# Improvement of the Gilbert-Varshamov Bound and Random Geometric Graphs

Ghid Maatouk
ALGO, I&C, EPFL

***Abstract*—The Gilbert-Varshamov (GV) bound is a fundamental lower bound in coding theory. We present an asymptotic improvement of the GV bound on the size of binary codes, by a factor linear in the code length [1]. This result relies on lower bounding the independence number of locally sparse graphs. We then describe a recent proof [2] that this bound is met by linear codes, namely, by an infinite family of double circulant codes. These improvements on the GV bound raise many interesting questions. One of them is whether the analysis in [1] makes full use of the properties of the underlying graph. We introduce the concept of random geometric graphs as they appear in [3] and propose to study the properties of these graphs with the goal of applying tools and techniques from this area to the problem of lower bounding the maximum size of codes.**

***Index Terms*—Binary codes, Gilbert-Varshamov bound, locally sparse graphs, linear codes, double circulant codes, random geometric graphs.**

## I. Introduction

Let $A_q(n,d)$ be the maximum size of a $q$-ary code of length $n$ and minimum distance $d$. The well-known Gilbert-Varshamov (GV) bound gives a lower bound on $A_q(n,d)$ in terms of $n$ and $d$. More specifically, it states that

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

We concern ourselves here with the binary case, where the GV bound can be expressed by the following theorem.

*Theorem 1: [Gilbert-Varshamov bound]*

$$A_2(n,d) \geq \frac{2^n}{V(n,d-1)}, \quad (1)$$

where $V(n,d-1) = \sum_{i=0}^{d-1} \binom{n}{i}$ is the volume of a Hamming ball of radius $d-1$.

For the nonlinear case, a simple greedy procedure yields this lower bound. For the linear case, a probabilistic proof based on choosing a parity check matrix at random and using the union bound to upper bound the probability of "bad events" shows that a random linear code achieves this bound with probability going to 1 as $n$ goes to infinity. In the binary case, despite the simplicity of these existential proofs, no explicit code constructions achieving the GV bound are known.

Let $f_{GV}(n,d) = \frac{2^n}{V(n,d-1)}$, i.e., $f_{GV}(n,d)$ is the lower bound on the maximum size of a binary code provided by Theorem 1. Jiang and Vardy [1] review prior improvements of the GV bound and show that all such improvements provide lower bounds on $A_2(n,d)$ which are linear in $f_{GV}(n,d)$. They derive a new lower bound that is of the order of $nf_{GV}(n,d)$, which we discuss in the next section. The novelty of their analysis lies in their reframing the problem of lower bounding the maximum size of a code into a graph-theoretical setting. Their analysis does not answer the question of whether this lower bound is met by linear codes. However, Gaborit and Zémor [2] proved that this is indeed the case by showing that an infinite family of double circulant codes satisfy the GV bound. We describe their work in section III. In section IV, we introduce the notion of random geometric graphs and motivate our choice to explore such structures. We discuss the graph model used in McDiarmid's work on random channel assignment in the plane [3] and outline some proofs showing the kind of tools and techniques used in the field. We conclude with a discussion of the relevance of such models and tools to the problem of lower bounding the maximum size of codes.

## II. An Asymptotic Improvement of the GV Bound

Jiang and Vardy [1] rely on graph-theoretical methods to prove that there exist families of nonlinear binary codes that

Proposal submitted to committee: July 10th, 2009; Candidacy exam date: July 16th, 2009; Candidacy exam committee: Rüdiger Urbanke, Amin Shokrollahi, Friedrich Eisenbrand.

This research plan has been approved:

Date: _____

Doctoral candidate: Ghid Maatouk (name and signature)

Thesis director: _____ (name and signature)

Thesis co-director: _____ (if applicable) (name and signature)

Doct. prog. director: _____ (R. Urbanke) (signature)

satisfy the following lower bound on the code size.

*Theorem 2:* [1] Let $n$ and $d$ be positive integers, with $d/n \leq 0.499$. Then there exists a positive constant $c$ such that

$$A_2(n,d) \geq c\frac{2^n}{V(n,d-1)} \log_2 V(n,d-1). \qquad (2)$$

Let us first check that this lower bound indeed improves the GV bound by a factor of $n$. Recall that $V(n,d-1)$ is given by

$$V(n,d-1) = \sum_{i=0}^{d-1} \binom{n}{i}.$$

For $\delta = d/n$ constant and strictly less than 0.5, the largest term in this sum is $\binom{n}{d-1} = \Theta(2^{n(H(\delta)+o(1))})$, so that

$$V(n,d-1) = \Theta(2^{n(H(\delta)+o(1))}).$$

The factor of $\log_2 V(n,d-1)$ is thus linear in $n$. Note that asymptotically, this constitutes an improvement in the maximum *size* of a code, not in the best achievable *rate* $r(n,d) = \log_2 A_2(n,d)/n$. The GV bound on the rate of binary codes is conjectured to be asymptotically exact.

In short, the idea behind Jiang and Vardy's bound is to restate the problem in a graph-theoretical setting. More specifically, they view codes as independent sets in a certain graph. The maximum size of a code thus becomes the maximum size of an independent set in this graph. They then prove that the graph they consider is "locally sparse" and use a lower bound on the independence number of such a graph to derive a lower bound for $A_2(n,d)$ in terms of the number of edges in the neighborhood of any given vertex. They finally use asymptotic analysis to derive the lower bound in (2).

### A. The Gilbert Graph is Locally Sparse

We start by defining the Gilbert graph, which is the locally sparse graph used by Jiang and Vardy in their analysis. The Gilbert graph $\mathcal{G}_G$ has vertex set equal to the set of all binary vectors of length $n$, and two vertices are adjacent if and only if the Hamming distance of the corresponding vectors is less than or equal to $d-1$. More formally,

*Definition 1:* For $n$ and $d \leq n$ positive integers, let $V = \mathbb{F}_2^n$ and $E = \{\{u,v\} : 1 \leq d(u,v) \leq d-1\}$. Then the corresponding Gilbert graph is the graph $\mathcal{G}_G = G(V,E)$.

It is easy to see that a code of length $n$ and minimum distance $d$ is nothing but an independent set in the corresponding Gilbert graph. Thus $A_2(n,d) = \alpha(\mathcal{G}_G)$, where $\alpha(\mathcal{G}_G)$ denotes the independence number of the Gilbert graph $\mathcal{G}_G$. Noting this, and using the fact that the Gilbert graph is $\Delta$-regular with $\Delta = V(n,d-1)-1$, Jiang and Vardy [1] readily rederive the GV bound using a trivial lower bound on the independence number of a graph of maximal degree $\Delta$, namely,

$$\alpha(\mathcal{G}_G) \geq \frac{n(\mathcal{G}_G)}{\Delta+1} = \frac{2^n}{V(n,d-1)}.$$

Deriving the GV bound from this trivial lower bound requires no knowledge of any special structure in $\mathcal{G}_G$. To refine their lower bound, Jiang and Vardy make use of an additional property of $\mathcal{G}_G$: local sparsity. Namely, they derive an exact expression for the number of edges in the neighborhood of any vertex, and use this expression in order to get a better lower bound on $\alpha(\mathcal{G}_G)$. For this, they use the following theorem, which relates a lower bound on the independence number of a graph to the maximum number of edges in any local neighborhood of this graph.

*Theorem 3:* [1] Let $G$ be a graph with maximum degree at most $\Delta$, 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

$$\alpha(G) \geq \frac{n(G)}{10\Delta}\left(\log_2 \Delta - \frac{1}{2}\log_2\left(\frac{t}{3}\right)\right).$$

In order to get an exact expression for the number of edges in the neighborhood of any vertex, Jiang and Vardy use a counting argument. They restrict their attention to the subgraph induced by the neighborhood of the vertex $\mathbf{0}$, i.e., the Hamming sphere graph $\mathcal{G}_S$; note that the neighborhood of any other vertex of the Gilbert graph is simply a translate of $\mathcal{G}_S$. They double-count the number $e(\mathcal{G}_S)$ of vertices in this subgraph by summing the degrees of its vertices. They obtain the degree of each vertex by counting the number of other vertices of each possible weight that are adjacent to this vertex. They finally obtain an expression for $e(\mathcal{G}_S)$, which, used in conjunction with Theorem 3, gives a lower bound for $A_2(n,d)$.

*Proposition 1:* [1]

$$e(\mathcal{G}_S) = \frac{1}{2}\sum_{w=1}^{d-1}\binom{n}{w}\left(\sum_{i=1}^{d-1}\sum_{j=\lceil\frac{w+i-d}{2}\rceil^+}^{\min\{w,i\}}\binom{w}{j}\binom{n-w}{i-j} - 1\right), \qquad (3)$$

where $\lceil x\rceil^+$ denotes the smallest nonnegative integer larger than or equal to $x$.

### B. Asymptotic Analysis

How does $e(\mathcal{G}_S)$ behave asymptotically? To answer this question, Jiang and Vardy upper bound separately the sum of the degrees of the vertices of "low weight", and the sum of the degrees of the vertices of "high weight" in the sphere graph $\mathcal{G}_S$, where the cutoff weight is $\lambda(d-1)$ for some tunable parameter $\lambda$, which is is a real number in the range $[2/3, 1)$. Their analysis results in the following proposition.

*Proposition 2:* [1] Let $\epsilon$ and $\lambda$ be positive real numbers strictly less than 1, with $\lambda \geq 2/3$. Then $e(\mathcal{G}_S) = o\left(V(n,d-1)^{2-\epsilon}\right)$, provided $\delta = (d-1)/n$ satisfies the following two conditions:

$$\begin{aligned}(1-\epsilon)H_2(\delta) &> H_2(\lambda\delta)\\ (1-\epsilon)H_2(\delta) &> \lambda\delta + (1-\lambda\delta)H_2\left(\frac{\delta-\lambda\delta/2}{1-\lambda\delta}\right),\end{aligned}$$

where $H_2$ denotes the binary entropy function.

They then show that for $\epsilon = 0.000001$ and $\lambda = 0.999$, the conditions of Proposition 2 are satisfied for any value of $\delta \leq 0.4994$. This proves that the number of edges in the neighborhood of any vertex grows asymptotically much slower than $V(n, d-1)^2$, which is the number of edges in the complete graph on $V(\mathcal{G}_S)$. Using this result in conjunction with Theorem 3 gives the asymptotic lower bound for $A_2(n, d)$ of Theorem 2.

## III. Improving the GV Bound for Linear Codes

The method of Jiang and Vardy lower bounds the size of nonlinear structures, namely independent sets in the Gilbert graph. A natural question is whether their improved bound can be shown to be met by families of linear codes. Gaborit and Zémor [2] show that random double circulant codes achieve this bound for an infinite sequence of block lengths.

Gaborit and Zémor start by restating the GV bound for linear codes within the specific setting of codes of rate $1/2$.

*Theorem 4:* [2] For every positive integer $n$ there exists a linear code of parameters $[2n, n, d]$ satisfying

$$|B_{2n}(d)| \geq 2^n,$$

where $B_{2n}(d)$ denotes the set of nonzero vectors of length $2n$ and weight at most $d$.

The simple probabilistic proof of this statement involves choosing a $n \times 2n$ parity check matrix uniformly at random. Let the random variable $X(w)$ denote the number of codewords of the resulting code $C_{rand}$ of weight at most $w$, for any positive real $w$. It is possible to compute the expected value of $X(w)$, and to bound the probability of the event $X(w) > 0$ by this expectation, since the random variable $X(w)$ is integer-valued. $X(w)$ is given by

$$X(w) = \sum_{x \in B_{2n}(w)} X_x,$$

where $X_x$ is a random variable equal to 1 if $x \in C_{rand}$ and 0 otherwise. With some computations, it can be shown that

$$\Pr[X(w) > 0] \leq E[X(w)] = |B_{2n}(w)| \frac{1}{2^n}.$$

Thus for any $n$ and $w$ satisfying $|B_{2n}(w)| < 2^n$, the probability that a randomly chosen linear code of length $2n$ and dimension at least $n$ has a codeword of weight at most $w$ is strictly less than 1. Hence there exists such a code with minimum distance strictly greater than $w$, and the theorem follows.

The idea of Gaborit and Zémor is, instead of randomly creating any $n \times 2n$ check matrix, to randomly construct the check matrix of a double circulant code, and use the properties of these codes to get a better bound on $\Pr[X(w) > 0]$.

### A. Random Double Circulant Codes Satisfy the Improved GV Bound

Binary double circulant codes are linear codes with rate $1/2$ that are invariant under simultaneous cyclic shifts of the two halves of their coordinate set. Formally, a double circulant code has an $n \times 2n$ parity check matrix of the form $H = [I_n | A]$, where $I_n$ is the $n \times n$ identity matrix and

$$A = \begin{bmatrix} a_0 & a_{n-1} & \cdots & a_1 \\ a_1 & a_0 & \cdots & a_2 \\ \vdots & & & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{bmatrix}.$$

It is not hard to see that such a code is invariant under the group action of $\mathbb{Z}/n\mathbb{Z}$ on $\{0,1\}^{2n}$ that, for any $j \in \mathbb{Z}/n\mathbb{Z}$ and $x = (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n})$, maps $(j, x)$ to $j \cdot x = (x_{n-j+1}, \ldots, x_{n-j}, x_{2n-j+1}, \ldots, x_{2n-j})$.

Picking the check matrix uniformly at random amounts to picking the vector $a = (a_0, \ldots, a_{n-1})$ uniformly at random. Note that a vector $x$ belongs to the resulting code $C_{rand}$ if and only if all its cyclic shifts also belong to $C_{rand}$. This is equivalent to saying that

$$X_x = X_{j \cdot x} \text{ for all } j \in \mathbb{Z}/n\mathbb{Z},$$

where $X_x$, as above, is an indicator random variable equal to 1 if $x \in C_{rand}$ and 0 otherwise. Now for any $w$, recall that $B_{2n}(w)$ is the set of nonzero vectors of weight at most $w$, and let $B'_{2n}(w)$ be a set of representatives of the orbits of the elements of $B_{2n}(w)$, i.e., for any $x \in B_{2n}(w)$, exactly one of its cyclic shifts belongs to $B'_{2n}(w)$ :

$$|B'_{2n}(w) \cap \{j \cdot x, j \in \mathbb{Z}/n\mathbb{Z}\}| = 1.$$

Define the random variable $X'(w)$ analogously to $X(w)$, as

$$X'(w) = \sum_{x \in B'_{2n}(w)} X_x.$$

The insightful idea of Gaborit and Zémor is that $X(w)$ is positive if and only if $X'(w)$ is positive, but $X'(w)$ can have a much smaller expected value than $X(w)$. Specifically,

$$\begin{aligned} X'(w) &= \sum_{x \in B'_{2n}(w)} X_x \\ &= \sum_{x \in B_{2n}(w)} \frac{X_x}{l(x)} \\ &= \sum_{d|n} \sum_{\substack{wgt(x) \leq w \\ l(x)=d}} \frac{X_x}{d}, \end{aligned}$$

where the length $l(x)$ of the orbit of $x$ is readily seen to divide $n$. This gives a refined upper bound on the probability that there exist codewords of weight at most $w$ for a specific $w$:

$$\begin{aligned} \Pr[X(w) > 0] &= \Pr[X'(w) > 0] \\ &\leq E[X'(w)] \\ &= \sum_{d|n} \sum_{\substack{wgt(x) \leq w \\ l(x)=d}} \frac{E[X_x]}{d}. \end{aligned}$$

Using this refined upper bound, Gaborit and Zémor start by proving the existence of some codes (but not necessarily an infinite family) that achieve the following improved (with respect to the GV bound) lower bound on the code size.

*Theorem 5:* [2] If $p$ is prime and 2 is primitive modulo $p$, then there exist double circulant codes of parameters $[2p, p, d > w]$ for any positive $w$ such that

$$2|B_{2p}(w)| < p2^p.$$

Since it is not known whether there exists an infinite family of primes $p$ such that 2 is prime modulo $p$, Gaborit and Zémor turn to the more intricate task of proving a similar theorem for an infinite family of prime powers. Their analysis culminates in the following theorem.

*Theorem 6:* There exist positive constants $b \leq 0.23$ and $q$, such that for any prime $p \geq q$ such that 2 is primitive modulo $p$ and $2^{p-1} \neq 1 \mod p^2$, and for *any power* $n = p^m$ of $p$, there exist double circulant codes of parameters $[2n, n, d > w]$ for any $w$ such that

$$B_{2n}(w) \leq bn2^n.$$

A suitable value of $q$ is $q = 14^3$ and the first suitable prime $p$ is $p = 2789$.

## IV. Random Geometric Graphs

Jiang and Vardy [1] delineate many open problems that arise from their work. One of them, answered in [2], is whether the improved lower bound can be met by linear codes. Other interesting questions concern applying similar methods to find out whether similar improved bounds can be met by spherical codes, covering codes, runlength-limited codes, and others.

One other line of investigation is to see whether there are ways to improve Jiang and Vardy's bound itself. It is not clear how much their analysis takes advantage of all the properties of the Gilbert graph, one of the most important being that it is a *geometric* graph with an associated metric, which satisfies, for example, the triangle inequality. Such properties of the Gilbert graph could be implicitly at work in their analysis, or there could be more to prove by exploiting these properties. In the course of our future work, we propose to study more deeply the field of geometric graphs, and understand what are the tools used in this field that could be applied to our problem.

This motivates our choice for McDiarmid's paper [3]. This paper concerns itself with random channel assignment in the plane: it models receivers as points thrown randomly in the plane, with two points being adjacent if they are close, and the problem is to assign different channels to close receivers. The number of channels needed is nothing but the chromatic number of the graph at hand. McDiarmid asymptotically relates the behavior of the chromatic number of such graphs to their clique number. In the course of his analysis, he also studies various related graph invariants, such as the hitting number of the random geometric graph, its maximum degree, and its degeneracy.

We adopt a different strategy for tackling this paper than for [1] and [2]. We are more concerned with the tools and techniques developed and used in this paper than in specific results (although the chromatic number of a graph can be interesting for our purposes, inasmuch as it provides a lower bound for the independence number). We will thus focus on the model for random graphs developed in [3], and discuss its applicability to our problem of lower bounding the maximum size of codes. For completeness, we will also include a result from [3] that will show some of the techniques for handling random geometric graphs in the plane at work.

### A. The Random Geometric Graph Model

We start by describing the graph model used in [3].

*Definition 2:* [4] Given a finite set $V$ of points in $\mathbb{R}^m$, a norm $||\cdot||$ on $\mathbb{R}^m$, and a positive parameter $d$, the graph $G(V, d)$ with vertex set $V$ and with undirected edges connecting all the pairs $\{x, y\}$ of points such that $||y - x|| \leq d$ is called a *geometric* graph or a *proximity* graph.

A *random geometric graph* considers random configurations of the vertex set in the space.

McDiarmid [3] considers geometric graphs in the plane, with the Euclidean distance as the associated norm. Such graphs are usually called *scaled unit disk* graphs. This terminology comes from the following remark: associate with each vertex an open disk of diameter $d$ centered at this vertex, and let $x$ and $y$ be adjacent if the corresponding disks intersect. This specifies the same geometric graph as in Definition 2, for the two-dimensional case. Further, he considers random distributions of the points in the plane, as follows: let $X_1, X_2, \cdots$ be independent random variables, identically distributed in the plane. Let $X^{(n)}$ denote the family consisting of the first $n$ points, and let $d = d(n)$ be a positive parameter that tends to 0 as $n$ goes to infinity. We consider the infinite family of random scaled unit disk graphs $G_n = G(X^{(n)}, d(n))$.

Note that McDiarmid [3] also studies and obtains results for a different graph model, the *frequency-distance* model. We do not concern ourselves with this model here as it is specific to the context of channel assignment problems with frequency-distance constraints, and is less related to our purpose.

### B. Some Results of [3]

We present here the main results of [3] and outline some of the proofs. We start with some graph theory definitions. Let $G = G(V, d)$ and let $\chi(G)$ be the *chromatic number* of the graph $G$, that is, the minimum number of colors required if one color is to be assigned to each vertex such that no two adjacent vertices are assigned the same color. Let $\omega(G)$ be the *clique number* of $G$, i.e., the size of the largest complete

subgraph of $G$. Let $\omega^-(G)$ be the *hitting number* of $G$, that is, the maximum over all open disks of diameter $d$, in the scaled unit disk representation of the graph, of the number of points of $V$ in any disk. Finally, let $\Delta(G)$ be the *maximum degree* of $G$, and let $\delta^*(G)$ be the *degeneracy* of $G$: this is the maximum, over all induced subgraphs $H$ of $G$, of the minimum degree of $H$. Then we have the following inequalities:

$$\omega^-(G) \leq \omega(G) \leq \chi(G) \leq \delta^*(G) + 1 \leq \Delta(G) + 1,$$

where the inequality $\chi(G) \leq \delta^*(G)+1$ follows from standard results in graph theory, and the inequality $\omega^-(G) \leq \omega(G)$ follows from observing that a set of point contained in a disk of diameter $d$ forms a clique. The other inequalities are obvious.

The main achievement of the paper is to determine the behavior of the graph invariants defined above, for two separate cases: the "sparse case", where $d^2n$ grows slower than $\ln n$ (but not too slowly), and the "dense case", where $d^2n$ grows faster than $\ln n$. No results are known for the case where $d^2n$ scales like $\ln n$. The following theorem summarize those results for the sparse case.

*Theorem 7:* [3] (On sparse random scaled unit disk graphs). Let $d = d(n)$ satisfy $d^2n = o(\ln n), d^2n = n^{o(1)}$. Let

$$k = k(n) = \frac{\ln n}{\ln\left(\frac{\ln n}{d^2 n}\right)}.$$

Then $k \to \infty$ as $n \to \infty$, and in probability $\Delta(G_n)/k \to 1$ and $\omega^-(G_n)/k \to 1$, and so $\chi(G_n)/\omega(G_n) \to 1$.

Here the constraints on $d$ mean that for the theorem to hold, $d^2n$ should be of the order of $n^{-\epsilon(n)}$, where $\epsilon(n)$ is a positive function of $n$ and is $o(1)$.

The next theorem handles the dense case. Here $\nu_{max}$ denotes the "maximum density" corresponding to the distribution $\nu$ of points in the plane, i.e.,

$$\nu_{max} = \sup_B \nu(B)/\lambda(B),$$

where $B$ spans all open disks in the plane, $\nu(B) = \Pr[X \in B]$ for any point $X$, and $\lambda(B)$ is the area of $B$.

*Theorem 8:* [3] (On dense random scaled unit disk graphs). Let $d = d(n)$ satisfy $d \to 0$ and $d^2n/\ln n \to \infty$ as $n \to \infty$. Let

$$k = k(n) = \nu_{max}\frac{\pi}{4}d^2n.$$

Then as $n \to \infty$, almost surely $\omega^-(G_n)/k \to 1$, $\omega(G_n)/k \to 1$, $\chi(G_n)/k \to 2\sqrt{3}/\pi$, $\delta^*(G_n)/k \to 2$, and $\Delta(G_n)/k \to 4$.

For illustrative purposes, we sketch the part of the proof of Theorem 8 pertaining to $\chi(G_n)$. For this we will need the following two lemmas.

*Lemma 1:* [3] Let $\sigma > \nu_{max}$. Let $d = d(n)$ be such that $d^2n/\ln n \to \infty$ as $n \to \infty$. Then

$$\chi(G_n) \leq \sigma\frac{\sqrt{3}}{2}d^2n$$

with probability $1 - e^{-\Omega(d^2n)}$.

*Lemma 2:* [3] Let $0 < \sigma < \nu_{max}$. Let $d = d(n) \to 0$ as $n \to \infty$. Then

$$\chi(G_n) \geq \sigma\frac{\sqrt{3}}{2}d^2n$$

with probability $1 - e^{-\Omega(d^2n)}$ as $n \to \infty$.

Clearly, Lemmas 1 and 2 combined prove that for $d = d(n)$ satisfying both $d \to 0$ and $d^2n/\ln n \to \infty$ as $n \to \infty$, $\chi(G_n)$ tends to

$$\nu_{max}\frac{\sqrt{3}}{2}d^2n = \frac{2\sqrt{3}}{\pi}k,$$

where $k$ is defined as in Theorem 8, with probability tending to 1.

The proof of Lemma 1 relies in turn on the following lemma:

*Lemma 3:* [3] Let $\mathcal{T}$ denote the triangular lattice, i.e., the set of all integer linear combinations of the points $(1,0)$ and $(1/2, \sqrt{3}/2)$. Let $V$ be a family of points in the plane, let $d > 0$, and consider the corresponding scaled unit disk graph $G = G(V, d)$. Let $\delta > 0$, assume that the maximum number of points of $V$ in a cell of the scaled triangular lattice $(\delta d)T$ is finite, and denote it by $y$. Then

$$\chi(G) < \left(\frac{1}{\delta} + 3\right)^2 y.$$

In particular, if $y \leq (\sqrt{3}/2)\tau(\delta d)^2 n$ for some $\tau$, then

$$\chi(G) < (1 + 3\delta)^2(\sqrt{3}/2)\tau d^2 n.$$

The proof of Lemma 3 upper bounds the chromatic number of $G(V, d)$ by a function of the chromatic number of the lattice graph $G(\delta dT, d + (2/\sqrt{3})\delta d)$, relating the two by the maximum number $y$ of points of $V$ in any single cell of the triangular lattice $\delta dT$. More specifically, it can be shown that

$$\chi(G) \leq y \cdot \chi\left(G(\delta dT, d + (2/\sqrt{3})\delta d)\right).$$

It then uses a known upper bound on the chromatic number of the triangular lattice graph to derive an upper bound for $\chi(G)$.

By Lemma 3, all that is needed to prove Lemma 1 is to upper bound the probability that the maximum number of points of $G(V, d)$ falling in a given cell of the scaled triangular lattice $sT$ is higher than a certain value. More specifically, let the random variable $Y_n$ denote the maximum number of points in a cell. Then it is sufficient to prove that

$$\Pr[Y_n > \frac{\sqrt{3}}{2}\tau s^2 n] \leq e^{-\Omega(d^2n)} \tag{4}$$

for some $\tau$ such that $\sigma > \tau > \nu_{max}$. This is done by partitioning the plane into at most $2/p + 1$ sets formed from

union of cells, such that each set $S$ has $\nu(S) \leq p$, with $p = p(n) = (\sqrt{3}/2)\nu_{max}s^2$. By using the union bound over these sets combined with a Chernoff-like bound, the upper bound of equation (4) is obtained.

Lemma 2 is proved using similar methods.

## V. Discussion and Thesis Plan

We presented Jiang and Vardy's asymptotic improvement, by a factor of $n$, of the GV bound on the maximum size of a binary code [1]. This improvement relied on graph-theoretical methods that exploited the local sparsity of the Gilbert graph. We also showed Gaborit and Zémor's work [2], which proved, using methods completely unrelated to graph theory, that this improved bound is actually met by an infinite family of double circulant codes. We then turned to the discussion, in section IV, of whether Jiang and Vardy's analysis could be further improved by taking into account the geometric nature of the Gilbert graph. To this purpose, we introduced random geometric graphs and presented McDiarmid's work on random chanel assignment in the plane [3] as a prototype of the kind of tools and techniques used to handle such graphs. Besides presenting some of the results in [3], we described the model it uses of random geometric graphs in the plane. How useful is this model for our problem?

We can identify several obstacles to the applicability of the random geometric graph model to our original problem of bounding the size of independent sets in the Gilbert graph. Working in a lower-dimensional space and with a continuous norm instead of the Hamming distance is a good simplification when first attempting to understand the problem. But a major ingredient used in this model is randomness, namely, the fact that points are randomly distributed in the space. This powerful tool makes the analysis of graph invariants easier to handle, but we are not yet clear on how it can be used for our problem. Another difference is that the parameter $d = d(n)$ is assumed to go to 0 as $n$ grows in the model considered by McDiarmid [3]. This makes sense in the context of random geometric graphs in the plane: points are assumed to be distributed in some finite area of the plane, and as the number of points grows, it is not reasonable to expect to say something meaningful about the graph $G(X^{(n)}, d(n))$ if we keep $d(n)$ large. But in our case, $d$ corresponds to the minimum distance of the codes we consider. The work of Jiang and Vardy assumed that $d$ was a constant fraction of $n$, and we would like to say something meaningful about codes with nonvanishing relative minimum distance. We do not yet know how to circumvent this issue.

In short, we propose to investigate random geometric graphs and see wether some of the tools used in this field can be extended to the problem of lower bounding the size of codes. We may need to work with a variation of the Gilbert graph if we want to be able to take advantage of such tools. As a first step, we would like to consider simpler settings than that of working in an $n$-dimensional space with the Hamming norm. One such simpler (because it uses a continuous norm) setting that will still be meaningful is spherical codes. Jiang and Vardy [1] propose the applicability of their method to spherical codes as an open problem; it seems feasible to start investigating how both the methods from [1] and [3] can be applied to this setting.

## References

[1] 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.

[2] P. Gaborit and G. Zémor, "Asymptotic Improvement of the Gilbert-Varshamov Bound for Linear Codes", *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3865-3872, Sept. 2008.

[3] C. McDiarmid, "Random Channel Assignment in the Plane", *Random Structures and Algorithms*, vol. 22, pp. 187-212, 2003.

[4] M. D. Penrose, *Random Geometric Graphs*. Oxford University Press, 2003.