e(\mathcal{G}_{\mathcal{S}})$, the number of edges in $\mathcal{G}_{\mathcal{S}}$, and then determine the asymptotic relationship between $e(\mathcal{G}_{\mathcal{S}})$ and the number of vertices in $\mathcal{G}_{\mathcal{S}}$. In view of Lemma 3 and Theorem 7, this would then provide a lower bound on $A_2(n,d) = \alpha(\mathcal{G}_{\rm G})$.

For convenience, let us write $d' = d-1$. Recall that $\lceil x \rceil^+$ denotes the smallest nonnegative integer m such that $m \geqslant x$, for all $x \in \mathbb{R}$. Consider the following simple lemma.

Lemma 8. *Let $v \in V(\mathcal{G}_{\mathcal{S}})$ be a vertex of weight w. Then the degree of v in $\mathcal{G}_{\mathcal{S}}$ is given by*

$$\deg(v) \;=\; \sum_{i=1}^{d'} \sum_{j=\lceil \frac{w+i-d'}{2} \rceil^+}^{\min\{w,i\}} \binom{w}{j}\binom{n-w}{i-j} \;-\; 1$$

Proof. Let $u \in V(\mathcal{G}_{\mathcal{S}})$ be a vertex of $\mathcal{G}_{\mathcal{S}}$ distinct from v, and suppose that $\mathrm{wt}(u) = i$ for some $i \in \{1,2,\ldots,d'\}$. Then $d(u,v) = \mathrm{wt}(u) + \mathrm{wt}(v) - 2|\chi(u) \cap \chi(v)|$, where $\chi(\cdot)$ denotes the support of a vector in $\mathbb{F}_2^n$. Write $j = |\chi(u) \cap \chi(v)|$. Then clearly $j \leqslant \min\{w,i\}$. Furthermore, u and v are adjacent in $\mathcal{G}_{\mathcal{S}}$ if and only if $d(u,v) = w + i - 2j \leqslant d'$. It follows that

$$\sum_{j=\lceil \frac{w+i-d'}{2} \rceil^+}^{\min\{w,i\}} \binom{w}{j}\binom{n-w}{i-j} \tag{20}$$

is the number of vertices of weight i that are adjacent to v, for all $i \neq w$. For $i = w$, we need to subtract 1 from the sum in (20), because the sum counts v itself. ∎

Proposition 9.

$$e(\mathcal{G}_{\mathcal{S}}) \;=\; \frac{1}{2}\sum_{w=1}^{d'}\binom{n}{w}\left(\sum_{i=1}^{d'}\sum_{j=\lceil \frac{w+i-d}{2} \rceil^+}^{\min\{w,i\}}\binom{w}{j}\binom{n-w}{i-j} - 1\right)$$

Proof. Since $\mathcal{G}_{\mathcal{S}}$ has $\binom{n}{w}$ vertices of weight w, this follows immediately from Lemma 8. ∎

Comparing the foregoing expression for $e(\mathcal{G}_{\mathcal{S}})$ with the expression for $e(n,d)$ in Theorem 1, we see that $e(n,d{-}1)$ is equal

to $e(\mathcal{G}_{\mathcal{S}})/3$. Thus Proposition 9 in conjunction with Theorem 7 establish (3). This completes the proof of Theorem 1.

Although Proposition 9 gives an exact expression for $e(\mathcal{G}_{\mathcal{S}})$, the asymptotic form of this expression is not immediately clear. Thus we now turn to asymptotic bounds on $e(\mathcal{G}_{\mathcal{S}})$. Observe that $|V(\mathcal{G}_{\mathcal{S}})| = V(n,d')-1$, so that a complete graph on $V(\mathcal{G}_{\mathcal{S}})$ has $\Omega\big(V(n,d')^2\big)$ edges. In contrast, we will show that under certain conditions, there is an $\varepsilon > 0$ such that $e(\mathcal{G}_{\mathcal{S}}) = o\big(V(n,d')^{2-\varepsilon}\big)$. To this end, the following lemma will be useful.

Lemma 10. *Let u and v be vertices in $V(\mathcal{G}_{\mathcal{S}})$ and suppose that $\mathrm{wt}(v) \leqslant \mathrm{wt}(u)$. Then $\deg(v) \geqslant \deg(u)$.*

Proof. It would suffice to prove that for all $w \in \{2,3,\ldots,d'\}$, we have $\deg(v) \geqslant \deg(u)$ if $\mathrm{wt}(u) = w$ and $\mathrm{wt}(v) = w-1$. Moreover, by Lemma 8 the degree of a vertex u in $\mathcal{G}_{\mathcal{S}}$ depends on u only through its Hamming weight $\mathrm{wt}(u)$. Thus we can assume without loss of generality that

$$\chi(u) = \{1,2,\ldots,w\} \quad \text{and} \quad \chi(v) = \{2,3,\ldots,w\}$$

Now consider $N(u)$ and $N(v)$, the neighborhoods of u and v in $\mathcal{G}_{\mathcal{S}}$. It is easy to see that

$$N(u) - N(v) \;=\; \{\, x \in V(\mathcal{G}_{\mathcal{S}}) \;:\; d(u,x) = d' \text{ and } x_1 = 1 \,\}$$
$$N(v) - N(u) \;=\; \{\, x \in V(\mathcal{G}_{\mathcal{S}}) \;:\; d(v,x) = d' \text{ and } x_1 = 0 \,\}$$

where x_1 denotes the first bit of the vector $x = (x_1, x_2, \ldots, x_n)$ in $V(\mathcal{G}_{\mathcal{S}})$. Let us denote the sets $N(u)-N(v)$ and $N(v)-N(u)$ by $\mathcal{A}$ and $\mathcal{B}$, respectively. Let $\varphi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be the mapping

$$\varphi(x) \;=\; x + (100\cdots0)$$

Note that $\varphi(u) = v$ and $\varphi(v) = u$. We claim that $\varphi(\mathcal{A}) \subseteq \mathcal{B}$. Indeed, let us write $\varphi(x) = y = (y_1, y_2, \ldots, y_n)$. Evidently, if $d(u,x) = d'$ and $x_1 = 1$, then $d(v,y) = d'$ and $y_1 = 0$. Moreover, for all $x \in \mathbb{F}_2^n$ with $x_1 = 1$, the weight of $\varphi(x)$ is $\mathrm{wt}(x)-1$. Thus if $x \in \mathcal{A}$, then $\varphi(x) \in V(\mathcal{G}_{\mathcal{S}})$ unless $x = (100\cdots0)$. However $(100\cdots0) \notin \mathcal{A}$, since the distance between $(100\cdots0)$ and u is given by $w-1 \leqslant d'-1 < d'$. This proves that $\varphi(\mathcal{A}) \subseteq \mathcal{B}$. Since φ is a bijection on $\mathbb{F}_2^n$, the fact that $\varphi(\mathcal{A}) \subseteq \mathcal{B}$ implies that $|\mathcal{A}| \leqslant |\mathcal{B}|$. Hence $|N(v)| \geqslant |N(u)|$, and the lemma follows. ∎

The rest of our asymptotic analysis involves the binary entropy function defined by

$$H_2(x) \;\stackrel{\text{def}}{=}\; -x\log_2 x \;-\; (1-x)\log_2(1-x)$$

for all $0 \leqslant x \leqslant 1$. In particular, we will make frequent use of the following lemma [31, pp. 308-310], which is a well-known estimate for a sum of binomial coefficients.

Lemma 11. *Let $\mu \in \mathbb{R}$, and suppose that μn is an integer in the range $1 \leqslant \mu n \leqslant 0.5n$. Then*

$$\frac{2^{nH_2(\mu)}}{\sqrt{8n\mu(1-\mu)}} \;\leqslant\; \sum_{k=0}^{\mu n}\binom{n}{k} \;\leqslant\; 2^{nH_2(\mu)} \tag{21}$$

Now, let λ be a real number in the range $2/3 \leqslant \lambda < 1$. To simplify notation, we henceforth assume that $d' < 0.5n$ and that $\lambda d'$ is an integer (this obviates the need for numerous $\lceil\cdot\rceil$ and $\lfloor\cdot\rfloor$ functions in what follows). We will derive a bound on $e(\mathcal{G}_{\mathcal{S}})$ by considering separately vertices of weight $< \lambda d'$ and vertices of weight $\geqslant \lambda d'$ in $\mathcal{G}_{\mathcal{S}}$. Thus we write

$$e(\mathcal{G}_{\mathcal{S}}) \;+\; \frac{1}{2}\sum_{i=1}^{d'}\binom{n}{i} \;=\; \frac{e_1(\lambda,n,d) \;+\; e_2(\lambda,n,d)}{2} \tag{22}$$

with

$$e_1(\lambda,n,d) \;\stackrel{\text{def}}{=}\; \sum_{\substack{v\in V(\mathcal{G}_{\mathcal{S}})\\ \mathrm{wt}(v)<\lambda d'}} (\deg(v)+1)$$
$$= \sum_{w=1}^{\lambda d'-1}\binom{n}{w}\sum_{i=1}^{d'}\sum_{j=\left\lceil\frac{w+i-d'}{2}\right\rceil^+}^{\min\{w,i\}}\binom{w}{j}\binom{n-w}{i-j} \tag{23}$$

$$e_2(\lambda,n,d) \;\stackrel{\text{def}}{=}\; \sum_{\substack{v\in V(\mathcal{G}_{\mathcal{S}})\\ \mathrm{wt}(v)\geqslant\lambda d'}} (\deg(v)+1)$$
$$= \sum_{w=\lambda d'}^{d'}\binom{n}{w}\sum_{i=1}^{d'}\sum_{j=\left\lceil\frac{w+i-d'}{2}\right\rceil^+}^{\min\{w,i\}}\binom{w}{j}\binom{n-w}{i-j} \tag{24}$$

where the explicit expressions for $e_1(\lambda,n,d)$ and $e_2(\lambda,n,d)$ follow from Lemma 8 and Proposition 9. Let v be a vertex in $V(\mathcal{G}_{\mathcal{S}})$ with $\mathrm{wt}(v) = 1$. Note that $\lceil(1+i-d')/2\rceil^+ = 0$ for all $i \leqslant d'-1$. Therefore, by Lemma 8, we have

$$\deg(v)+1 \;=\; \sum_{i=1}^{d'-1}\left(\binom{n-1}{i} + \binom{n-1}{i-1}\right) \;+\; \binom{n-1}{d'-1}$$
$$\leqslant\; \sum_{i=1}^{d'}\binom{n}{i} \;\leqslant\; 2^{nH_2(\delta)}$$

where $\delta = d'/n$ and the last inequality follows from Lemma 11. Combining the definition of $e_1(\lambda,n,d)$ in (23) with Lemma 10 thus produces the following bound

$$e_1(\lambda,n,d) \;\leqslant\; 2^{nH_2(\delta)}\sum_{w=1}^{\lambda d'-1}\binom{n}{w} \;\leqslant\; 2^{n\left(H_2(\delta)+H_2(\lambda\delta)\right)} \tag{25}$$

Now, let v be a vertex in $V(\mathcal{G}_{\mathcal{S}})$ with $\mathrm{wt}(v) = \lambda d'$. Then, again by Lemma 8, the degree of v in $\mathcal{G}_{\mathcal{S}}$ is given by

$$\deg(v)+1 \;=\; h_1(\lambda,n,d) \;+\; h_2(\lambda,n,d)$$

with

$$h_1(\lambda,n,d) \;\stackrel{\text{def}}{=}\; \sum_{i=1}^{\mu d'}\sum_{j=0}^{i}\binom{w}{j}\binom{n-w}{i-j} \tag{26}$$

$$h_2(\lambda,n,d) \;\stackrel{\text{def}}{=}\; \sum_{i=\mu d'+1}^{w-1}\sum_{j=\left\lceil\frac{i-\mu d'}{2}\right\rceil}^{i}\binom{w}{j}\binom{n-w}{i-j}$$
$$+\; \sum_{i=w}^{d'}\sum_{j=\left\lceil\frac{i-\mu d'}{2}\right\rceil}^{w}\binom{w}{j}\binom{n-w}{i-j} \tag{27}$$

where we have introduced the notation $w = \lambda d'$ and $\mu = 1-\lambda$. To upper-bound $h_1(\lambda,n,d)$, observe that for all i and j in the

double-sum of (26), we have $j \leqslant i \leqslant \mu d' \leqslant 0.5w$ and therefore $\binom{w}{j} \leqslant \binom{w}{i}$. Thus

$$\begin{aligned} h_1(\lambda,n,d) &\leqslant \sum_{i=1}^{\mu d'} \binom{w}{i} \sum_{j=0}^{i} \binom{n-w}{i-j} \\ &\leqslant \sum_{i=0}^{\mu d'} \binom{w}{i} \sum_{j=0}^{\mu d'} \binom{n-w}{j} \\ &\leqslant 2^{n\lambda\delta H_2\left(\frac{\mu}{\lambda}\right) \,+\, n(1-\lambda\delta)H_2\left(\frac{\mu\delta}{1-\lambda\delta}\right)} \end{aligned} \tag{28}$$

To upper-bound $h_2(\lambda,n,d)$ in (27), we will use the trivial estimate $\binom{w}{j} \leqslant 2^w = 2^{n\lambda\delta}$ for all j (in the case of (27), this estimate is actually not too far off). Thus

$$\begin{aligned} h_2(\lambda,n,d) &\leqslant 2^{n\lambda\delta} \sum_{i=\mu d'+1}^{w-1} \sum_{j=\left\lceil \frac{i-\mu d'}{2} \right\rceil}^{i} \binom{n-w}{i-j} \\ &\quad + 2^{n\lambda\delta} \sum_{i=w}^{d'} \sum_{j=\left\lceil \frac{i-\mu d'}{2} \right\rceil}^{w} \binom{n-w}{i-j} \end{aligned} \tag{29}$$

Since the summation on j in the second double-sum of (29) is up to $w \leqslant i$, we can proceed with the upper bound by uniting the two double-sums as follows

$$\begin{aligned} h_2(\lambda,n,d) &\leqslant 2^{n\lambda\delta} \sum_{i=\mu d'+1}^{d'} \sum_{j=\left\lceil \frac{i-\mu d'}{2} \right\rceil}^{i} \binom{n-w}{i-j} \\ &= 2^{n\lambda\delta} \sum_{i=\mu d'+1}^{d'} \sum_{j=0}^{\left\lfloor \frac{i+\mu d'}{2} \right\rfloor} \binom{n-w}{j} \end{aligned} \tag{30}$$

where the equality in (30) follows by a straightforward change of variables. Finally, observing that $(i+\mu d')/2 \leqslant d' - \frac{\lambda}{2}d'$ for all $i \leqslant d'$, we get

$$\begin{aligned} h_2(\lambda,n,d) &\leqslant 2^{n\lambda\delta} \sum_{i=\mu d'+1}^{d'} \sum_{j=0}^{\left\lfloor d' - \frac{\lambda}{2}d' \right\rfloor} \binom{n-w}{j} \\ &\leqslant n\lambda\delta\, 2^{n\lambda\delta \,+\, n(1-\lambda\delta)H_2\left(\frac{\delta-\frac{\lambda}{2}\delta}{1-\lambda\delta}\right)} \end{aligned} \tag{31}$$

Combining (28) and (31) with the definition of $e_2(\lambda,n,d)$ in (24) and once again invoking Lemma 10, we obtain the following bound

$$e_2(\lambda,n,d) \leqslant \big(\deg(v)+1\big) \sum_{w=\lambda d'}^{d'} \binom{n}{w} \tag{32}$$

$$\leqslant \Big(h_1(\lambda,n,d) + h_2(\lambda,n,d)\Big) \sum_{w=0}^{d'} \binom{n}{w} \tag{33}$$

$$\begin{aligned} &\leqslant 2^{n\left(H_2(\delta)+\lambda\delta H_2\left(\frac{\mu}{\lambda}\right)+(1-\lambda\delta)H_2\left(\frac{\mu\delta}{1-\lambda\delta}\right)\right)} \\ &\quad + n\lambda\delta\, 2^{n\left(H_2(\delta)+\lambda\delta+(1-\lambda\delta)H_2\left(\frac{\delta-\lambda\delta/2}{1-\lambda\delta}\right)\right)} \end{aligned} \tag{34}$$

$$\leqslant (n\lambda\delta+1)\, 2^{n\left(H_2(\delta)+\lambda\delta+(1-\lambda\delta)H_2\left(\frac{\delta-\lambda\delta/2}{1-\lambda\delta}\right)\right)} \tag{35}$$

where (35) follows from the fact that for $2/3 < \lambda < 1$ and $\delta \leqslant 0.5$, the first exponent in (34) is strictly less than the second exponent. We are now ready to prove the following proposition.

Proposition 12. *Let ε and λ be positive real numbers strictly less than 1, with $\lambda \geqslant 2/3$. Then $e(\mathcal{G}_\mathcal{S}) = o\big(V(n,d')^{2-\varepsilon}\big)$, providing $\delta = d'/n$ satisfies the following two conditions:*

$$(1-\varepsilon)\, H_2(\delta) \;>\; H_2(\lambda\delta) \tag{36}$$

$$(1-\varepsilon)\, H_2(\delta) \;>\; \lambda\delta \,+\, (1-\lambda\delta)\, H_2\left(\frac{\delta-\lambda\delta/2}{1-\lambda\delta}\right) \tag{37}$$

Proof. We estimate $e(\mathcal{G}_\mathcal{S})$ by combining (22) with the upper bounds in (25) and (35) on $e_1(\lambda,n,d)$ and $e_2(\lambda,n,d)$. It follows that the ratio $e(\mathcal{G}_\mathcal{S})/V(n,d')^{2-\varepsilon}$ is upper-bounded by

$$\begin{aligned} \frac{e(\mathcal{G}_\mathcal{S})}{V(n,d')^{2-\varepsilon}} &\leqslant \frac{2^{n\left(H_2(\lambda\delta) \,-\, (1-\varepsilon)H_2(\delta)\right)}}{\big(8n\delta(1-\delta)\big)^{\frac{\varepsilon}{2}-1}} \\ &\quad + \frac{(n\lambda\delta+1)\, 2^{n\left(\lambda\delta \,+\, (1-\lambda\delta)H_2\left(\frac{\delta-\lambda\delta/2}{1-\lambda\delta}\right) \,-\, (1-\varepsilon)H_2(\delta)\right)}}{\big(8n\delta(1-\delta)\big)^{\frac{\varepsilon}{2}-1}} \end{aligned}$$

where we used Lemma 11 to bound $V(n,d')$. It is clear that if δ satisfies (36)–(37), then the right-hand side of the above expression tends to zero (exponentially fast) as $n \to \infty$. ∎

Motivated by Proposition 12, we now introduce the functions $f_{\varepsilon,\lambda}(\delta)$ and $g_{\varepsilon,\lambda}(\delta)$ with domain $\delta \in [0, 0.5]$, parametrized by ε and λ and defined as follows

$$\begin{aligned} f_{\varepsilon,\lambda}(\delta) &\stackrel{\text{def}}{=} (1-\varepsilon)\, H_2(\delta) \;-\; H_2(\lambda\delta) \\ g_{\varepsilon,\lambda}(\delta) &\stackrel{\text{def}}{=} (1-\varepsilon)\, H_2(\delta) \;-\; \lambda\delta \;-\; (1-\lambda\delta)\, H_2\left(\frac{\delta-\lambda\delta/2}{1-\lambda\delta}\right) \end{aligned}$$

The two functions $f_{\varepsilon,\lambda}(\delta)$ and $g_{\varepsilon,\lambda}(\delta)$ are plotted in Figure 1 and Figure 2, respectively, for $\varepsilon = 0.000001$ and $\lambda = 0.999$. Figure 3 shows a close-up view of these two functions (for the same ε and λ) in the range $\delta \in [0.499, 0.5]$. It can be seen from Figures 1, 2, and 3 that conditions (36) and (37) of Proposition 12 are satisfied whenever $d'/n \leqslant 0.4994$.

We are now ready to complete the proof of Theorem 2. By Lemma 3, $A_2(n,d) = \alpha(\mathcal{G}_\mathrm{G})$, where $\mathcal{G}_\mathrm{G}$ is the Gilbert graph defined in Section III. The Gilbert graph is a Δ-regular graph on $|V(\mathcal{G}_\mathrm{G})| = 2^n$ vertices with constant degree $\Delta = V(n,d')-1$. The subgraph of $\mathcal{G}_\mathrm{G}$ induced by the neighborhood of any vertex in $V(\mathcal{G}_\mathrm{G})$ is isomorphic to the sphere graph $\mathcal{G}_\mathcal{S}$ and has exactly $e(\mathcal{G}_\mathcal{S})$ edges. Therefore, by Theorem 7, for all $\varepsilon > 0$, we have

$$\begin{aligned} A_2(n,d) &\geqslant \frac{2^n}{V(n,d')} \cdot \frac{\log_2 V(n,d') - 1/2 \log_2 e(\mathcal{G}_\mathcal{S})}{10} \\ &= \frac{2^n}{V(n,d')} \left(\frac{\varepsilon \log_2 V(n,d')}{20} \right. \\ &\qquad \left. + \frac{\log_2 V(n,d')^{2-\varepsilon} - \log_2 e(\mathcal{G}_\mathcal{S})}{20} \right) \end{aligned}$$

By Proposition 12, the ratio $e(\mathcal{G}_\mathcal{S})/V(n,d')^{2-\varepsilon}$ tends to zero for $\varepsilon = 0.000001$, whenever $d'/n < d/n \leqslant 0.4994$ (cf. Figure 3). Therefore, the second fraction in parentheses becomes positive for all sufficiently large n, and Theorem 2 follows.

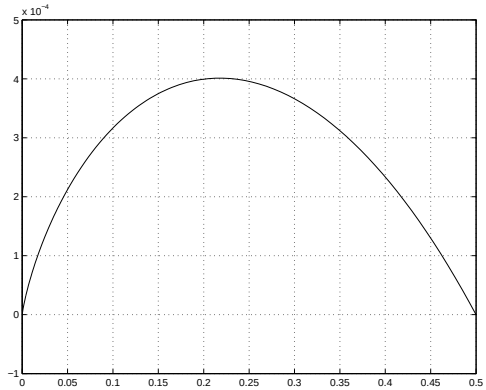

Figure 1. *Plot of the function* $f_{\varepsilon,\lambda}(\delta)$ *for* $\varepsilon = 0.000001$ *and* $\lambda = 0.999$

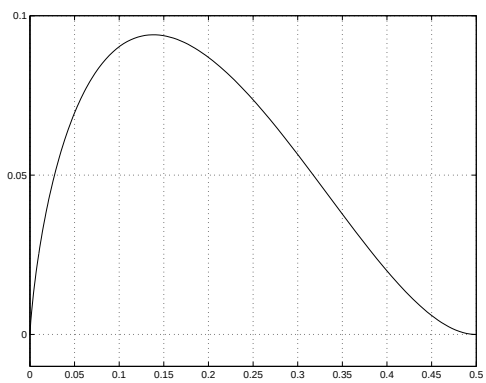

Figure 2. *Plot of the function* $g_{\varepsilon,\lambda}(\delta)$ *for* $\varepsilon = 0.000001$ *and* $\lambda = 0.999$

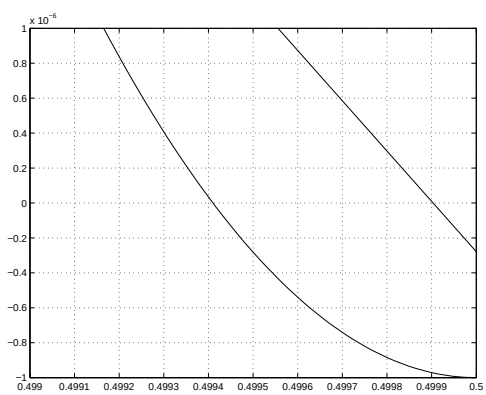

Figure 3. *Close-up view of the functions* $f_{\varepsilon,\lambda}(\delta)$ *and* $g_{\varepsilon,\lambda}(\delta)$ *in the neighborhood of* $\delta = 0.5$ *for* $\varepsilon = 0.000001$ *and* $\lambda = 0.999$

Remark. We note that the degree of a vertex v in $\mathcal{G}_{\mathcal{S}}$ is related to the so-called *intersection numbers* $p^w_{i,k}$ of the Hamming association scheme $\mathcal{H}(n,2)$ — see [13] and [31, Chapter 21] for a detailed description of $\mathcal{H}(n,2)$. Specifically, given any two vectors $u, v \in \mathbb{F}_2^n$ with $d(u,v) = w$, the intersection number $p^w_{i,k}$ is defined as the number of vectors $x \in \mathbb{F}_2^n$ such that $d(x,u) = i$ and $d(x,v) = k$. Thus the sum (20) can be written as

$$p^w_{i,0} + p^w_{i,1} + \cdots + p^w_{i,d'}$$

An explicit expression for $p^w_{i,k}$ is given in [31, p. 656]. However, the proof of Lemma 8 above, which does not use the intersection numbers, appears to be simpler and shorter.

Remark. To get the best threshold on d/n such that (5) holds, one should optimize the value of λ for a given ε in Proposition 12 (alternatively, one could try to directly find the maximum term in the triple-sum of Proposition 9). We have made no special effort to optimize this threshold beyond 0.499. However, we believe that with an appropriate choice of ε, λ in Proposition 12 (or with other methods), one can get as close as desired to the ultimate threshold $d/n \leqslant 0.5$. It is, therefore, surprising that for $\delta = 0.5$, the number of edges in $\mathcal{G}_{\mathcal{S}}$ is very close to $V(n,d')^2$.

Proposition 13. *If* $d'/n = 0.5$, *then* $e(\mathcal{G}_{\mathcal{S}}) \geqslant 0.25 V(n,d')^2$.

Proof. Let $v \in V(\mathcal{G}_{\mathcal{S}})$ be a vertex of weight $d' = n/2$, and let $\mathbf{1}$ denote the all-one vector $(11\cdots1)$ in $\mathbb{F}_2^n$. Then $\mathbf{1} + v$ is another vertex of weight d' in $V(\mathcal{G}_{\mathcal{S}})$. Given any other vertex $u \in V(\mathcal{G}_{\mathcal{S}})$, we have $d(u,v) + d(u,\mathbf{1}+v) = n = 2d'$, so that u is adjacent to at least one of v or $\mathbf{1}+v$. Thus every vertex in $\mathcal{G}_{\mathcal{S}}$ is adjacent to at least half of the vertices of weight d' (excluding, possibly, itself). This implies that

$$\sum_{\substack{v \in V(\mathcal{G}_{\mathcal{S}}) \\ \mathrm{wt}(v) = d'}} (\deg(v) + 1) \;\geqslant\; \frac{1}{2} \sum_{w=1}^{d'} \binom{n}{w} \binom{n}{d'} \tag{38}$$

By Lemma 8, all the vertices of weight d' have the same degree in $\mathcal{G}_{\mathcal{S}}$. Thherefore, it follows from (38) that for *every* $v \in V(\mathcal{G}_{\mathcal{S}})$ with $\mathrm{wt}(v) = d'$, we have

$$\deg(v) + 1 \;\geqslant\; \frac{1}{2} \sum_{w=1}^{d'} \binom{n}{w} \tag{39}$$

Now, by Lemma 10, the degree of all other vertices in $\mathcal{G}_{\mathcal{S}}$ is greater or equal to the degree of a vertex of weight d'. This essentially establishes the proposition. It remains to worry about the fact that the sum on the right-hand side of (39) does not include the term $\binom{n}{0}$ and about the extra 1 on the left-hand side of (39). We omit these tedious details. ∎

Thus it appears that the sphere graph $\mathcal{G}_{\mathcal{S}}$ transitions abruptly from being sparse to being nearly complete at $d'/n = 0.5$. We do not have an intuitive "explanation" for this phenomenon, but note that it is reminiscent of threshold phenomena for codes and graphs observed in [47] and in [33], respectively.

We also note that for $d/n \geqslant 0.5$, the problem of determining $A_2(n,d)$ is essentially settled. Provided enough Hadamard matrices exist, $A_2(2d,d) = 4d$ and $A_2(n,d) = 2\lfloor d/(2d-n) \rfloor$ for all even d with $2d > n$. This is the well-known result of Levenshtein [28], who constructed codes achieving the Plotkin bound [31, pp. 41–43] from Hadamard matrices.

V. Generalizations and Open Problems

The well-known proofs by Gilbert [18] and Varshamov [42] of the bounds in (2) and (8), respectively, are "constructive" in that they provide simple (but exponential-time) algorithms to construct codes whose parameters meet or exceed the corresponding bounds. Moreover, Gilbert's "constructive" argument [18] has been extended to quite general contexts [20], [38], [46] using the so-called altruistic algorithm (which is also exponential-time).

We would like to point out that the bound of Theorem 2 is "constructive" in the same sense as [20], [38], [42], and [46].

Hofmeister and Lefmann [22] provide an algorithm which, given any Δ-regular graph G with at most $n(G)\Delta^{2-\varepsilon}$ triangles, finds an independent set of size at least $\Omega(n(G)\log_2(\Delta)/\Delta)$ in G. By the results of Section IV, the Gilbert graph $\mathcal{G}_{\mathrm{G}}$ contains at most $O(n(\mathcal{G}_{\mathrm{G}})\Delta^{2-\varepsilon})$ triangles whenever $d/n \leqslant 0.499$. Thus, when applied to the Gilbert graph $\mathcal{G}_{\mathrm{G}}$, the Hofmeister-Lefmann algorithm [22] will produce codes satisfying (5). The Hofmeister-Lefmann algorithm runs in time that is polynomial in the size of $\mathcal{G}_{\mathrm{G}}$ but, of course, exponential in the code length n.

Up to now, for the sake of brevity, we have focused exclusively on binary codes. Nevertheless, it should be clear that Theorems 1 and 2 can be generalized to arbitrary alphabets of size q, where q need not even be a prime power. Here, we give a generalization to q-ary alphabets of Theorem 1.

Theorem 14. *Let q, n, and d be positive integers with $d \leqslant n$ and $q \geqslant 2$. Define the volume of a q-ary Hamming sphere of radius d as $V_q(n,d) = \sum_{i=0}^{d}\binom{n}{i}(q-1)^i$, and let*

$$e_q(n,d) \stackrel{\text{def}}{=} \frac{1}{6}\sum_{w=1}^{d}\sum_{i=1}^{d}\sum_{j=1}^{a}\sum_{k=b}^{a-j}\frac{n!\,(q-2)^k(q-1)^{w+i-c}}{j!\,k!\,(w-c)!\,(i-c)!\,(n+c-w-i)!} - \frac{V_q(n,d)}{6}$$

where $a \stackrel{\text{def}}{=} \min\{w,i\}$, $c \stackrel{\text{def}}{=} j+k$, and b is the smallest nonnegative integer that is greater or equal to $(w+i)-j-\min\{d+j,n\}$. Then

$$A_q(n,d) \geqslant \frac{q^n}{V_q(n,d-1)}\cdot\frac{\log_2 V_q(n,d-1) - \log_2\sqrt{e_q(n,d-1)}}{10} \tag{40}$$

Proof. Let $\mathcal{A}$ be an alphabet with q letters. We define the q-ary Gilbert graph $\mathcal{G}_{q,\mathrm{G}}$ as before, namely $V(\mathcal{G}_{q,\mathrm{G}}) = \mathcal{A}^n$ and $\{u,v\} \in E(\mathcal{G}_{q,\mathrm{G}})$ if and only if $1 \leqslant d(u,v) \leqslant d'$. Then $\mathcal{G}_{q,\mathrm{G}}$ is Δ-regular with $\Delta = V_q(n,d')-1$, and Theorem 7 applies. It remains to count the number of edges in the graphs induced in $\mathcal{G}_{q,\mathrm{G}}$ by the neighborhoods of its vertices. Without loss of generality, we can call any one of the letters of $\mathcal{A}$ "zero," and consider the graph $\mathcal{G}_{q,\mathcal{S}}$ which is induced in the q-ary Gilbert graph by the neighborhood $N(\mathbf{0})$ of the vertex $\mathbf{0} \in \mathcal{A}^n$.

Let $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$ be two vertices of $\mathcal{G}_{q,\mathcal{S}}$ with $\mathrm{wt}(v) = w$ and $\mathrm{wt}(u) = i$ (observe that Hamming weight is well-defined, once we have identified a $0 \in \mathcal{A}$). Let

$$j \stackrel{\text{def}}{=} \big|\{l : u_l = v_l, v_l \neq 0, u_l \neq 0\}\big|$$
$$k \stackrel{\text{def}}{=} \big|\{l : u_l \neq v_l, v_l \neq 0, u_l \neq 0\}\big|$$

It is obvious that $j \leqslant \min\{w,i\}$. Further, if j is already fixed, then clearly $k \leqslant \min\{w,i\} - j$. Moreover, $w-k-j$ is the number of positions l such that $v_l \neq 0$ and $u_l = 0$. This number cannot be greater than $n - \mathrm{wt}(u) = n-i$, which implies that $k \geqslant (w+i)-j-n$. Finally, it is easy to see that

$$d(u,v) = w+i-2j-k$$

so that the vertices u and v are adjacent in $\mathcal{G}_{q,\mathcal{S}}$ if and only if $k \geqslant (w+i)-j-(d'+j)$. Putting all this together, we can enumerate the total number of vertices of weight $i \neq w$ that are adjacent in $\mathcal{G}_{q,\mathcal{S}}$ to a fixed vertex $v \in V(\mathcal{G}_{q,\mathcal{S}})$ of weight $\mathrm{wt}(v) = w$ as follows

$$\sum_{j=0}^{a}\sum_{k=b}^{a-j}\binom{w}{j}\binom{w-j}{k}(q-2)^k\binom{n-w}{i-c}(q-1)^{i-c} \tag{41}$$

where a, b, and c are as defined in the theorem. For $i = w$, we again need to subtract 1 from the sum in (41) since the sum then counts v itself. Enumerating over all possible values of i, we find that the degree of v in $\mathcal{G}_{q,\mathcal{S}}$ is given by

$$\sum_{i=1}^{d'}\sum_{j=0}^{a}\sum_{k=b}^{a-j}\binom{w}{j}\binom{w-j}{k}\binom{n-w}{i-c}(q-2)^k(q-1)^{i-c} - 1 \tag{42}$$

The total number of vertices of weight w in $\mathcal{G}_{q,\mathcal{S}}$ is $\binom{n}{w}(q-1)^w$. Combining this with (42) produces an expression for $e(\mathcal{G}_{q,\mathcal{S}})$, and it is easy to see that $e_q(n,d-1) = e(\mathcal{G}_{q,\mathcal{S}})/3$. ∎

Remark. We could have used the intersection numbers $p^w_{i,j}$ of the Hamming association scheme $\mathcal{H}(n,q)$ in the proof of Theorem 14. Specifically, the sum in (41) can again be written as $p^w_{i,0} + p^w_{i,1} + \cdots + p^w_{i,d'}$. Therefore

$$e(\mathcal{G}_{q,\mathcal{S}}) = \frac{1}{2}\sum_{w=1}^{d'}\sum_{i=1}^{d'}\sum_{j=1}^{d'}\binom{n}{w}p^w_{i,j}\,(q-1)^w$$

with the convention that $p^w_{i,j} = 0$ when $w > i+j$. A formula for the intersection numbers of the q-ary Hamming scheme $\mathcal{H}(n,q)$ may be found in [5, eq. (2)]. While the resulting expression for $e_q(n,d)$ is shorter than its counterpart in Theorem 14, we prefer the latter since it is more explicit.

In the original version of this paper, we have left the asymptotic investigation of the bound in Theorem 14 as an open problem, and conjectured that it should lead to

$$A_q(n,d) \geqslant c\,\frac{q^n}{V_q(n,d-1)}\,\log_2 V_q(n,d-1) \tag{43}$$

for some positive constant c. This conjecture has been proved in the recent work of Vu and Wu [43]. Specifically, Vu and Wu [43] show that if $d/n < (q-1)/q$, then (43) holds for a constant c that depends on the ratio d/n. They also give an explicit, though rather elaborate, expression for c in terms of d/n.

Our general approach can be extended to many other situations where generalizations of the Gilbert-Varshamov bound are currently used. We give just one concrete example.

Let $A(n,2d,w)$ denote the the maximum number of codewords in a binary code of length n, constant weight w, and minimum Hamming distance $2d$. Levenshtein [29] has generalized the Gilbert bound (2) to constant-weight codes. It is shown in [29] that

$$A(n,2d,w) \geqslant \frac{|\mathbb{F}_2(n,w)|}{V(n,d-1,w)} = \frac{\binom{n}{w}}{\sum_{i=0}^{d-1}\binom{w}{i}\binom{n-w}{i}} \tag{44}$$

where $\mathbb{F}_2(n,w)$ is the set of binary vectors of length n and weight w and $V(n,d,w)$ is the volume of a sphere of radius d in the Johnson metric. Using the same approach as in Theorems 1 and 14, we can improve upon the bound in (44) as follows.

Theorem 15. *Let n, d, and w be three positive integers such that $d \leqslant w \leqslant n/2$. For positive integers i, j, k, all less than or equal to w, define $p_{i,j}^k$ as follows*

$$p_{i,j}^k \stackrel{\text{def}}{=} \sum_{l=a}^{b} \binom{n-w-k}{l} \binom{k}{i-l} \binom{k}{j-l} \binom{w-k}{i+j-k-l} \tag{45}$$

for all $k \leqslant i+j$, where

$$a \stackrel{\text{def}}{=} \max\{0, i-k, j-k, i+j-w\}$$
$$b \stackrel{\text{def}}{=} \min\{i, j, i+j-k, n-w-k\}$$

Set $p_{i,j}^k = 0$ for $k > i+j$, and define the following quantity

$$e(n,d,w) \stackrel{\text{def}}{=} \frac{1}{6} \sum_{i=1}^{d} \sum_{j=1}^{d} \sum_{k=1}^{d} \binom{w}{k} \binom{n-w}{k} p_{i,j}^k \tag{46}$$

Then

$$A(n,2d,w) \geqslant \frac{|\mathbb{F}_2(n,w)|}{V(n,d-1,w)} \cdot \frac{\log_2 V(n,d-1,w) - \log_2 \sqrt{e(n,d-1,w)}}{10}$$

Proof. The underlying "Gilbert graph" $\mathcal{G}$ can be defined as follows: $V(\mathcal{G}) = \mathbb{F}_2(n,w)$ and $\{u,v\} \in E(\mathcal{G})$ if and only if $2 \leqslant d(u,v) \leqslant 2d'$. Now fix a vertex $z \in V(\mathcal{G})$ and consider the graph $\mathcal{G}_{\mathcal{S}}$ that is induced in $\mathcal{G}$ by the neighborhood $N(z)$. Clearly, all such graphs are isomorphic. The numbers $p_{i,j}^k$ in (45) are precisely the intersection numbers of the Johnson association scheme [31, p. 665]. It follows that if v is a vertex of $\mathcal{G}_{\mathcal{S}}$ such that $d(z,v) = 2k$, then the degree of v in $\mathcal{G}_{\mathcal{S}}$ is given by

$$\deg(v) = \sum_{i=1}^{d'} \sum_{j=1}^{d'} p_{i,j}^k$$

Hence $e(\mathcal{G}_{\mathcal{S}}) = 3e(n,d-1,w)$, where $e(n,d,w)$ is the quantity defined in (46). The desired bound on $A(n,2d,w)$ now follows, as before, from Theorem 7. ∎

We leave the asymptotic analysis of Theorem 15 as an open problem for future research.

In the original version of this paper, we have also suggested the following problem: generalize the results of Theorem 1 and Theorem 2 to lattices and sphere-packings, where the counterpart of the Gilbert-Varshamov bound is the Minkowski-Hlawka theorem [12], [30]. This problem was recently solved in [27]. Specifically, Krivelevich, Litsyn, and Vardy [27] show that using graph-theoretic methods similar to those of Section III, the classical Minkowski bound [34] on the density of sphere packings in $\mathbb{R}^n$ can be also improved by a factor that is linear in n.

Other interesting problems for future work would be the extension of Theorems 1 and 2 to spherical codes [44], to covering codes [11, Section 12.1], to codes correcting arbitrary error patterns [30], to runlength-limited codes [24], and to more general constrained systems [32]. The general approach introduced in this paper should work whenever an underlying "Gilbert graph" can be defined, and happens to be locally sparse.

Our results herein have applications outside of coding theory as well. For example, the following problem arises in the study of scalability of optical networks [36]. Let $\mathcal{H}_n$ be the n-dimensional hypercube, defined in Section III. What is the minimum number $\chi_d(n)$ of colors needed to color the vertices of $\mathcal{H}_n$ so that vertices at distance $\leqslant d$ from each other have different colors? Ngo, Du, and Graham [35] have recently established the following bound

$$\chi_d(n) \leqslant 2^{\lfloor \log_2 V(n-1,d-1) \rfloor + 1} = \frac{2}{2^{\{\log_2 V(n-1,d-1)\}}} V(n-1,d-1) \tag{47}$$

In fact, this follows immediately from the Varshamov bound (8), since given any *linear* binary code $\mathbb{C}$, assigning different colors to the cosets of $\mathbb{C}$ in $\mathbb{F}_2^n$ produces a valid coloring. While Theorems 1 and 2 improve upon (8), unfortunately, we do not know whether there exist *linear* codes that attain (3) and/or (5). Nevertheless, we can still improve upon (47), as follows: if $d/n \leqslant 0.499$, then there exists a positive constant c such that

$$\chi_d(n) \leqslant c \frac{V(n,d)}{\log_2 V(n,d)} \tag{48}$$

This uses a result of Alon, Krivelevich, and Sudakov [2], who show that locally sparse graphs with maximum degree Δ can be colored using $O(\Delta/\log \Delta)$ colors. Specifically, let G be a graph with maximum degree Δ such that the number of edges in the subgraphs induced in G by the neighborhood of any vertex is at most Δ^2/f. Then it is proved in [2, Theorem 1.1] that the chromatic number $\chi(G)$ of G satisfies $\chi(G) \leqslant c_1 \Delta/\log_2 f$ for some positive constant c_1. Since the Gilbert graph $\mathcal{G}_{\mathrm{G}}$, defined in Section III, is $\mathcal{H}_n$ to the power $(d-1)$, it should be clear that $\chi_{d-1}(n) = \chi(\mathcal{G}_{\mathrm{G}})$. The Gilbert graph $\mathcal{G}_{\mathrm{G}}$ has maximum degree $\Delta = V(n,d-1) - 1$. Moreover, we have shown in the previous section that this graph is locally sparse: if $\mathcal{G}_{\mathcal{S}}$ is the graph induced in $\mathcal{G}_{\mathrm{G}}$ by the neighborhood of any vertex $v \in V(\mathcal{G}_{\mathrm{G}})$, then $e(\mathcal{G}_{\mathcal{S}}) \leqslant c_2 \Delta^2/V(n,d-1)^{\varepsilon}$ for $\varepsilon = 0.000001$ and some positive constant c_2, provided $d/n \leqslant 0.499$. Combining this with [2, Theorem 1.1] establishes (48).

Finally, we would like to point out some questions concerning Theorems 1 and 2 that remain open. Our proof of these theorems gives no hint of linearity. Nevertheless, we ask: are there linear codes whose parameters satisfy (5)? It is conceivable that a suitable modification of the Varshamov [42] argument for constructing a parity-check matrix could produce such codes. It is well known that a random (linear) code meets the Gilbert-Varshamov bound with probability approaching 1 as $n \to \infty$. Thus we ask: do random codes also meet the improved version of this bound in Theorem 2? Progress on this question was recently reported by Cohen [10]. Of course, the most interesting question of all is whether the term $\log n$ in (7) can be further improved to a linear term. In other words, it it true that the Gilbert-Varshamov bound on the rate of binary codes is asymptotically exact?

ACKNOWLEDGMENT

We are grateful to Alexander Barg for helpful discussions about [5]. We would also like to thank Gérard Cohen, Ralf Koetter, Van Vu, and the anonymous referees for valuable comments.

REFERENCES

[1] M. AJTAI, J. KOMLÓS, AND E. SZEMERÉDI, A note on Ramsey numbers, *J. Combinatorial Theory (A)*, **29**, (1980), 354–360.

[2] N. ALON, M. KRIVELEVICH, AND B. SUDAKOV, Coloring graphs with sparse neighborhoods, *J. Combinatorial Theory (B)*, **77**, (1999), 73–82.

[3] N. ALON AND J. SPENCER, *The Probabilistic Method*, 2-nd edition, New York: John Wiley & Sons, 2000.

[4] A. ASHIKHMIN, A. BARG, AND S. LITSYN, Estimates of the distance distribution of codes and designs, *IEEE Trans. Inform. Theory*, **47**, (2001), 1050–1061.

[5] A. BARG, S.GURITMAN, AND J. SIMONIS, Strengthening the Gilbert-Varshamov bound, *Linear Algebra Appl.*, **307**, (2000), 119–129.

[6] E.R. BERLEKAMP AND J. JUSTESEN, Some long cyclic linear binary codes are not so bad, *IEEE Trans. Inform. Theory*, **20**, (1974), 351–356.

[7] B. BOLLOBÁS, *Random Graphs*, London: Academic Press, 1985.

[8] R.L. BROOKS, On colouring the nodes of a network, *Proc. Cambridge Philos. Soc.* **37**, (1941), 194–197.

[9] P. CHEN, T. LEE, AND Y.S. HAN, Distance-spectrum formulas on the largest minimum distance of block codes, *IEEE Trans. Inform. Theory*, **46**, (2000), 869–885.

[10] G.D. COHEN, private communication, January 2004.

[11] G.D. COHEN, I. HONKALA, S. LITSYN, AND A. LOBSTEIN, *Covering Codes*, Amsterdam: North-Holland/Elsevier, 1997.

[12] J.H. CONWAY AND N.J.A. SLOANE, *Sphere Packings, Lattices, and Groups*, New York: Springer-Verlag, 1988.

[13] PH. DELSARTE, An algebraic approach to the association schemes of coding theory, *Philips J. Research*, **10**, (1973), 1–97.

[14] Y. EDEL, *Eine Verallgemeinerung von BCH-Codes*, Ph.D. Thesis, University of Heidelberg, 1996, (in German).

[15] M. ELIA, Some results on the existence of binary linear codes, *IEEE Trans. Inform. Theory*, **29**, (1983), 933–934.

[16] N.D. ELKIES, Still better nonlinear codes from modular curves, e-print, `http://arXiv.org/abs/math.NT/0308046`, August 2003.

[17] F. FABRIS, Sharpening the Gilbert-Varshamov bound in the finite case, *J. Discrete Math. Sci. Cryptography*, **4**, (2001), 65–75.

[18] E.N. GILBERT, A comparison of signalling alphabets, *Bell Syst. Tech. J.*, **31**, (1952), 504–522.

[19] V.D. GOPPA, Bounds for codes, *Dokl. Acad. Nauk*, **333**, (1993), 423.

[20] J. GU AND T.E. FUJA, A generalized Gilbert-Varshamov bound derived via analysis of a code-search algorithm, *IEEE Trans. Inform. Theory*, **39**, (1993), 1089–1093.

[21] A.A. HASHIM, Improvement on Varshamov-Gilbert lower bound on minimum Hamming distance of linear codes, *Proc. Inst. Elec. Engrs.*, **125**, (1978), 104–106.

[22] T. HOFMEISTER AND H. LEFMANN, Independent sets in graphs with triangles, *Inform. Process. Lett.*, **58**, (1996), 207–210.

[23] G. KALAI AND N. LINIAL, On the distance distribution of codes, *IEEE Trans. Inform. Theory*, **41**, (1995), 1467–1472.

[24] V.D. KOLESNIK AND V.Y. KRACHKOVSKY, Generating functions and lower bounds on rates for limited error-correcting codes, *IEEE Trans. Inform. Theory*, **37**, (1991), 778-788.

[25] I. KRASIKOV AND S. LITSYN, On the accuracy of the binomial approximation to the distance distribution of codes, *IEEE Trans. Inform. Theory*, **41**, (1995), 1472–1474.

[26] I. KRASIKOV AND S. LITSYN, Bounds on spectra of codes with known dual distance, *Des. Codes Cryptogr.*, **13**, (1998), 285–297.

[27] M. KRIVELEVICH, S. LITSYN, AND A. VARDY, A lower bound on the density of sphere packings via graph theory, *International Math. Research Notices*, to appear.

[28] V.I. LEVENSHTEIN, The application of Hadamard matrices to a problem in coding, *Probl. Kibernetiki*, **5**, (1961), 123–136, (in Russian).

[29] V.I. LEVENSHTEIN, Upper bound estimates for fixed-weight codes, *Probl. Inform. Transmission*, **7**, (1971), 281–287.

[30] H.-A. LOELIGER, Averaging bounds for lattices and linear codes, *IEEE Trans. Inform. Theory*, **43**, (1997), 1767–1773.

[31] F.J. MACWILLIAMS AND N.J.A. SLOANE, *The Theory of Error Correcting Codes*, Amsterdam: North-Holland/Elsevier, 1977.

[32] B.H. MARCUS AND R.M. ROTH, Improved Gilbert-Varshamov bound for constrained systems, *IEEE Trans. Inform. Theory*, **38**, (1992), 1213–1221.

[33] G. MARGULIS, Probabilistic characteristics of graphs with large connectivity, *Probl. Peredachi Inform.*, **10**, (1974), 101–108, (in Russian).

[34] H. MINKOWSKI, Diskontinuitäsbereich für arithmetische Aequivallenz, *J. Reine Angew. Math.*, **129**, 1905, 220–274.

[35] H.Q. NGO, D.-Z. DU, AND R.L. GRAHAM, New bounds on a hypercube coloring problem, *Inform. Process. Lett.*, **84**, (2002), 265–269.

[36] A. PAVAN, P.-J. WAN, S.-R. TONG, AND D.H.C. DU, A new multihop lightwave network based on the generalized de-Bruijn graph, *Proc. 21-st IEEE Conf. Local Computer Networks*, (1996), 498–507.

[37] V.S. PLESS AND W.C. HUFFMAN (Editors), *Handbook of Coding Theory*, Amsterdam: North-Holland/Elsevier, 1998.

[38] L.M.G.M. TOLHUIZEN, The generalized Gilbert-Varshamov bound is implied by Turán's theorem, *IEEE Trans. Inform. Theory*, **43**, (1997), 1605–1606.

[39] M.A. TSFASMAN AND S.G. VLĂDUŢ, *Algebraic Geometry Codes*, Dodrecht: Kluwer Academic Publishers, 1991.

[40] M.A. TSFASMAN, S.G. VLĂDUŢ, AND T. ZINK, Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound, *Mathematische Nachrichten*, **104**, (1982), 13–28.

[41] J.H. VAN LINT AND R.M. WILSON, *A Course in Combinatorics*, Cambridge, UK: Cambridge University Press, 1992.

[42] R.R. VARSHAMOV, Estimate of the number of signals in error correcting codes, *Dokl. Acad. Nauk*, **117**, (1957), 739–741, (in Russian).

[43] V. VU AND L. WU, Improving the Gilbert-Varshamov bound for q-ary codes, manuscript in preparation, March 2004.

[44] A.D. WYNER, Random packings and coverings of the unit n-sphere, *Bell Syst. Tech. Journal*, **46**, (1967), 2111–2118.

[45] C. XING, Nonlinear codes from algebraic curves improving the Tsfasman-Vlăduţ-Zink bound, *IEEE Trans. Inform. Theory*, **49**, (2003), 1653–1657.

[46] Ø. YTREHUS, *Codes for Error Control*, Ph.D. Thesis, University of Bergen, Norway, 1989.

[47] G. ZÉMOR AND G.D. COHEN, The threshold probability of a code, *IEEE Trans. Inform. Theory*, **41**, (1995), 469–477.

[48] V.A. ZINOVIEV AND S. LITSYN, On codes exceeding the Gilbert bound, *Probl. Peredachi Inform.*, **21**, (1985), 109–111, (in Russian).