

The Voronoi Spherical CDF for Lattices and Linear Codes: New Bounds for Quantization and Coding

Or Ordentlich

Abstract—For a lattice/linear code, we define the Voronoi spherical cumulative density function (CDF) as the CDF of the ℓ_2 -norm/Hamming weight of a random vector uniformly distributed over the Voronoi cell. Using the first moment method together with a simple application of Jensen’s inequality, we develop lower bounds on the expected Voronoi spherical CDF of a random lattice/linear code. Our bounds are valid for any finite dimension and are quite close to a ball-based lower bound. They immediately translate to new non-asymptotic upper bounds on the normalized second moment and the error probability of a random lattice over the additive white Gaussian noise channel, as well as new non-asymptotic upper bounds on the Hamming distortion and the error probability of a random linear code over the binary symmetric channel. In particular, we show that for most lattices in $\mathbb{R}^n$ the second moment is greater than that of a Euclidean ball with the same covolume only by a $(1 + O(\frac{1}{n}))$ multiplicative factor. Similarly, for most linear codes in $\mathbb{F}_2^n$ the expected Hamming distortion is greater than that of a corresponding Hamming ball only by an additive universal constant.

I. INTRODUCTION AND MAIN RESULTS

This paper studies two fundamental quantities associated with lattices in $\mathbb{R}^n$, as well as their counterparts for linear codes in $\mathbb{F}_2^n$. In particular, for lattices we study the normalized second moment (NSM) and the resilience to Gaussian iid noise. For linear codes, we study the analogous quantities: the Hamming distortion (expected Hamming distance of a uniform point on $\mathbb{F}_2^n$ to the code), and the resilience to Bernoulli iid noise. Those quantities are instrumental for characterizing the performance of the lattice/linear code as a quantizer, as well as its usefulness for reliable transmission of information over an additive white Gaussian noise (AWGN) channel for the lattice case, and over a binary symmetric channel (BSC) for the linear code case.

We now briefly describe our main results:

- The normalized second moment (NSM) of a unit covolume lattice $L \subset \mathbb{R}^n$ is defined as $G_L = \frac{1}{n} \mathbb{E} \|U_L\|_2^2$, where U_L is uniformly distributed over the Voronoi cell of L (when $\text{covol}(L) \neq 1$, one further normalizes by $(\text{covol}(L))^{2/n}$). The NSM is trivially lower bounded by the second moment of the uniform distribution on a unit-volume Euclidean ball. We show that for a random lattice in $\mathbb{R}^n$ drawn from the natural distribution on the space of lattices (the Haar-Siegel probability distribution μ_n , to be defined in the sequel), the expected NSM exceeds this lower bound only by a factor of $1 + O(\frac{1}{n})$. The exact statement is in Theorem II.5 and its Corollary II.7, that

provide explicit expressions for any n and an extension for the p th moment of a lattice is proved in Theorem D.1. In particular, Theorem II.5 shows the existence of a lattice with NSM close to that of the ball by a factor $1 + O(\frac{1}{n})$ (this is actually true for almost all lattices, Lemma II.6). Prior to this work, the tightest asymptotic upper bound on the NSM of the “best” lattice in $\mathbb{R}^n$ was $1 + O(\frac{\log n}{n})$ larger than that of the ball [1]. This bound relied on upper bounding the covering density of the best lattice. Since the covering density of any lattice in $\mathbb{R}^n$ is known to be $\Omega(n)$ [2], this technique is inherently limited, and cannot yield bounds with factor smaller than $1 + O(\frac{\log n}{n})$ of the ball’s second moment. We note that not only does Theorem II.5 improve the optimal asymptotic scaling of the NSM, but it improves upon the best known upper bounds even for moderate values of n . In particular, for $36 \leq n \leq 48$ it attains tighter upper bounds on the NSM than the best known ones, as reported in [3].

Furthermore, a canonical upper bound on the NSM of the “best” infinite constellation with a given point density was derived by Zador [4]. To date, it was not known whether or not this bound can be attained by lattices. In Theorem II.8 we show that for large n there are lattices attaining Zador’s upper bound (to within a $e^{-\Omega(n)}$ additive term). Furthermore, in Section II-B1 we show that both Zador’s upper bound for non-lattice quantizers and our new upper bound from Theorem II.8 for lattice quantizers approach Conway and Sloane’s conjectured lower bound on the NSM of any quantizer [5] at rate $O(\frac{\log^2 n}{n^2})$. This can be seen as an evidence that for large n lattice quantizers are as good as any other quantizer, as was essentially postulated in Gersho’s conjecture [6].

- The error probability $P_{e,\sigma^2}(L)$ of a lattice L at noise level σ^2 is defined as the probability that a Gaussian iid noise with zero mean and variance σ^2 falls outside of the Voronoi cell of L . In Theorem II.11 we prove a novel upper bound on the expected error probability of a random lattice (drawn from μ_n). This bound is numerically shown to be similar to the best known previous upper bound due to [7], [8], but we were not able to compare the two bounds analytically.
- For a linear code $\mathcal{C} \subset \mathbb{F}_2^n$ of dimension $0 \leq k \leq n$, the Voronoi region $\mathcal{V}_{\mathcal{C}}$ is the set of all points in $\mathbb{F}_2^n$ that are closer under Hamming distance to 0 than to any other codeword in $\mathcal{C}$. See Section III for the precise definition. The Hamming distortion $D_{\mathcal{C}}$ is defined as the expected Hamming weight of a vector uniformly distributed over the Voronoi cell. This is also the expected

Hamming distortion when quantizing a uniform random vector on $\mathbb{F}_2^n$ to its nearest point in $\mathcal{C}$. The Hamming distortion of any such $\mathcal{C}$ is trivially lower bounded by the expected Hamming weight of the uniform distribution on a quasi Hamming ball of size 2^{n-k} (see Lemma III.8). In Theorem III.5 we show that for a random linear code of dimension k , the expected Hamming distortion exceeds this lower bound only by an additive universal constant (independent of n). To the best of our knowledge, such a tight characterization was not known for linear codes prior to this work.

- The error probability $P_e(\mathcal{C}, p)$ of a linear code $\mathcal{C} \subset \mathbb{F}_2^n$ of dimension $0 \leq k \leq n$ at noise level p is defined as the probability that a Bernoulli(p) iid noise falls outside of the Voronoi cell. Equivalently, this is the block error probability of the $[n, k]$ linear code $\mathcal{C}$ over the BSC with crossover probability p . In Theorem III.11 we prove a new upper bound on the expected error probability of a random linear code. Near capacity, this bound is numerically seen to improve upon the best known finite-blocklength error probability upper bounds for the BSC due to Poltyrev [9] and Polyanskiy-Poor-Verdú [10].

A. Technical innovation.

We give a high-level overview of the main ideas used in the proofs for the results on lattices. The same ideas are used for the analysis of linear codes.

The Voronoi cell $\mathcal{V}_L$ of a lattice $L \subset \mathbb{R}^n$ is the set of all points in $\mathbb{R}^n$ that are closer to 0 than to any other lattice point in L . Many of the most important figures of merit of L are defined through its Voronoi cell. For instance, the packing radius is the radius of the largest ball contained in $\mathcal{V}_L$, the covering radius is the maximum norm of a point in $\mathcal{V}_L$, the second moment of the lattice is the expected energy of a random vector uniformly distributed on $\mathcal{V}_L$, and the lattice error probability is the probability that iid Gaussian noise falls outside of $\mathcal{V}_L$. Thus, studying the geometry of $\mathcal{V}_L$ is key to analyzing the above quantities. However, the Voronoi cell is a polytope dictated by an exponential number of lattice points, and therefore characterizing it exactly becomes intractable as n increases.

Our first observation is that many of the important lattice figures of merit, including the four mentioned above, are rotation invariant, and therefore only depend on $\mathcal{V}_L$ through the function

$$g_L(r) = \frac{|r\mathcal{B} \cap \mathcal{V}_L|}{|\mathcal{V}_L|}, \quad r > 0,$$

which we refer to as the Voronoi spherical cumulative density function (CDF) of the lattice. Here, $\mathcal{B}$ is a unit radius Euclidean ball, and $|\cdot|$ denotes the volume of a set in $\mathbb{R}^n$ (for a discrete set $\mathcal{A}$, we abuse notation and use $|\mathcal{A}|$ to denote the number of points in $\mathcal{A}$). Note that if $U_L \sim \text{Uniform}(\mathcal{V}_L)$, then $g_L(r) = \Pr(\|U_L\|_2 \leq r)$ is the CDF of its ℓ_2 -norm, justifying the name Voronoi spherical CDF. Under the criteria mentioned above, a lattice is considered “good” if its Voronoi cell is “close” to a Euclidean ball with the same volume. In terms of the Voronoi spherical CDF, this corresponds to having

large $g_L(r)$ for all $r > 0$. We therefore seek lower bounds on $g_L(r)$, which in turn, translate to upper bounds on the NSM and error probability of the lattice L .

Assume without loss of generality that L has unit covolume, so that $|\mathcal{V}_L| = 1$. Define the projection of $x \in \mathbb{R}^n$ to $\mathcal{V}_L$ as $\pi_L(x) = x - Q_L(x)$, where $Q_L(x)$ maps x to its nearest neighbor in the lattice L . The projection of the ball $r\mathcal{B}$ to $\mathcal{V}_L$ is defined as $\pi_L(r\mathcal{B}) = \{\pi_L(x) : x \in r\mathcal{B}\}$. Since $\|\pi_L(x)\| \leq \|x\|$, we have that $r\mathcal{B} \cap \mathcal{V}_L = \pi_L(r\mathcal{B})$. Thus, computation of $g_L(r) = |r\mathcal{B} \cap \mathcal{V}_L|$ reduces to computation of $|\pi_L(r\mathcal{B})|$.

In [11, Proof of Proposition 3.6], it was observed that

$$\begin{aligned} |\pi_L(r\mathcal{B})| &= \int_{x \in r\mathcal{B}} \frac{1}{|(x+L) \cap r\mathcal{B}|} dx \\ &= \int_{x \in r\mathcal{B}} \frac{1}{1 + |(L \setminus \{0\}) \cap (r\mathcal{B} - x)|} dx. \end{aligned}$$

Evaluation of the expression above for a particular lattice L still seems challenging. However, for a random lattice L , we can use the convexity of $t \mapsto \frac{1}{1+t}$ together with Jensen’s inequality and obtain

$$\mathbb{E}_L[g_L(r)] \geq \int_{x \in r\mathcal{B}} \frac{1}{1 + \mathbb{E}[|(L \setminus \{0\}) \cap (r\mathcal{B} - x)|]} dx.$$

By Siegel’s summation formula (Minkowski-Hlawka Theorem) [12], we have that if L is drawn from the natural probability distribution μ_n on the space of unit covolume lattices in $\mathbb{R}^n$, then

$$\mathbb{E}[|(L \setminus \{0\}) \cap (r\mathcal{B} - x)|] = |r\mathcal{B}|, \quad \forall x \in r\mathcal{B}.$$

Consequently,

$$\mathbb{E}_{\mu_n}[g_L(r)] \geq \frac{|r\mathcal{B}|}{1 + |r\mathcal{B}|}.$$

Note that the “best” (highest) Voronoi spherical CDF we could hope for is $\min\{|r\mathcal{B}|, 1\}$, corresponding a perfect unit-volume ball. Our lower bound on $\mathbb{E}_{\mu_n}[g_L(r)]$ is quite close to this utopian behavior, and consequently, using it for controlling the NSM and error probability of a random lattice yields tight bounds. See Figure 1 for an illustration.

A remarkable feature of our analysis is that it relies solely on the first moment method, completely circumventing the need to deal with the intricate statistical dependencies between k -tuples of points ($k > 2$) of a random lattice.

B. Related work

Our analysis of the NSM of a random lattice, as well as its error probability, involves studying the distribution of the distance between $X \sim \text{Uniform}([-a, a]^n)$ for large $a > 0$, and a lattice $L \subset \mathbb{R}^n$, as characterized by the Voronoi spherical CDF $g_L(r)$. Hamprecht and Agrell [13] have previously considered the complementary function $1 - g_L(r)$ and called it the *radial function*. They have also observed that it completely characterizes the packing and covering radii of a lattice, as well as its second moment. They further evaluated and plotted this function for $\mathbb{Z}^n$, A_2 , A_4^* , D_4 , A_8^* , E_8 , A_{16}^* and Λ_{16} . For non-lattice point configurations $L \subset \mathbb{R}^n$, Torquato and co-authors [14], [15] studied the distribution of the random variable $V = \min_{y \in L} \|X - y\|$. In particular, they defined the

void exclusion probability $E_V(r) = 1 - \Pr(V \leq r)$. When L is a lattice, this specializes to the radial function $1 - g_L(r)$. When the constellation $L \subset \mathbb{R}^n$ is generated via a random process called *ghost random sequential addition (RSA)*, which does not result in a lattice, Torquato used an inclusion-exclusion argument, together with the statistical properties for ghost RSA [16], to derive an upper bound on $\mathbb{E}[E_V(r)]$ as a function of the point density. This bound immediately translates to an upper bound on normalized second moment of ghost RSA processes. We also note that for the lattice case, a random variable related to V was studied in [17], where the distance to the lattice was normalized by the covering radius, such that the normalized value is in $[0, 1]$.

The NSM of a lattice $L \subset \mathbb{R}^n$ is a well-studied object, as it characterizes its performance as a quantizer under mean squared error distortion (when entropy coding is further applied for describing the obtained lattice point in bits). This is true in the limit of high resolution quantization for any continuous source satisfying mild regularity conditions, and if the source is Gaussian iid, this is true for any distortion level [18]. Consequently, characterizing/approximating the optimal NSM G_n at any dimension n is a topic that received considerable attention [19], [20], [21], [22], [5], [23], [1], [24], [25], [3], [26], [27], [28], [29]. It is well known that the NSM is lower bounded by the second moment of a uniform distribution on a unit volume Euclidean ball. Using the trivial fact that the second moment of a lattice is upper bounded by its squared (normalized) covering radius,¹ and the well-known fact that there exist lattices in $\mathbb{R}^n$ whose covering radius is only $1 + O(\frac{\log n}{n})$ greater than the radius of the corresponding effective ball [32], it was deduced in² [1] that G_n approaches the ball lower bound at rate $1 + O(\frac{\log n}{n})$. To the best of the author's knowledge, this was the best known asymptotic upper bound on G_n prior to this work. The bounds presented in this work not only improve the asymptotic convergence rate of [1] from $1 + O(\frac{\log n}{n})$ to $1 + O(\frac{1}{n})$, but are effective already in relatively small dimensions, and improve upon the best known NSM even for $36 \leq n \leq 48$. The optimal normalized second moment G_n is also related to the quantity $b_{2,n}$ defined by Zador [4], which quantifies the ‘‘quantization efficiency’’ [6], [18]. The quantity $b_{2,n}$ essentially measures the smallest mean squared error (MSE) distortion of any quantizer in $\mathbb{R}^n$ with unit point density for a source $X \sim \text{Uniform}([-a, a]^n)$ in the limit $a \rightarrow \infty$. In particular, $G_n \geq b_{2,n}$. Zador have proved an upper bound on $b_{2,n}$ that essentially follows from drawing the quantizer reconstruction points according to a Poisson point process in $\mathbb{R}^n$ with unit intensity [4, Lemma 5] (see also [15] for an analysis of the quantization efficiency for the ghost RSA point process). The resulting quantizer is not a lattice, and to date it was not known if lattices can achieve this upper bound. Our Theorem II.8 shows that for large n there are indeed lattices that achieve Zador's bound (up to an $e^{-\Omega(n)}$ additive term). In fact, a well-known conjecture due to Gershon [6]

postulates that the quantization cells of the optimal quantizer are all congruent to some polytope (as is of course the case for lattice quantizers), and our Theorem II.8 is perhaps another evidence for the validity of this conjecture.

The application of lattices as codebooks for reliable communication over the AWGN channel has a rich history, dating back to Blake [33], de Buda [34], Conway and Sloane [35] and continuing with [36], [37], [38], [7], [39], [40], [41], [42], [43], [44], [45], [8], [46], as well as many other works. See also, e.g., [47], [48], [49], [50] and [18, Chapter 12] for applications of lattices for multi-user problems. In the classic communication setup, a rate- R power-constrained codebook with 2^{nR} vectors is constructed by taking the intersection of $L \subset \mathbb{R}^n$ and a shaping region $S \subset \mathbb{R}^n$ (which is ideally a Euclidean ball, or Euclidean ball-like) chosen such as to enforce the power constraint. In order to single-out the geometry of L , ignoring effects of shaping, Poltyrev [7] studied the tradeoff between the point density of an infinite constellation and its error probability (in a properly defined sense). When the infinite constellation is a lattice, this corresponds to the question: what is the smallest probability, among all lattices with unit covolume, that an iid $\mathcal{N}(0, \sigma^2)$ Gaussian noise leaves the Voronoi cell? Poltyrev derived upper bounds on the expected error probability of a random lattice [7] (see also [39]), and later an equivalent bound was derived in simpler form in [8]. It was shown in [8] that for σ^2 smaller than, but close to, the normalized squared radius of a ball with unit volume, the error probability is greater than that of a ball only by a constant. See [18, Chapter 13], as well as [51], for a comprehensive analysis of the error probability of a random lattice. In Theorem II.11 we prove a different upper bound on the expected error probability of a random lattice. This bound is close to the bound given in [8], but it seems (numerically) that one bound does not dominate the other in general. We also note in passing that for a non-lattice unit density infinite constellation, tighter upper bounds on the error probability are derived in [52].

The Hamming distortion of linear codes in $\mathbb{F}_2^n$ was first studied by Glick [53], who proved that such codes can asymptotically attain Shannon's rate-distortion function for a symmetric binary source under Hamming distortion. In fact, Glick's proof relied on showing that for every $0 \leq r \leq n$ there exists of a linear code $\mathcal{C} \subset \mathbb{F}_2^n$ for which the Voronoi spherical CDF $Q_{\mathcal{C}}(r)$, as defined in Section III, is large. This follows by choosing the generators of the code sequentially, and ensuring that every new generator that is added sufficiently increases the number of points in $\mathbb{F}_2^n$ that are r -covered. This type of argument is also used for showing the existence of linear codes with small covering radius [54]. Our bounding technique, on the other hand, enables to lower bound $\mathbb{E}_{\mathcal{C}}[Q_{\mathcal{C}}(r)]$ *simultaneously* for all $0 \leq r \leq n$, where the expectation is with respect to the natural random linear code ensemble. It does not involve a sequential selection of the generators, and results in a short and simple derivation of an upper bound on the expected Hamming distortion of a linear code, that is greater than the ball lower bound only by an additive constant. To the best of our knowledge, such a

¹The second moment of any lattice is also at least $1/3$ of its squared (normalized) covering radius, and this bound is attained with equality for $L = \mathbb{Z}^n$. This was conjectured by [17] and proved in [30, Lemme 3.2] and in [31].

²In fact, this result is attributed to Poltyrev in [1]

constant gap result was not previously known for *linear codes*. We also note that the problem of designing practical quantizers based on linear codes whose expected Hamming distortion approaches that of the corresponding ball at rate $1 + o(1)$ was studied quite intensively. See e.g. [55], [56], [57], [58], [59].

Bounding the error probability of a code with $M = 2^k$ codewords for transmission over n uses of a binary symmetric channel with crossover probability p (BSC(p)), and in particular when the code is linear, is one of the most classic topics in coding theory, see e.g., [60], [9], [61], [10] for a very partial list of references. While the vast majority of known bounds are based on some variation of the union bound (perhaps, after discarding rare events) see [62, Chapter 1], the new upper bound we derive in Theorem III.11 avoids the union bound, as well as the weight distribution of the code, altogether. Instead, it bounds the error probability directly through the geometry as the Voronoi region, as captured by the Voronoi spherical CDF. As we only analyze the expected error probability of a random code from the natural ensemble, and do not explore expurgation, our bound is most useful for rates close to capacity, where the sphere-packing lower bound is exponentially tight. In this regime, the best known bound prior to this work is that of Poltyrev [9], which is also equivalent to the RCU bound of [10]. Near capacity our new bound is numerically shown to be tighter than those bounds.

C. Paper structure

All results regarding lattices are developed in Section II, whereas all results regarding linear codes are developed in Section III. The two sections are self-contained, though the techniques and ideas used in the two sections are analogous. Thus, a reader interested only in lattices but not in linear codes (or vice versa), may read only Section II (or only Section III).

D. Acknowledgments

The author is grateful to Erik Agrell, Bruce Allen, Uri Erez, Bo'az Klartag, Yury Polyanskiy, Oded Regev and Barak Weiss for many valuable discussions that improved this paper. A special thanks is due to Erik Agrell for his valuable observation that our new upper bound in Theorem II.8 is close to the conjectured lower bound of Conway and Sloane, which led to the analysis in Subsection II-B1. We also thank the anonymous reviewers and associate editor for many helpful suggestions.

II. LATTICES

For a unit covolume lattice $L \subset \mathbb{R}^n$, we define the Voronoi region as

$$\mathcal{V}_L \stackrel{\text{def}}{=} \{x \in \mathbb{R}^n : \|x\|_2 \leq \|x - y\|_2, \forall y \in L \setminus \{0\}\}, \quad (1)$$

where $\|x\|_2 = (\sum_{i=1}^n x_i^2)^{1/2}$ is the ℓ_2 norm, and ties are broken in a systematic manner, such that $\mathcal{V}_L$ is a fundamental cell of L . Let $U_L \sim \text{Uniform}(\mathcal{V}_L)$. The Voronoi spherical cumulative density function (CDF) of L is defined as

$$g_L(r) \stackrel{\text{def}}{=} \Pr(\|U_L\|_2 \leq r), \quad 0 \leq r < \infty. \quad (2)$$

Many important properties of the lattice L are encoded in its Voronoi spherical CDF. Before specifying how $g_L(r)$ encodes these properties, we will need some definitions.

Recall that we denote the volume of a measurable set $\mathcal{A} \subset \mathbb{R}^n$ by $|\mathcal{A}| \stackrel{\text{def}}{=} \text{vol}(\mathcal{A})$. The unit-radius closed Euclidean ball in $\mathbb{R}^n$ is denoted

$$\mathcal{B} \stackrel{\text{def}}{=} \{x \in \mathbb{R}^n : \|x\|_2 \leq 1\}, \quad (3)$$

and its volume is

$$V_n \stackrel{\text{def}}{=} |\mathcal{B}| = \frac{\pi^{n/2}}{\Gamma(1 + \frac{n}{2})}, \quad (4)$$

where $\Gamma(\cdot)$ is the Gamma function. Let

$$r_{\text{eff}} \stackrel{\text{def}}{=} V_n^{-\frac{1}{n}}, \quad (5)$$

be such that $|r_{\text{eff}}\mathcal{B}| = 1$. Note that

$$g_L(r) = \frac{1}{|\mathcal{V}_L|} |r\mathcal{B} \cap \mathcal{V}_L| = \frac{|r\mathcal{B} \cap \mathcal{V}_L|}{V_n r^n} \cdot \left(\frac{r}{r_{\text{eff}}}\right)^n, \quad (6)$$

where the last equality follows since L has unit covolume.

Proposition II.1. *Let $L \subset \mathbb{R}^n$ be a unit covolume lattice in $\mathbb{R}^n$. Then*

1) *The packing radius of L is*

$$r_{\text{pack}}(L) = \sup \left\{ r > 0 : g_L(r) = \left(\frac{r}{r_{\text{eff}}}\right)^n \right\} \quad (7)$$

2) *The covering radius of L is*

$$r_{\text{cov}}(L) = \inf \{ r > 0 : g_L(r) = 1 \} \quad (8)$$

3) *The normalized second moment (NSM) of L is*

$$G_L \stackrel{\text{def}}{=} \frac{\mathbb{E}\|U_L\|_2^2}{n} = \frac{1}{n} \int_0^\infty 1 - g_L(\sqrt{r}) dr. \quad (9)$$

4) *Let $Z \sim \mathcal{N}(0, I_n)$, The σ^2 -Gaussian error probability of L is*

$$P_{e,\sigma^2}(L) \stackrel{\text{def}}{=} \Pr(\sigma Z \notin \mathcal{V}_L) = \mathbb{E} \left[1 - \frac{g_L(\sqrt{\sigma^2 W})}{\left(\frac{\sigma^2 W}{r_{\text{eff}}^2}\right)^{\frac{n}{2}}} \right], \quad (10)$$

where $W \sim \chi_{n+2}^2$ is a chi-squared random variable with $n + 2$ degrees of freedom.

The first two items in the proposition above are trivial, whereas the third item has appeared in different form in [15, eq. 75] (see also [63, Section III]) for analyzing performance of non-lattice infinite constellations, and re-deriving Zador's formula. For completeness, we bring the proof of Proposition II.1 in Appendix A. The fourth item is a consequence of the following more general proposition, whose proof is also brought in Appendix A.

Proposition II.2. *Let $Z \sim \mathcal{N}(0, I_n)$, let $\mathcal{K} \subset \mathbb{R}^n$ be a measurable subset of $\mathbb{R}^n$, and define*

$$\mu_{\sigma^2}(\mathcal{K}) \stackrel{\text{def}}{=} \Pr(\sigma Z \in \mathcal{K}). \quad (11)$$

For $U_{\mathcal{K}} \sim \text{Uniform}(\mathcal{K})$, define

$$g_{\mathcal{K}}(r) = \Pr(\|U_{\mathcal{K}}\|_2 \leq r) = \frac{|\mathcal{K} \cap r\mathcal{B}|}{|\mathcal{K}|}. \quad (12)$$

Then

$$\mu_{\sigma^2}(\mathcal{K}) = \mathbb{E} \left[\frac{g_{\mathcal{K}}(\sqrt{\sigma^2 W})}{\left(\frac{\sigma^2 W}{r_{\text{eff}}(\mathcal{K})^2}\right)^{\frac{n}{2}}} \right], \quad (13)$$

where $W \sim \chi_{n+2}^2$ is a chi-squared random variable with $n+2$ degrees of freedom, and $r_{\text{eff}}(\mathcal{K})$ is such that $|r_{\text{eff}}(\mathcal{K}) \cdot \mathcal{B}| = |\mathcal{K}|$.

A. Estimates for the expected Voronoi spherical CDF

We say that a CDF $F(r)$ majorizes a CDF $G(r)$, and denote $G \preceq F$, if $G(r) \leq F(r)$ for all $r > 0$. All four lattice properties above are “improved” if the Voronoi spherical CDF g_L is replaced by a majorizing CDF. In particular, from (6) it is clear that for any unit covolume lattice $g_L \preceq g_{\mathcal{B}}$ where

$$g_{\mathcal{B}}(r) = \min \left\{ \left(\frac{r}{r_{\text{eff}}} \right)^n, 1 \right\} \quad (14)$$

is the CDF function for the norm of a random variable uniformly distributed over the Euclidean ball of radius r_{eff} (such that its volume is the same as that of $\mathcal{V}_L$). Thus, the Euclidean ball provides “in-existence” bounds for the 4 quantities above. Our goal in this paper is to develop new “existence” bounds for G_L and P_{e,σ^2} . To that end, we find a CDF $\underline{g}(r)$ for which

$$\mathbb{E}[g_L] \succeq \underline{g}, \quad (15)$$

where the expectation is with respect to some probability measure on $\mathcal{L}_n$, the space of lattices in $\mathbb{R}^n$ with covolume 1. If $g_{\mathcal{B}}(r) - \underline{g}(r)$ is small for all $r > 0$, we will get useful bounds for the NSM and the Gaussian error probability of a “typical” lattice.

Let $\mathbb{T}_L = \mathbb{R}^n/L$ be the quotient torus, and let $\pi_L : \mathbb{R}^n \rightarrow \mathbb{T}_L$ be the quotient map. Note that $\mathcal{V}_L$ is isomorphic to $\mathbb{T}_L$. Thus, one can think of the quotient map as $\pi_L(x) = x - Q_L(x)$, where $Q_L : \mathbb{R}^n \rightarrow L$ maps each point in $\mathbb{R}^n$ to $y \in L$, such that $x \in y + \mathcal{V}_L$. Let $m_L : \mathbb{T}_L \rightarrow [0, 1]$ denote the Haar probability distribution on $\mathbb{T}_L$ (equivalently, one can think of m_L as the uniform distribution on $\mathcal{V}_L$). Namely, for any $\mathcal{A} \subset \mathbb{T}_L$ we have $m_L(\mathcal{A}) = |\mathcal{A}|$. Observe that

$$g_L(r) = \Pr(\|U_L\|_2 \leq r) = |r\mathcal{B} \cap \mathcal{V}_L| = m_L(\pi_L(r\mathcal{B})), \quad (16)$$

where the last equality holds since, when we identify $\mathcal{V}_L$ with $\mathbb{T}_L$, it holds that $\|\pi_L(x)\|_2 \leq \|x\|_2$ for any $x \in \mathbb{R}^n$. In particular, for all $x \in r\mathcal{B}$ we have that $\pi_L(x) \in r\mathcal{B}$. Thus, $\pi_L(r\mathcal{B}) \subset (r\mathcal{B} \cap \mathcal{V}_L)$. On the other hand, for any point $x \in \mathcal{V}_L$ we have that $\pi_L(x) = x$, and consequently $\pi_L(r\mathcal{B}) \supset \pi_L(r\mathcal{B} \cap \mathcal{V}_L) = (r\mathcal{B} \cap \mathcal{V}_L)$. Thus, $\pi_L(r\mathcal{B}) = (r\mathcal{B} \cap \mathcal{V}_L)$. The measure $m_L(\pi_L(\mathcal{K}))$ of the projection of a compact set $\mathcal{K} \subset \mathbb{R}^n$ to the torus has been extensively studied in works ranging from the classic papers of Rogers [64] and Schmidt [65] in the middle of the previous century up to the recent progress in [66], [11]. Using these works, we now

develop two lower bounds on $\mathbb{E}[g_L(r)]$ under two different distributions on L , as we elaborate below.

The collection $\mathcal{L}_n$ of lattices of covolume one in $\mathbb{R}^n$ can be identified with the quotient $\text{SL}_n(\mathbb{R})/\text{SL}_n(\mathbb{Z})$, via the map

$$g \text{SL}_n(\mathbb{Z}) \mapsto g\mathbb{Z}^n \quad (g \in \text{SL}_n(\mathbb{R})). \quad (17)$$

This identification endows $\mathcal{L}_n$ with a natural probability measure; namely, there is a unique $\text{SL}_n(\mathbb{R})$ -invariant Borel probability measure on $\mathcal{L}_n$. Following [66], we will refer to this measure as the *Haar-Siegel measure* and denote it by μ_n . Due to its $\text{SL}_n(\mathbb{R})$ -invariance, the measure μ_n is referred to as the natural measure on the space of lattices in the literature.

Theorem II.3. For $L \sim \mu_n$ we have

$$\mathbb{E}[g_L(r)] \geq g_{\text{Jensen}}(r) \stackrel{\text{def}}{=} \frac{\left(\frac{r}{r_{\text{eff}}}\right)^n}{1 + \left(\frac{r}{r_{\text{eff}}}\right)^n}, \quad \forall r > 0. \quad (18)$$

Using the characterization (16), the proof of Theorem II.3 is an immediate consequence of the derivation in [11, Proof of Proposition 3.6]. This derivation relies only on the first moment method (Siegel’s summation formula/the Minkowski-Hlawka-Siegel Theorem) and an application of Jensen’s inequality. For completeness, we repeat the derivation from [11, Proof of Proposition 3.6] below.

Proof of Theorem II.3. Observe that for any compact set $\mathcal{K} \subset \mathbb{R}^n$ it holds that

$$m_L(\pi_L(\mathcal{K})) = \int_{x \in \mathcal{K}} \frac{1}{|(x+L) \cap \mathcal{K}|} dx \quad (19)$$

$$= \int_{x \in \mathcal{K}} \frac{1}{1 + |(L \setminus \{0\}) \cap (\mathcal{K} - x)|} dx. \quad (20)$$

The function $t \mapsto \frac{1}{1+t}$ is convex in the regime $t > 0$, and we can therefore write

$$\begin{aligned} \mathbb{E}[m_L(\pi_L(\mathcal{K}))] &= \mathbb{E} \left[\int_{x \in \mathcal{K}} \frac{1}{1 + |(L \setminus \{0\}) \cap (\mathcal{K} - x)|} dx \right] \\ &= \int_{x \in \mathcal{K}} \mathbb{E} \left[\frac{1}{1 + |(L \setminus \{0\}) \cap (\mathcal{K} - x)|} \right] dx \end{aligned} \quad (21)$$

$$\geq \int_{x \in \mathcal{K}} \frac{1}{1 + \mathbb{E}[|(L \setminus \{0\}) \cap (\mathcal{K} - x)|]} dx \quad (22)$$

$$= \int_{x \in \mathcal{K}} \frac{1}{1 + |\mathcal{K}|} dx \quad (23)$$

$$= \frac{|\mathcal{K}|}{1 + |\mathcal{K}|}, \quad (24)$$

where (21) follows from Fubini’s Theorem, (22) from Jensen’s inequality and (23) from Siegel’s summation formula. Taking $\mathcal{K} = r\mathcal{B}$ and applying this in conjunction with (16) we obtain

$$\mathbb{E}[g_L(r)] = \mathbb{E}[m_L(\pi_L(r\mathcal{B}))] \geq \frac{|r\mathcal{B}|}{1 + |r\mathcal{B}|} = \frac{\left(\frac{r}{r_{\text{eff}}}\right)^n}{1 + \left(\frac{r}{r_{\text{eff}}}\right)^n}, \quad (25)$$

as claimed. $\square$

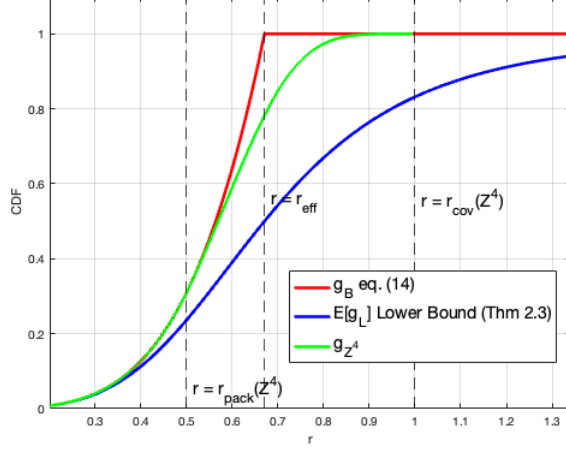
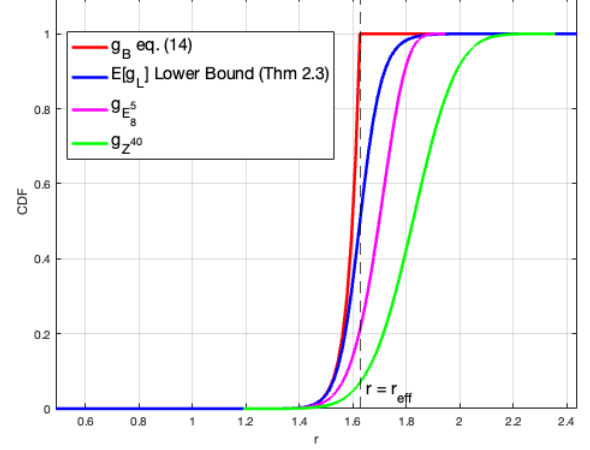
(a) $n = 4$ (b) $n = 40$

Figure 1: Various bounds and exact expressions for the the Voronoi Spherical CDF. For dimension $n = 4$ we plot $g_B(r)$ from (14), the lower bound on $\mathbb{E}_{\mu_n}[g_L(r)]$ from (18), as well as the exact Voronoi Spherical CDF for $L = \mathbb{Z}^4$. We also indicate the points $r_{\text{pack}}(\mathbb{Z}^4)$ where $g_{\mathbb{Z}^4}(r)$ and $g_B(r)$ diverge, $r_{\text{cov}}(\mathbb{Z}^4)$ where $g_{\mathbb{Z}^4}(r) = 1$ for the first time, and r_{eff} which is common to all unit covolume lattices, and this is where $g_B(r) = 1$ for the first time. For dimension $n = 40$. We plot $g_B(r)$ from (14), the lower bound on $\mathbb{E}_{\mu_n}[g_L(r)]$ from (18), as well as the exact Voronoi Spherical CDF for $L = E_8^{\otimes 5}$ (5 copies of E_8) and $L = \mathbb{Z}^{40}$. It is seen that our bound from (18) is not very effective for $n = 4$, but is already quite effective for $n = 40$.

Figure 1 illustrates our bound from Theorem II.5 for $n = 40$, along with $g_B(r)$ for the same dimension, which upper bounds $g_L(r)$ for any lattice $L \subset \mathbb{R}^n$. We also plot $g_L(r)$ for two particular lattices in $\mathbb{R}^{40}$: the integer lattice $\mathbb{Z}^n$ and $E_8^{\otimes 5} \subset \mathbb{R}^{40}$ which consists of 5 copies of the lattice E_8 .

While $g_{\text{Jensen}}(r)$ is quite close to $g_B(r)$ for $r < r_{\text{eff}}$, it is strictly smaller than 1 for all $r > r_{\text{eff}}$. This does not stem from a weakness of our bounding technique. In fact, it is a consequence of the known fact that for $L \sim \mu_n$, the probability that L avoids a set $\mathcal{K} \subset \mathbb{R}^n$ of large volume $|\mathcal{K}| \gg 1$, decays only as $1/|\mathcal{K}|$ [67]. On the other hand, recent work [66] showed that the covering radius of a random lattice $L \sim \mu_n$ is $(1 + O(\frac{\log n}{n})) r_{\text{eff}}$ with probability $1 - e^{-\Omega(n)}$. In light of this, we consider a distribution $\tilde{\mu}_n$ on the space of lattices $\mathcal{L}_n$, obtained by conditioning μ_n on the event that $r_{\text{cov}}(L)$ is small.

In particular, let

$$\eta = \eta_n \stackrel{\text{def}}{=} \frac{n}{8} \log \left(\frac{4}{3} \right), \quad (26)$$

and define the event

$$\mathcal{E}_\eta = \left\{ L \in \mathcal{L}_n : \left(\frac{r_{\text{cov}}(L)}{r_{\text{eff}}} \right)^n \leq 4n^2\eta \right\}. \quad (27)$$

We define the distribution $\tilde{\mu}_n$ on $\mathcal{L}_n$ as

$$\tilde{\mu}_n \stackrel{\text{def}}{=} \mu_n|_{\mathcal{E}_\eta}. \quad (28)$$

Relying on classic results by Rogers [64] and Schmidt [65] and the more recent result [66] on the covering density of a random lattice, we prove the following in Appendix B.

Theorem II.4. Assume $n \geq 13$, and define η and $\tilde{\mu}_n$ as in (26) and (28), respectively. For $L \sim \tilde{\mu}_n$ we have $\mathbb{E}[g_L(r)] \geq \underline{g}_{\text{covering}}(r)$, $\forall r > 0$, where

$$\begin{aligned} \underline{g}_{\text{covering}}(r) &= \begin{cases} 1 - e^{-\left(\frac{r}{r_{\text{eff}}}\right)^n} - 23 \cdot e^{-\frac{\eta}{2}} & \left(\frac{r}{r_{\text{eff}}}\right)^n < \frac{\eta}{2} \\ 1 - 24 \cdot e^{-\frac{\eta}{2}} & \frac{\eta}{2} \leq \left(\frac{r}{r_{\text{eff}}}\right)^n < 4n^2\eta \\ 1 & \left(\frac{r}{r_{\text{eff}}}\right)^n \geq 4n^2\eta \end{cases} \\ &\geq 1 - \left(e^{-\left(\frac{r}{r_{\text{eff}}}\right)^n} + 24e^{-\frac{\eta}{2}} \right) \mathbf{1} \left\{ \left(\frac{r}{r_{\text{eff}}}\right)^n < 4n^2\eta \right\} \end{aligned}$$

We note that Theorem II.4 above is the only result in this paper that requires further tools beyond the first moment method.

B. Bounds on the NSM

We derive two upper bounds on $\mathbb{E}[G_L]$: one for $L \sim \mu_n$ and one for $L \sim \tilde{\mu}_n$.

Theorem II.5. Let n be an integer and $L \sim \mu_n$. We have that

$$\mathbb{E}[G_L] \leq \frac{1}{nV_n^{\frac{2}{n}}} \cdot \frac{1}{\text{sinc}(2/n)}, \quad (29)$$

where

$$\text{sinc}(t) \stackrel{\text{def}}{=} \frac{\sin(\pi t)}{\pi t}. \quad (30)$$

Note that for $36 \leq n \leq 48$ this upper bound is smaller than the best known NSM as reported in [3, Table 1].

Proof. Using Proposition II.1 part 3 (and Tonelli's Theorem)

$$n\mathbb{E}[G_L] = \int_0^\infty \mathbb{E}[1 - g_L(\sqrt{r})]dr = \int_0^\infty 1 - \mathbb{E}[g_L(\sqrt{r})]dr. \quad (31)$$

Applying Theorem II.3, we therefore have

$$n\mathbb{E}[G_L] \leq \int_0^\infty \frac{1}{1 + \left(\frac{r}{r_{\text{eff}}^2}\right)^{\frac{n}{2}}} dr \quad (32)$$

$$= r_{\text{eff}}^2 \int_0^\infty \frac{1}{1 + t^{\frac{n}{2}}} dt. \quad (33)$$

Finally, recalling that [68, Section 3.241] for any $\nu > 0$,

$$\int_0^\infty \frac{1}{1 + t^\nu} dt = \frac{\pi/\nu}{\sin(\pi/\nu)} = \frac{1}{\text{sinc}(1/\nu)}, \quad (34)$$

and that $r_{\text{eff}}^2 = \frac{1}{V_n^{\frac{2}{n}}}$, we obtain that

$$\mathbb{E}[G_L] \leq \frac{1}{nV_n^{\frac{2}{n}}} \cdot \frac{1}{\text{sinc}(2/n)} \quad (35)$$

and the claimed result follows. $\square$

It is well-known [23] that among all bodies in $\mathbb{R}^n$ of unit volume, the second moment is minimized by $r_{\text{eff}}\mathcal{B}$, and

$$G_{r_{\text{eff}}\mathcal{B}} \stackrel{\text{def}}{=} \frac{\mathbb{E}\|U_{r_{\text{eff}}\mathcal{B}}\|_2^2}{n} = \frac{n}{n+2} \cdot \frac{1}{nV_n^{2/n}} \stackrel{\text{def}}{=} G_n^*, \quad (36)$$

where $U_{r_{\text{eff}}\mathcal{B}} \sim \text{Uniform}(r_{\text{eff}}\mathcal{B})$. A simple application of Markov's inequality shows that for large n , almost all lattices have near-optimal NSM.

Lemma II.6. Assume $n \geq 8$ and let $L \sim \mu_n$. Then for any $\kappa > 0$

$$\Pr(G_L \geq (1 + \kappa)G_n^*) \leq \frac{4}{\kappa n}. \quad (37)$$

Proof. Define the random variable $Y = Y_L = \frac{G_L}{G_n^*} - 1$, which is non-negative with probability 1. By Markov's inequality, we have

$$\Pr(G_L \geq (1 + \kappa)G_n^*) = \Pr(Y \geq \kappa) \leq \frac{\mathbb{E}[Y]}{\kappa}. \quad (38)$$

Using $\sin(x) \geq x(1 - \frac{x^2}{6})$ for $x > 0$, we have that for any $0 < x \leq \frac{1}{\pi}$ it holds that

$$\frac{1}{\text{sinc}(x)} \leq \frac{\pi x}{\pi x(1 - \frac{(\pi x)^2}{6})} \leq 1 + \frac{1}{5}(\pi x)^2 < 1 + 2x^2. \quad (39)$$

Applying Theorem II.5 we obtain (for $n \geq 8$, such that $\frac{2}{n} \leq \frac{1}{\pi}$)

$$\begin{aligned} \mathbb{E}[Y] &\leq \frac{n+2}{n} \frac{1}{\text{sinc}(2/n)} - 1 \leq \left(1 + \frac{2}{n}\right) \left(1 + \frac{8}{n^2}\right) - 1 \\ &= \frac{2}{n} + \frac{8}{n^2} + \frac{16}{n^3} < \frac{4}{n}, \end{aligned} \quad (40)$$

which yields the claimed result. $\square$

Setting $\kappa = c/n$ in Lemma II.6, we obtain the following straightforward corollary that shows, e.g., that there are lattices $L \subset \mathbb{R}^n$ with $G_L < (1 + \frac{5}{n})G_n^*$.

Corollary II.7. Assume $n \geq 8$ and let $L \sim \mu_n$. Then for any $c > 0$

$$\Pr\left(G_L \geq \left(1 + \frac{c}{n}\right)G_n^*\right) \leq \frac{4}{c}. \quad (41)$$

The normalized second moment characterizes the expected squared ℓ_2 distance between X drawn uniformly over a very large ball, and a unit covolume lattice L . Similarly, we can define the normalized p th moment $G_L^{(p)}$ of a unit covolume lattice L as the expected p th power of the ℓ_p distance between X and L . In Appendix D we provide the precise definition and extend Theorem II.5 for upper bound $\mathbb{E}[G_L^{(p)}]$ for $L \sim \mu_n$.

Next, we derive an upper bound for the expected NSM $\mathbb{E}[G_L]$ for $L \sim \tilde{\mu}_n$.

Theorem II.8. Let $n \geq 13$ be an integer, and $L \sim \tilde{\mu}_n$. We have that

$$\mathbb{E}[G_L] \leq \frac{1}{nV_n^{\frac{2}{n}}} \left(\Gamma\left(1 + \frac{2}{n}\right) + 60ne^{-\frac{\eta}{2}} \right) \quad (42)$$

where $\eta = \frac{n}{8} \log\left(\frac{4}{3}\right)$ is defined in (26) and $\Gamma(\cdot)$ is the Gamma function.

Note that as n grows, our upper bound approaches from above the well-known Zador [4, Lemma 5] upper bound

$$\overline{G}_n^{\text{Zador}} \stackrel{\text{def}}{=} \frac{\Gamma\left(1 + \frac{2}{n}\right)}{nV_n^{\frac{2}{n}}} \quad (43)$$

on the smallest MSE a unit-density quantizer can achieve. In particular, Zador's upper bound shows that there exists an infinite constellation $\mathcal{C} \subseteq \mathbb{R}^n$ with unit density, whose second moment is at most $\overline{G}_n^{\text{Zador}}$. To the best of the author's knowledge, until this work it was not known whether or not there exist lattices in high dimensions that attain this bound. Theorem II.8 shows that this bound is indeed attained by lattices, up to a multiplicative factor of $1 + c_1 e^{-c_2 n}$ for universal constants $c_1, c_2 > 0$.

Proof. Let $r_1 = r_{\text{eff}}^2 \cdot \left(\frac{\eta}{2}\right)^{\frac{2}{n}}$ and $r_2 = r_{\text{eff}}^2 \cdot (4n^2\eta)^{\frac{2}{n}}$. Using Proposition II.1 part 3, together with Theorem II.4, we have (using Tonelli's Theorem)

$$n\mathbb{E}[G_L] = \int_0^\infty \mathbb{E}[1 - g_L(\sqrt{r})]dr \quad (44)$$

$$\leq \int_0^{r_1} e^{-\left(\frac{r}{r_{\text{eff}}^2}\right)^{\frac{n}{2}}} + 23 \cdot e^{-\eta/2} dr + \int_{r_1}^{r_2} 24 \cdot e^{-\frac{\eta}{2}} dr \quad (45)$$

$$\leq 24r_2 e^{-\frac{\eta}{2}} + \int_0^{r_1} e^{-\left(\frac{r}{r_{\text{eff}}^2}\right)^{\frac{n}{2}}} dr. \quad (46)$$

Set $c = r_{\text{eff}}^{-n}$, and make the change of variables $r = \left(\frac{u}{c}\right)^{\frac{2}{n}}$, $dr = \frac{2}{nc^{2/n}} u^{\frac{2}{n}-1} du$. The integral above is

$$\int_0^{r_1} e^{-\left(\frac{r}{r_{\text{eff}}}\right)^{\frac{n}{2}}} dr = \int_0^{r_1} e^{-cr^{\frac{n}{2}}} dr \quad (47)$$

$$= \frac{2}{nc^{2/n}} \int_0^{cr_1^{n/2}} u^{\frac{2}{n}-1} e^{-u} du \quad (48)$$

$$\leq r_{\text{eff}}^2 \cdot \frac{2}{n} \cdot \int_0^\infty u^{\frac{2}{n}-1} e^{-u} du \quad (49)$$

$$= r_{\text{eff}}^2 \cdot \frac{2}{n} \cdot \Gamma\left(\frac{2}{n}\right). \quad (50)$$

Recalling that $r_{\text{eff}}^2 = V_n^{-\frac{2}{n}}$ and that $\Gamma(1 + \frac{2}{n}) = \frac{2}{n}\Gamma(\frac{2}{n})$, we obtained

$$\int_0^{r_1} e^{-\left(\frac{r}{r_{\text{eff}}}\right)^{\frac{n}{2}}} dr = V_n^{-\frac{2}{n}} \Gamma\left(1 + \frac{2}{n}\right). \quad (51)$$

Furthermore, since $(4n^2\eta)^{2/n} < 5/2$ for all $n \geq 13$, we have

$$24r_2 \leq 24(4n^2\eta)^{\frac{2}{n}} r_{\text{eff}}^2 \leq 60r_{\text{eff}}^2 = 60V_n^{-\frac{2}{n}}, \quad \forall n \geq 13. \quad (52)$$

This establishes our claimed result. $\square$

1) *Gap to Conway and Sloane's Conjectured Bound:* In [5], Conway and Sloane conjectured that the normalized second moment of any (not necessarily lattice) quantizer in $\mathbb{R}^n$ is lower bounded by

$$\underline{G}_n^{\text{CS}} \stackrel{\text{def}}{=} \frac{n+3-2H_{n+2}}{4n(n+1)} (n+1)^{1/n} (n!)^{4/n} f_n(n)^{2/n}, \quad (53)$$

where $H_m = \sum_{i=1}^m \frac{1}{i}$ is a harmonic sum, and $f_n(\cdot)$ is the Schlöfli function. While the definition of $f_n(\cdot)$ [5] is recursive, and does not admit a closed form expression, in [69] (see also [70], [71]) Rogers and H. E. Daniels derived the approximation

$$f_n(n) = \frac{\sqrt{n+1}}{\sqrt{2}e n!} \left(\frac{2e}{\pi n}\right)^{n/2} \left(1 + \frac{31}{12n} + O(n^{-2})\right). \quad (54)$$

Furthermore, in [71] an efficient algorithm with high numerical precision was developed for computing $f_n(x)$ in the range $x \in [n-1, n+1]$. Using this algorithm, Erik Agrell [72] has observed numerically that Zador's upper bound (43) on the NSM is remarkably close to $\underline{G}_n^{\text{CS}}$ for large n . See Figure 2, reproduced from [72] (see also [63, Figure 1] for a similar figure). Since our upper bound from Theorem II.8 is only $(1 + c_1 e^{-c_2 n})$ greater than Zador's upper bound, for universal $c_1, c_2 > 0$, the same holds also for this bound. The next lemma, proved in Appendix C, validates the numerical findings of [72].

Lemma II.9.

$$\frac{\overline{G}_n^{\text{Zador}}}{\underline{G}_n^{\text{CS}}} = 1 + O\left(\frac{\log^2(n)}{n^2}\right). \quad (55)$$

To appreciate this result, note that

$$\frac{\overline{G}_n^{\text{Zador}}}{G_n^*} = \frac{\overline{G}_n^{\text{Zador}}}{\frac{1}{(n+2)V_n^{2/n}}} = 1 + \Omega\left(\frac{1}{n}\right). \quad (56)$$

Thus, Conway and Sloane's conjectured lower bound is significantly tighter than the ball-bound G_n^* (often referred to as Zador's lower bound). As an immediate corollary of Lemma II.9 and Theorem II.8 we obtain the following.

Corollary II.10. *For $L \sim \tilde{\mu}_n$ we have*

$$\frac{\mathbb{E}[G_L]}{\underline{G}_n^{\text{CS}}} = 1 + O\left(\frac{\log^2(n)}{n^2}\right). \quad (57)$$

This shows that if Conway and Sloane's conjectured lower bound is correct, then there exist lattices that achieve the *optimal NSM among all quantizers* to within a $1 + O\left(\frac{\log^2(n)}{n^2}\right)$ factor (in fact this is true for almost all lattices). This constitutes a significant step towards establishing Gersho's conjecture, that essentially postulates that for dimension n sufficiently large the best lattice quantizer is at least as good as any other quantizer in the same dimension.

C. Error probability of a random lattice

The error probability of a unit covolume lattice $L \subset \mathbb{R}^n$ is defined as

$$P_e(L, \sigma^2) = \Pr(\sigma Z \notin \mathcal{V}_L) = 1 - \Pr(\sigma Z \in \mathcal{V}_L) \quad (58)$$

$$= 1 - \mu_{\sigma^2}(\mathcal{V}_L). \quad (59)$$

Clearly,

$$\mu_{\sigma^2}(\mathcal{V}_L) \leq \mu_{\sigma^2}(r_{\text{eff}}\mathcal{B}), \quad (60)$$

and similarly

$$P_e(L, \sigma^2) \geq P^{\text{SP}}(\sigma^2) \stackrel{\text{def}}{=} 1 - \mu_{\sigma^2}(r_{\text{eff}}\mathcal{B}). \quad (61)$$

We prove the following.

Theorem II.11. *Let n be an integer, let $W \sim \chi_{n+2}^2$ be a chi-squared random variable with $n+2$ degrees of freedom, and let*

$$X_W \stackrel{\text{def}}{=} \left(\frac{\sqrt{\sigma^2 W}}{r_{\text{eff}}}\right)^n. \quad (62)$$

Then, for any $\sigma^2 > 0$ we have that

$$\mathbb{E}_{\mu_n}[P_e(L, \sigma^2)] \leq P^{\text{SP}}(\sigma^2) + \mathbb{E}\left[\frac{\min\{X_W, X_W^{-1}\}}{1 + X_W}\right]. \quad (63)$$

Proof. By Proposition II.2, for any unit-covolume $L \subset \mathbb{R}^n$ we have that

$$\Delta(L, \sigma^2) \stackrel{\text{def}}{=} \mu_{\sigma^2}(r_{\text{eff}}\mathcal{B}) - \mu_{\sigma^2}(\mathcal{V}_L) \quad (64)$$

$$= \mathbb{E}\left[\frac{1}{\left(\frac{\sqrt{\sigma^2 W}}{r_{\text{eff}}}\right)^n} \left(g_{\mathcal{B}}(\sqrt{\sigma^2 W}) - g_L(\sqrt{\sigma^2 W})\right)\right] \quad (65)$$

$$= \mathbb{E}\left[\frac{1}{X_W} \left(g_{\mathcal{B}}\left(r_{\text{eff}} X_W^{1/n}\right) - g_L\left(r_{\text{eff}} X_W^{1/n}\right)\right)\right]. \quad (66)$$

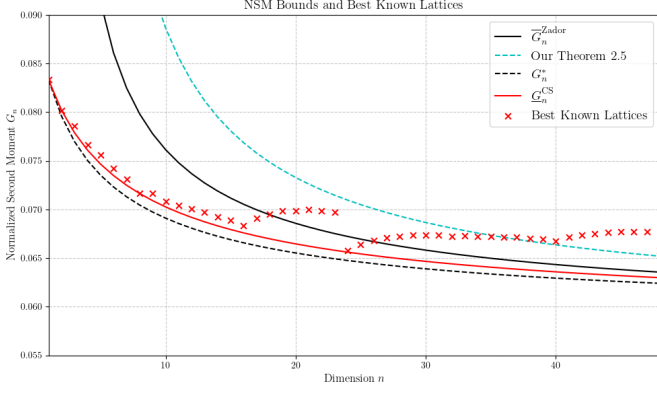
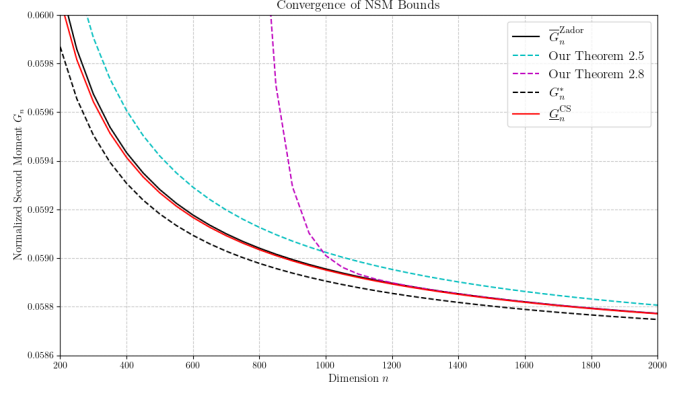
(a) $n \in [1, 48]$ (b) $n \in [200, 2000]$

Figure 2: Various bounds on the optimal NSM (due to [72]).

Consequently,

$$\mathbb{E}[P_e(L, \sigma^2)] = P^{\text{SP}}(\sigma^2) + (\mathbb{E}[P_e(L, \sigma^2)] - P^{\text{SP}}(\sigma^2)) \quad (67)$$

$$= P^{\text{SP}}(\sigma^2) + (\mu_{\sigma^2}(r_{\text{eff}}\mathcal{B}) - \mathbb{E}[\mu_{\sigma^2}(\mathcal{V}_L)]) \quad (68)$$

$$= P^{\text{SP}}(\sigma^2) + \mathbb{E}_{\mu_n}[\Delta(L, \sigma^2)] \quad (69)$$

$$= P^{\text{SP}}(\sigma^2) + \mathbb{E}_W \left[\frac{1}{X_W} \left(g_B \left(r_{\text{eff}} X_W^{1/n} \right) - \mathbb{E}_{\mu_n} \left[g_L \left(r_{\text{eff}} X_W^{1/n} \right) \right] \right) \right] \quad (70)$$

$$= P^{\text{SP}}(\sigma^2) + \mathbb{E}_W \left[\frac{1}{X_W} \left(\min\{X_W, 1\} - \mathbb{E}_{\mu_n} \left[g_L \left(r_{\text{eff}} X_W^{1/n} \right) \right] \right) \right] \quad (71)$$

$$\leq P^{\text{SP}}(\sigma^2) + \mathbb{E}_W \left[\frac{1}{X_W} \left(\min\{X_W, 1\} - \frac{X_W}{1 + X_W} \right) \right], \quad (72)$$

where in (71) we used $g_B(r_{\text{eff}} X_W^{1/n}) = \min\{X_W, 1\}$ which follows from (14), and (72) follows from Theorem II.3. This establishes (63). $\square$

One can also use Theorem II.4 to derive an upper bound on $\mathbb{E}_{\mu_n}[P_e(L, \sigma^2)]$. However, such bound is not useful for most values of n and σ^2 due to the $e^{-\eta/2}$ term in $\underline{g}_{\text{covering}}(r)$.

Remark II.12. Let $\tilde{Z} \sim \chi_n^2$ be a chi-squared random variable with n degrees of freedom. The best known upper bound to date on $\mathbb{E}[P_e(L, \sigma^2)]$, due to Poltyrev [7] and Ingber, Zamir, and Feder [8, Theorem 2], see also [18, Chapter 13.4], is the bound

$$\begin{aligned} \mathbb{E}_{\mu_n}[P_e(L, \sigma^2)] &\leq P_e^{\text{MLB}}(\sigma^2) \stackrel{\text{def}}{=} \mathbb{E} \left[\min \left\{ \left(\frac{\sigma^2 \tilde{Z}}{r_{\text{eff}}^2} \right)^{\frac{n}{2}}, 1 \right\} \right] \\ &= P^{\text{SP}}(\sigma^2) + \mathbb{E}[X_{\tilde{Z}} \mathbf{1}\{X_{\tilde{Z}} \leq 1\}], \end{aligned} \quad (73)$$

where

$$X_{\tilde{Z}} \stackrel{\text{def}}{=} \left(\frac{\sqrt{\sigma^2 \tilde{Z}}}{r_{\text{eff}}} \right)^n. \quad (74)$$

The bound we obtained in Theorem II.11, is quite similar to $P_e^{\text{MLB}}(\sigma^2)$. An analytic comparison seems non-trivial. In Figure 3 we evaluate the two bounds numerically, along with $P^{\text{SP}}(\sigma^2)$ for $\sigma^2 = \frac{0.95}{2\pi e}$ and for $\sigma^2 = \frac{0.98}{2\pi e}$, and growing n . The two bounds are seen to be very close.

III. LINEAR CODES

Let $\mathcal{C} \subset \mathbb{F}_2^n$ be a linear code of dimension $0 \leq k \leq n$. Denote the Voronoi region of the code by

$$\mathcal{V}_{\mathcal{C}} \stackrel{\text{def}}{=} \{x \in \mathbb{F}_2^n : d_H(x, 0) \leq d_H(x, y) \forall y \in \mathcal{C} \setminus \{0\}\}, \quad (75)$$

where $d_H(x, y)$ denotes the Hamming distance between $x, y \in \mathbb{F}_2^n$, and ties are broken in a systematic manner such that the cells $c + \mathcal{V}_{\mathcal{C}}$, $c \in \mathcal{C}$ form a disjoint partition of $\mathbb{F}_2^n$. Clearly, $|\mathcal{V}_{\mathcal{C}}| = 2^{n-k}$. Let $U_{\mathcal{C}} \sim \text{Uniform}(\mathcal{V}_{\mathcal{C}})$. The Voronoi spherical CDF of $\mathcal{C}$ is defined as

$$Q_{\mathcal{C}}(r) \stackrel{\text{def}}{=} \Pr(|U_{\mathcal{C}}| \leq r), \quad r = 0, 1, \dots, n. \quad (76)$$

Here and throughout, for a vector $x \in \mathbb{F}_2^n$ we denote its Hamming weight by $|x| = \sum_{i=1}^n x_i$. Recall that we abuse notation and also denote the size of a set $\mathcal{A} \subset \mathbb{F}_2^n$ as $|\mathcal{A}|$.

As is the case for lattices, $Q_{\mathcal{C}}(r)$ encodes many of the important properties of the code $\mathcal{C}$. Before specifying how $Q_{\mathcal{C}}(r)$ encodes these properties, we will need some definitions.

For integers $0 \leq r \leq n$, denote the Hamming sphere of radius r in $\mathbb{F}_2^n$ by

$$\mathcal{S}_{n,r} \stackrel{\text{def}}{=} \{x \in \mathbb{F}_2^n : |x| = r\}, \quad (77)$$

and the closed Hamming ball in $\mathbb{F}_2^n$ with radius r by

$$\mathcal{B}_{n,r} \stackrel{\text{def}}{=} \{x \in \mathbb{F}_2^n : |x| \leq r\}. \quad (78)$$

Denote the size of $\mathcal{B}_{n,r}$ as

$$V_{n,r} = |\mathcal{B}_{n,r}| = \sum_{j=0}^r \binom{n}{j}. \quad (79)$$

Note that

$$Q_{\mathcal{C}}(r) = \frac{1}{|\mathcal{V}_{\mathcal{C}}|} |\mathcal{B}_{n,r} \cap \mathcal{V}_{\mathcal{C}}| = 2^{k-n} |\mathcal{B}_{n,r} \cap \mathcal{V}_{\mathcal{C}}|. \quad (80)$$

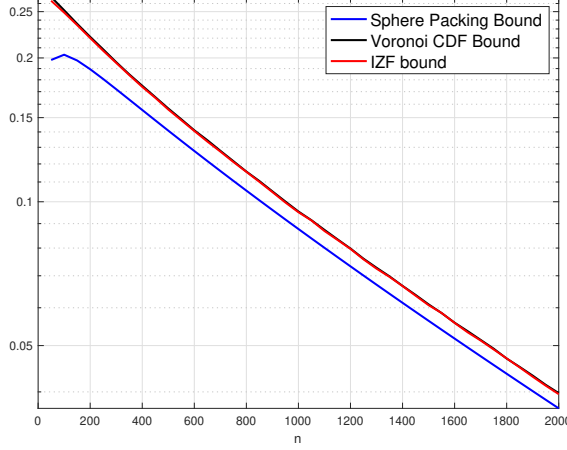
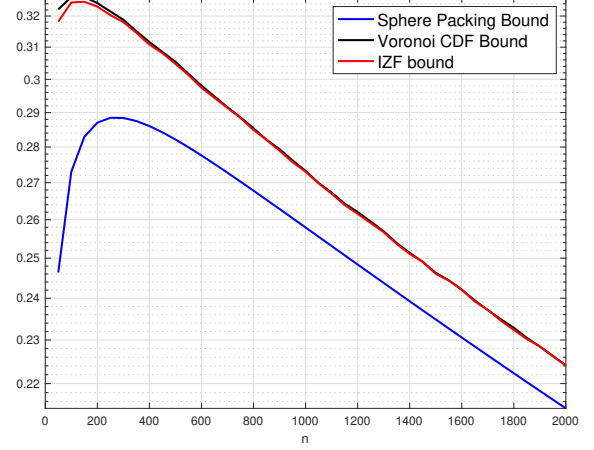
(a) $\sigma^2 = \frac{0.95}{2\pi e}$ (b) $\sigma^2 = \frac{0.98}{2\pi e}$

Figure 3: Computation of the sphere packing lower bound, the $P_e^{\text{MLB}}(\sigma^2)$ bound from [8, Theorem 2], and the new upper bound from Theorem II.11. The bounds are plotted for $\sigma^2 = \frac{0.95}{2\pi e}$ and $\sigma^2 = \frac{0.98}{2\pi e}$.

Proposition III.1. Let $\mathcal{C} \subset \mathbb{F}_2^n$ be a linear code of dimension $0 \leq k \leq n$. Then

1) The packing radius of $\mathcal{C}$ is

$$r_{\text{pack}}(\mathcal{C}) = \max \{r \in \{0, 1, \dots, n\} : Q_{\mathcal{C}}(r) = 2^{k-n} V_{n,r}\} \quad (81)$$

2) The covering radius of $\mathcal{C}$ is

$$r_{\text{cov}}(\mathcal{C}) = \min \{r \in \{0, 1, \dots, n\} : Q_{\mathcal{C}}(r) = 1\} \quad (82)$$

3) The Hamming distortion of $\mathcal{C}$ is

$$D_{\mathcal{C}} \stackrel{\text{def}}{=} \frac{\mathbb{E}|U_{\mathcal{C}}|}{n} = \frac{1}{n} \sum_{r=0}^n 1 - Q_{\mathcal{C}}(r). \quad (83)$$

4) Let $Z \sim \text{Ber}^{\otimes n}(p)$, The error probability of $\mathcal{C}$ for crossover probability p is

$$\begin{aligned} P_e(\mathcal{C}, p) &= \Pr(Z \notin \mathcal{V}_{\mathcal{C}}) \\ &= 1 - 2^{n-k} \left(\frac{p}{1-p} \cdot p^n + \frac{1-2p}{1-p} \mathbb{E} \left[\frac{Q_{\mathcal{C}}(|Z|)}{\binom{n}{|Z|}} \right] \right), \end{aligned} \quad (84)$$

where $|Z| \sim \text{Binomial}(n, p)$.

The proof is given in Appendix E. The fourth item is a consequence of the following more general proposition, whose proof is also brought in Appendix E.

Proposition III.2. Let $\mathcal{K} \subset \mathbb{F}_2^n$ be a subset, and for $U_{\mathcal{K}} \sim \text{Uniform}(\mathcal{K})$ define

$$Q_{\mathcal{K}}(r) = \Pr(|U_{\mathcal{K}}| \leq r) = \frac{|\mathcal{K} \cap \mathcal{B}_{n,r}|}{|\mathcal{K}|}. \quad (85)$$

Then, for $Z \sim \text{Ber}^{\otimes n}(p)$ we have

$$\begin{aligned} \mu_p(\mathcal{K}) &\stackrel{\text{def}}{=} \Pr(Z \in \mathcal{K}) \\ &= |\mathcal{K}| \left(\frac{p}{1-p} \cdot p^n + \frac{1-2p}{1-p} \mathbb{E} \left[\frac{Q_{\mathcal{K}}(|Z|)}{\binom{n}{|Z|}} \right] \right), \end{aligned} \quad (86)$$

where $|Z| \sim \text{Binomial}(n, p)$.

A. Estimates for the expected Voronoi spherical CDF

For $k \in \{1, \dots, n\}$, let the discrete Grassmannian $\text{Gr}_{n,k}(\mathbb{F}_2)$ denote the collection of subspaces of dimension k in $\mathbb{F}_2^n$, or equivalently, all linear codes of dimension k in $\mathbb{F}_2^n$. Let $\mathbb{T}_{\mathcal{C}} = \mathbb{F}_2^n / \mathcal{C}$ be the quotient group corresponding to $\mathcal{C} \in \text{Gr}_{n,k}(\mathbb{F}_2)$, and let $\pi_{\mathcal{C}} : \mathbb{F}_2^n \rightarrow \mathbb{T}_{\mathcal{C}}$ be the projection operator to the quotient group. Note that $\mathcal{V}_{\mathcal{C}}$ is isomorphic to $\mathbb{T}_{\mathcal{C}}$. Thus, one can think of the quotient map as $\pi_{\mathcal{C}}(x) = x - f_{\mathcal{C}}(x)$, where $f_{\mathcal{C}}(x) : \mathbb{F}_2^n \rightarrow \mathcal{C}$ maps each point in $\mathbb{F}_2^n$ to its nearest codeword $c \in \mathcal{C}$ such that $x \in c + \mathcal{V}_{\mathcal{C}}$. For a set $\mathcal{K} \subset \mathbb{F}_2^n$ we denote $\pi_{\mathcal{C}}(\mathcal{K}) = \{\pi_{\mathcal{C}}(x) : x \in \mathcal{K}\}$. Let $m_{\mathcal{C}} : \mathbb{T}_{\mathcal{C}} \rightarrow [0, 1]$ denote the normalized counting measure (uniform distribution) on $\mathbb{T}_{\mathcal{C}}$. Namely, for any $\mathcal{A} \subset \mathbb{T}_{\mathcal{C}}$ we have

$$m_{\mathcal{C}}(\mathcal{A}) \stackrel{\text{def}}{=} \frac{|\mathcal{A}|}{|\mathbb{T}_{\mathcal{C}}|} = 2^{k-n} |\mathcal{A}|. \quad (87)$$

Observe that for any $\mathcal{K} \subset \mathbb{F}_2^n$ it holds that

$$m_{\mathcal{C}}(\pi_{\mathcal{C}}(\mathcal{K})) = \sum_{x \in \mathcal{K}} \frac{2^{k-n}}{|(x + \mathcal{C}) \cap \mathcal{K}|} \quad (88)$$

$$= \sum_{x \in \mathcal{K}} \frac{2^{k-n}}{1 + |(\mathcal{C} \setminus \{0\}) \cap (\mathcal{K} - x)|}. \quad (89)$$

Furthermore, observe that

$$Q_{\mathcal{C}}(r) = \Pr(|U_{\mathcal{C}}| \leq r) = 2^{k-n} |\mathcal{B}_{n,r} \cap \mathcal{V}_{\mathcal{C}}| = m_{\mathcal{C}}(\pi_{\mathcal{C}}(\mathcal{B}_{n,r})), \quad (90)$$

where the last equality holds since, when we identify $\mathcal{V}_{\mathcal{C}}$ with $\mathbb{T}_{\mathcal{C}}$, it holds that $|\pi_{\mathcal{C}}(x)| \leq |x|$ for any $x \in \mathbb{F}_2^n$. In particular, for all $x \in \mathcal{B}_{n,r}$ we have that $\pi_{\mathcal{C}}(x) \in \mathcal{B}_{n,r}$. Thus, $\pi_{\mathcal{C}}(\mathcal{B}_{n,r}) \subset (\mathcal{B}_{n,r} \cap \mathcal{V}_{\mathcal{C}})$. On the other hand, for any point $x \in \mathcal{V}_{\mathcal{C}}$ we have that $\pi_{\mathcal{C}}(x) = x$, and consequently $\pi_{\mathcal{C}}(\mathcal{B}_{n,r}) \supset \pi_{\mathcal{C}}(\mathcal{B}_{n,r} \cap \mathcal{V}_{\mathcal{C}}) = (\mathcal{B}_{n,r} \cap \mathcal{V}_{\mathcal{C}})$. Thus, $\pi_{\mathcal{C}}(\mathcal{B}_{n,r}) = (\mathcal{B}_{n,r} \cap \mathcal{V}_{\mathcal{C}})$.

Theorem III.3. Let $\mathcal{C}$ be a random code drawn uniformly over $\text{Gr}_{n,k}(\mathbb{F}_2)$. Then, for any $\mathcal{K} \in \mathbb{F}_2^n$ we have that

$$\mathbb{E}[m_{\mathcal{C}}(\pi_{\mathcal{C}}(\mathcal{K}))] \geq \frac{2^{k-n}|\mathcal{K}|}{1 + 2^{k-n}|\mathcal{K}|}. \quad (91)$$

In particular,

$$\mathbb{E}_{\mathcal{C}}[Q_{\mathcal{C}}(r)] \geq \frac{2^{k-n}V_{n,r}}{1 + 2^{k-n}V_{n,r}}. \quad (92)$$

Proof. Starting from (89), and using Jensen's inequality with the convexity of $t \mapsto \frac{1}{1+t}$, we obtain

$$\mathbb{E}[m_{\mathcal{C}}(\pi_{\mathcal{C}}(\mathcal{K}))] = \mathbb{E}\left[\sum_{x \in \mathcal{K}} \frac{2^{k-n}}{1 + |(\mathcal{C} \setminus \{0\}) \cap (\mathcal{K} - x)|}\right] \quad (93)$$

$$\geq \sum_{x \in \mathcal{K}} \frac{2^{k-n}}{1 + \mathbb{E}[|(\mathcal{C} \setminus \{0\}) \cap (\mathcal{K} - x)|]}. \quad (94)$$

Since $\mathcal{C} \sim \text{Uniform}(\text{Gr}_{n,k}(\mathbb{F}_2))$, for any $x \in \mathcal{K}$ it holds that

$$\mathbb{E}[|(\mathcal{C} \setminus \{0\}) \cap (\mathcal{K} - x)|] = \frac{2^k - 1}{2^n - 1}(|\mathcal{K}| - 1) < 2^{k-n}|\mathcal{K}|. \quad (95)$$

Thus,

$$\mathbb{E}[m_{\mathcal{C}}(\pi_{\mathcal{C}}(\mathcal{K}))] \geq \sum_{x \in \mathcal{K}} \frac{2^{k-n}}{1 + 2^{k-n}|\mathcal{K}|} = \frac{2^{k-n}|\mathcal{K}|}{1 + 2^{k-n}|\mathcal{K}|}, \quad (96)$$

establishing (91). Combining (90) with (91) applied with $\mathcal{K} = \mathcal{B}_{n,r}$, we obtain

$$\mathbb{E}[Q_{\mathcal{C}}(r)] = \mathbb{E}[\Pr(|U_{\mathcal{C}}| \leq r)] \geq \frac{2^{k-n}|\mathcal{B}_{n,r}|}{1 + 2^{k-n}|\mathcal{B}_{n,r}|} \quad (97)$$

$$= \frac{2^{k-n}V_{n,r}}{1 + 2^{k-n}V_{n,r}}, \quad (98)$$

which establishes (92). $\square$

B. Hamming distortion of a linear code

As a straightforward consequence of Proposition III.1 and of Theorem III.3 we obtain the following.

Theorem III.4. Let $\mathcal{C}$ be a random code drawn uniformly over $\text{Gr}_{n,k}(\mathbb{F}_2)$. Then,

$$\mathbb{E}[D_{\mathcal{C}}] \leq \frac{1}{n} \sum_{r=0}^{n-1} \frac{1}{1 + 2^{k-n}V_{n,r}}. \quad (99)$$

Proof. Combining part 3 of Proposition III.1 and (92) of Theorem III.3, we obtain

$$\mathbb{E}[D_{\mathcal{C}}] = \frac{1}{n} \sum_{r=0}^{n-1} \mathbb{E}[1 - Q_{\mathcal{C}}(r)] \quad (100)$$

$$\leq \frac{1}{n} \sum_{r=0}^{n-1} 1 - \frac{2^{k-n}V_{n,r}}{1 + 2^{k-n}V_{n,r}} \quad (101)$$

$$= \frac{1}{n} \sum_{r=0}^{n-1} \frac{1}{1 + 2^{k-n}V_{n,r}}, \quad (102)$$

as claimed. $\square$

For a set $\mathcal{K} \subset \mathbb{F}_2^n$ of size $|\mathcal{K}|$, we define $r_{\text{eff}} = r_{\text{eff}}(\mathcal{K})$ as the unique integer $0 \leq r_{\text{eff}} \leq n$ such that $V_{n,r_{\text{eff}}-1} < |\mathcal{K}| \leq V_{n,r_{\text{eff}}}$, with the convention that $V_{n,-1} = -\infty$. We further define the quasi-ball $\mathcal{B}_{\mathcal{K}}$ as the union of $\mathcal{B}_{n,r_{\text{eff}}-1}$ and the first $|\mathcal{K}| - V_{n,r_{\text{eff}}-1}$ vectors of Hamming weight r_{eff} in lexicographic order (there is no significance to which $|\mathcal{K}| - V_{n,r_{\text{eff}}-1}$ vectors of Hamming weight r_{eff} we choose, we take the first ones in lexicographic order just to avoid ambiguity). For a linear code $\mathcal{C} \subset \mathbb{F}_2^n$ of dimension $0 \leq k \leq n$, we have that $r_{\text{eff}}(\mathcal{V}_{\mathcal{C}})$, as well as $\mathcal{B}_{\mathcal{V}_{\mathcal{C}}}$, depend only on k and n , and we therefore denote them by

$$r_{\text{eff}}(n, k) \stackrel{\text{def}}{=} \min\{r : 2^{n-k} \leq V_{n,r}\}, \quad (103)$$

and $\bar{\mathcal{B}}^{n,k}$, respectively.

Let $U_{\bar{\mathcal{B}}^{n,k}} \sim \text{Uniform}(\bar{\mathcal{B}}^{n,k})$. We clearly have that for any $\mathcal{C} \in \text{Gr}_{n,k}(\mathbb{F}_2)$

$$D_{\mathcal{C}} \geq D_{n,k}^* = \frac{1}{n} \mathbb{E}[|U_{\bar{\mathcal{B}}^{n,k}}|]. \quad (104)$$

See Lemma III.8 below for a more general statement. Defining $Q_{\bar{\mathcal{B}}^{n,k}}(r)$ as in (85), we also have that

$$Q_{\bar{\mathcal{B}}^{n,k}}(r) = \min\{2^{k-n}V_{n,r}, 1\}, \quad (105)$$

and therefore, using item 3 of Proposition III.1, that holds for any set, not just a Voronoi region, we have

$$D_{n,k}^* = \frac{1}{n} \sum_{r=0}^{r_{\text{eff}}(n,k)-1} 1 - 2^{k-n}V_{n,r}. \quad (106)$$

Combining this with Theorem III.4 we obtain

$$\Delta(n, k) \stackrel{\text{def}}{=} n(\mathbb{E}[D_{\mathcal{C}}] - D_{n,k}^*) \quad (107)$$

$$\leq \sum_{r=0}^{r_{\text{eff}}(n,k)-1} \frac{x_r^2}{1 + x_r} + \sum_{r=r_{\text{eff}}(n,k)}^{n-1} \frac{1}{1 + x_r}, \quad (108)$$

where

$$x_r = x_{r,n,k} \stackrel{\text{def}}{=} 2^{k-n}V_{n,r}. \quad (109)$$

We prove the following result in Appendix E.

Theorem III.5. Assume $k > \alpha n$ for some $\alpha > 0$. Then, there exists a universal constant $c = c_{\alpha} > 0$, independent of n , such that $\Delta(n, k) < c$.

Remark III.6. The result above requires that k is not too small. We claim that while our requirement $k = \Omega(n)$ may possibly be relaxed, a lower bound on k is unavoidable. In particular, if $k = 1$, the expected distortion $D_{\mathcal{C}}$ is minimized by $\mathcal{C} = \{0 \dots 0, 1 \dots 1\}$ (which is a perfect code, that attains the lower bound $D_{n,1}^*$). On the other hand, $\mathbb{E}[D_{\mathcal{C}}]$ is higher by $\Omega(\sqrt{n})$.

Remark III.7. A related quantity to $D_{\mathcal{C}}$ is the covering radius $r_{\text{cov}}(\mathcal{C})$. In particular, $nD_{\mathcal{C}} \leq r_{\text{cov}}(\mathcal{C})$. For any code, the covering radius is at least $r_{\text{eff}}(n, k)$, and there exist codes with covering radius $r_{\text{eff}}(n, k) + O(\log n)$ [54]. One can use such bounds to deduce that there exists $\mathcal{C}$ with $n(D_{\mathcal{C}} - D_{n,k}^*) = O(\log n)$. Our Theorem III.5 is significantly tighter as it bounds this gap by a constant.

1) *Lossy compression of binary symmetric source under Hamming distortion:* Let $X \sim \text{Ber}^{\otimes n}(1/2)$, and let $0 \leq R \leq 1$. An (n, R, D) code for X consists of an encoder³ $f: \mathbb{F}_2^n \rightarrow \llbracket 2^{nR} \rrbracket$, and a decoder $g: \llbracket 2^{nR} \rrbracket \rightarrow \mathbb{F}_2^n$, such that

$$\frac{1}{n} \mathbb{E}[d_H(X, g(f(X)))] \leq D. \quad (110)$$

Denote

$$D_n(R) = \min\{D : \exists(n, R, D) - \text{code}\}. \quad (111)$$

It is well-known [73], [74] that

$$D(R) \leq D_n(R) < D(R) + O\left(\frac{\log n}{n}\right). \quad (112)$$

where

$$D(R) = 1 - h_2^{-1}(R), \quad (113)$$

and $h_2(p) = -p \log_2(p) - (1-p) \log_2(1-p)$, whereas $h_2^{-1}(\cdot)$ is its inverse restricted to $[0, 1/2)$. In fact, [75, Theorem 1] shows that

$$D_n(R) = D(R) - D'(R) \frac{\log n}{2 \log n} + o\left(\frac{\log n}{n}\right) \quad (114)$$

The following claim is essentially⁴ stated in [53, eq. 4.6-4.7], and for completeness of exposition we provide a proof in Appendix E.

Lemma III.8. Assume $R = \frac{k}{n}$ for some integer $0 \leq k \leq n$, then $D_n(R) \geq D_{n,k}^*$.

In light of this, and of Theorem III.5, we have the following.

Theorem III.9. Let $0 \leq k \leq n$ be an integer, and $R = \frac{k}{n} > \alpha > 0$. Then

$$D_n(R) = D_{n,k}^* + O_\alpha\left(\frac{1}{n}\right), \quad (115)$$

and this is achievable using a linear code.

Proof. The lower bound $D_n(R) \geq D_{n,k}^*$ follows from Lemma III.8. For the upper bound, we construct f and g from a linear code $\mathcal{C}$ as follows. We enumerate the 2^k points in $\mathcal{C}$. The encoder $f(X)$ outputs the index of the codeword $c \in \mathcal{C}$ for which $X \in c + \mathcal{V}_\mathcal{C}$, and the decoder g outputs c based on this index. The reconstruction error is uniformly distributed on $\mathcal{V}_\mathcal{C}$ and therefore the obtained distortion is $D_\mathcal{C}$. By Theorem III.5, there must exist a code $\mathcal{C}$ with $D_\mathcal{C} \leq \mathbb{E}[D_\mathcal{C}] < D_{n,k}^* + c_\alpha/n$, establishing our claim. $\square$

Remark III.10. Let $\mathcal{C}$ be the image of the decoder $g(\cdot)$. If $\mathcal{C}$ is not restricted to be a linear code (a subspace of $\mathbb{F}_2^n$), one can obtain even better upper bounds on the expected distortion. In

particular, if we draw the $2^{nR} = 2^k$ points of $\mathcal{C}$ iid uniformly on $\mathbb{F}_2^n$, we will obtain [76],[74, Ex. V3]

$$n\mathbb{E}[D] = \sum_{r=0}^n (1 - 2^{-n} V_{n,r})^{2^k} \leq \sum_{r=0}^n (1 - 2^{k-n} V_{n,r}) \quad (116)$$

$$\leq \sum_{r=0}^n \frac{1}{1 + 2^{k-n} V_{n,r}}, \quad (117)$$

where the last bound is the bound from Theorem III.4. However, the first equality relies on the statistical independence of all 2^k codewords. Since codewords in a linear code are just pairwise independent, this derivation is not valid for linear codes.

C. Error probability of a linear code

Let $p \in (0, 1/2)$ and let $Z \sim \text{Ber}^{\otimes n}(p)$. For a set $\mathcal{K} \subset \mathbb{F}_2^n$ let

$$\mu_p(\mathcal{K}) \stackrel{\text{def}}{=} \Pr(Z \in \mathcal{K}) = (1-p)^n \sum_{x \in \mathcal{K}} \left(\frac{p}{1-p}\right)^{|x|}. \quad (118)$$

By definition, $|\bar{\mathcal{B}}^{n,k}| = |\mathcal{V}_\mathcal{C}|$, and since $\left(\frac{p}{1-p}\right)^{|x|}$ is monotonically decreasing in $|x|$, we have that

$$\mu_p(\mathcal{V}_\mathcal{C}) \leq \mu_p(\bar{\mathcal{B}}^{n,k}). \quad (119)$$

Let $X \sim \text{Uniform}(\mathcal{C})$ be statistically independent of Z . The error probability in maximum-likelihood decoding of X from the output $Y = X + Z$ of the binary symmetric channel with crossover probability p , is

$$P_e(\mathcal{C}, p) = 1 - \mu_p(\mathcal{V}_\mathcal{C}). \quad (120)$$

Clearly,

$$P_e(\mathcal{C}, p) \geq P_e(\bar{\mathcal{B}}^{n,k}, p) = 1 - \mu_p(\bar{\mathcal{B}}^{n,k}) \stackrel{\text{def}}{=} P_{n,k}^{\text{SP}}(p), \quad (121)$$

which is referred to as the sphere packing lower bound in the literature. We prove the following.

Theorem III.11. Let $\mathcal{C}$ be a random code drawn uniformly over $\text{Gr}_{n,k}(\mathbb{F}_2)$. Then, for any $p \in (0, 1/2)$ we have that

$$\mathbb{E}[P_e(\mathcal{C}, p)] \leq P_{n,k}^{\text{SP}}(p) + \frac{1-2p}{1-p} \mathbb{E}\left[\frac{V_{n,W}}{\binom{n}{W}} \cdot \frac{\min\{x_W, x_W^{-1}\}}{1+x_W}\right] \quad (122)$$

where $W \sim \text{Binomial}(n, p)$, and $x_r = 2^{k-n} V_{n,r}$.

Proof. We have

$$\mathbb{E}[P_e(\mathcal{C}, p)] = P_{n,k}^{\text{SP}}(p) + (\mathbb{E}[P_e(\mathcal{C}, p)] - P_{n,k}^{\text{SP}}(p)) \quad (123)$$

$$= P_{n,k}^{\text{SP}} + (\mu_p(\bar{\mathcal{B}}^{n,k}) - \mathbb{E}[\mu_p(\mathcal{V}_\mathcal{C})]). \quad (124)$$

By Proposition III.2 and (105), we have that

$$\begin{aligned} \mu_p(\bar{\mathcal{B}}^{n,k}) &= 2^{n-k} \left(\frac{p}{1-p} \cdot p^n + \frac{1-2p}{1-p} \mathbb{E}\left[\frac{\min\{2^{k-n} V_{n,|Z|}, 1\}}{\binom{n}{|Z|}}\right] \right). \end{aligned} \quad (125)$$

³For $x > 1$ we write $\lfloor x \rfloor$ to denote the largest integer smaller than x , and $\llbracket x \rrbracket = \{1, \dots, \lfloor x \rfloor\}$.

⁴Our definition of $D_{n,k}^*$ corresponds to the average distortion of a quasi-ball with size 2^{n-k} , whereas Gobblick lower bounds the expected distortion of a code with 2^k codewords by the average distortion of the largest ball whose size is at most than 2^{n-k} .

Similarly, by Proposition III.2 (or part 4 of Proposition III.1) together with Theorem III.3, we obtain that for $\mathcal{C} \sim \text{Uniform}(\text{Gr}_{n,k}(\mathbb{F}_2))$

$$\mathbb{E}[\mu_p(\mathcal{V}_\mathcal{C})] \geq 2^{n-k} \left(\frac{p}{1-p} p^n + \frac{1-2p}{1-p} \mathbb{E} \left[\frac{2^{k-n} V_{n,|Z|}}{\binom{n}{|Z|} (1 + 2^{k-n} V_{n,|Z|})} \right] \right). \quad (126)$$

Consequently, we obtain

$$\Delta_{n,k}^p \stackrel{\text{def}}{=} \mu_p(\mathcal{B}^{n,k}) - \mathbb{E}[\mu_p(\mathcal{V}_\mathcal{C})] \quad (127)$$

$$\leq \frac{1-2p}{1-p} 2^{n-k} \mathbb{E} \left[\frac{1}{\binom{n}{|Z|}} \left(\min\{x_{|Z|}, 1\} - \frac{x_{|Z|}}{1+x_{|Z|}} \right) \right] \quad (128)$$

$$= \frac{1-2p}{1-p} 2^{n-k} \mathbb{E} \left[\frac{1}{\binom{n}{|Z|}} \left(\frac{\min\{x_{|Z|}^2, 1\}}{1+x_{|Z|}} \right) \right] \quad (129)$$

$$= \frac{1-2p}{1-p} 2^{n-k} \cdot \mathbb{E} \left[\frac{1}{\binom{n}{|Z|}} \left(\frac{\min\{2^{k-n} V_{n,|Z|} \cdot x_{|Z|}, 2^{k-n} V_{n,|Z|} \cdot x_{|Z|}^{-1}\}}{1+x_{|Z|}} \right) \right] \quad (130)$$

$$= \frac{1-2p}{1-p} \mathbb{E} \left[\frac{V_{n,|Z|}}{\binom{n}{|Z|}} \cdot \frac{\min\{x_{|Z|}, x_{|Z|}^{-1}\}}{1+x_{|Z|}} \right]. \quad (131)$$

Substituting this into (124) established the claim. $\square$

Remark III.12. The benchmark upper bound to date for the binary symmetric channel is the so-called random coding upper bound (RCU bound) from [9] and [10, Theorem 33], which implies that for a random linear code

$$\mathbb{E}[P_e(\mathcal{C}, p)] \leq \text{RCU}(n, k, p) \stackrel{\text{def}}{=} \mathbb{E}[\min\{1, 2^{k-n} V_{n,W}\}]. \quad (132)$$

It is not straightforward to compare the upper bound from Theorem III.11 and the RCU bound. However, numerically it seems that the new bound from Theorem III.11 does dominate the RCU bound. See Figure 4 for a numeric demonstration.

APPENDIX A

PROOFS OF CLAIMS FOR LATTICES

Proof of Proposition II.1. The first item follows since

$$r_{\text{pack}}(L) = \sup\{r : r\mathcal{B} \subset \mathcal{V}_L\} \quad (133)$$

$$= \sup\left\{r : g_L(r) = \left(\frac{r}{r_{\text{eff}}}\right)^n\right\}, \quad (134)$$

where in the second equality we have used (6). The second item follows since

$$r_{\text{cov}}(L) = \sup_{x \in \mathbb{R}^n} \min_{y \in L} \|x - y\|_2 = \sup_{x \in \mathcal{V}_L} \|x\|_2. \quad (135)$$

For the third item, we write

$$\mathbb{E}\|U_L\|^2 = \int_{r=0}^{\infty} \Pr(\|U_L\|^2 > r) dr \quad (136)$$

$$= \int_{r=0}^{\infty} 1 - \Pr(\|U_L\| \leq \sqrt{r}) dr. \quad (137)$$

The fourth item follows directly from Proposition III.2. $\square$

Proof of Proposition II.2. Denote $C_n = C_{\sigma^2, n} = \frac{1}{(2\pi\sigma^2)^{n/2}}$ and let $U = U_{\mathcal{K}} \sim \text{Uniform}(\mathcal{K})$. It immediately follows that

$$\mu_{\sigma^2}(\mathcal{K}) = C_n \cdot |\mathcal{K}| \cdot \mathbb{E} \left[e^{-\frac{\|U\|_2^2}{2\sigma^2}} \right] \quad (138)$$

$$= C_n \cdot |\mathcal{K}| \cdot \int_0^{\infty} \Pr \left(e^{-\frac{\|U\|_2^2}{2\sigma^2}} \geq r \right) dr \quad (139)$$

$$= C_n \cdot |\mathcal{K}| \cdot \int_0^1 \Pr \left(\|U\|_2 \leq \left(2\sigma^2 \log \left(\frac{1}{r} \right) \right)^{\frac{1}{2}} \right) dr \quad (140)$$

$$= C_n \cdot V_n r_{\text{eff}}^n \cdot \int_0^1 \Pr \left(\|U\|_2 \leq \left(2\sigma^2 \log \left(\frac{1}{r} \right) \right)^{\frac{1}{2}} \right) dr \quad (141)$$

Making the change of variables $r = e^{-\frac{w}{2}}$, $dr = -\frac{1}{2}e^{-\frac{w}{2}} dw$, we obtain

$$\mu_{\sigma^2}(\mathcal{K}) = C_n \cdot V_n r_{\text{eff}}^n \cdot \int_0^{\infty} \frac{1}{2} e^{-\frac{w}{2}} \Pr \left(\|U\|_2 \leq \sqrt{\sigma^2 w} \right) dw \quad (142)$$

$$= C_n \cdot V_n r_{\text{eff}}^n \cdot 2^{\frac{n}{2}} \Gamma \left(1 + \frac{n}{2} \right) \cdot \int_0^{\infty} \frac{w^{\frac{n+2}{2}-1} e^{-\frac{w}{2}} \Pr \left(\|U\|_2 \leq \sqrt{\sigma^2 w} \right)}{2^{\frac{n+2}{2}} \Gamma \left(\frac{n+2}{2} \right) w^{\frac{n}{2}}} dw \quad (143)$$

$$= C_n \cdot V_n \cdot 2^{\frac{n}{2}} \Gamma \left(1 + \frac{n}{2} \right) \cdot \mathbb{E} \left[\frac{\Pr \left(\|U\|_2 \leq \sqrt{\sigma^2 W} \right)}{\left(\frac{W}{r_{\text{eff}}^2} \right)^{\frac{n}{2}}} \right]. \quad (144)$$

It remains to evaluate the term multiplying the expectation. Recalling the definitions of V_n , and of C_n , we have

$$C_n \cdot V_{2,n} \cdot 2^{\frac{n}{2}} \Gamma \left(1 + \frac{n}{2} \right) = \frac{1}{(\sigma^2)^{\frac{n}{2}}}. \quad (145)$$

Substituting this into (144), establishes the claim. $\square$

APPENDIX B

PROOF OF THEOREM II.4

We now recall some fundamental results of Rogers and Schmidt. For a Borel measurable subset $J \subset \mathbb{R}^n$, and a lattice $L \in \mathcal{L}_n$, let

$$\varepsilon(J, L) \stackrel{\text{def}}{=} 1 - m_L(\pi_L(J));$$

equivalently, $\varepsilon(J, L)$ is the density of points in $\mathbb{R}^n$ not covered by $L + J$. Also recall the definition of η from (26). With these notations, the following is a corollary of [65] (see also [64], where a similar bound was shown for larger η , but with a large constant c_{Rog} instead of the constant 7 below):

Theorem B.1 (Corollary of Theorem 4 of [65]). *For all $n > 13$ and for every Borel measurable $J \subset \mathbb{R}^n$ with*

$$V \stackrel{\text{def}}{=} |J| \leq \eta$$

and bounded diameter we have

$$|\mathbb{E}_{\mu_n}[\varepsilon(J, L)] - e^{-V}| < 7 \cdot e^{-\eta}.$$

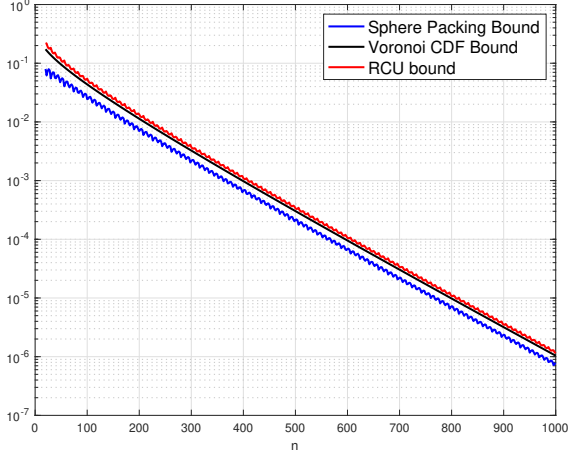
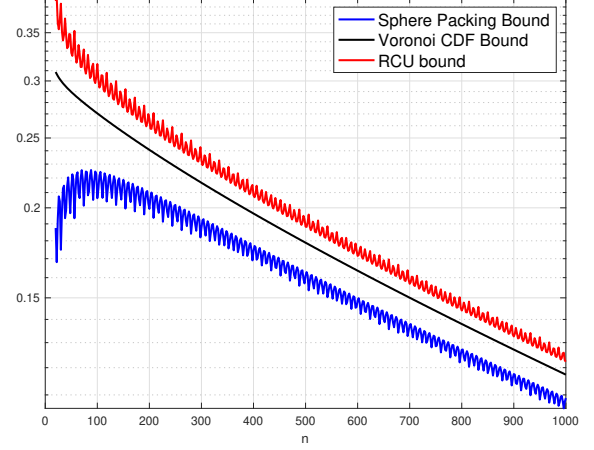
(a) $p = 0.07$ (b) $p = 0.1$

Figure 4: Computation of the sphere packing lower bound, the RCU bound from [10, Theorem 33], and the new upper bound from Theorem III.11. The bounds are plotted for $p = 0.07$ and $p = 0.1$, even values of n and $k = n/2$.

Proof. First, it is straightforward to verify that for $V \leq \eta$ we have that

$$e^{-V} (3/4)^{n/2} e^{4V} \leq e^{-\eta}, \quad e^{-V} V^{n-1} n^{-n+1} e^{V+n} \leq e^{-\eta}, \quad (146)$$

and consequently for $|R|$ defined in [65, eq. (3)], we have $e^{-V}|R| < 7e^{-\eta}$.

Let $z = \text{diam}(J) \cdot \sqrt{\frac{1}{4n}} \cdot [1 \ \cdots \ 1]^\top \in \mathbb{R}^n$, and define $\text{CUBE}(a) = z + [0, a]^n \subset \mathbb{R}^n$. Note that for any $t \in \text{CUBE}(a)$ there is no $x \in \mathbb{R}^n$ such that both $x \in (t+J)$ and $-x \in (t+J)$. We have that

$$\varepsilon(J, L) = \lim_{a \rightarrow \infty} \frac{1}{a^n} \int_{x \in \text{CUBE}(a)} \mathbb{1}\{|L \cap (x+J)| = \emptyset\} dx. \quad (147)$$

Consequently, by the bounded convergence theorem

$$\mathbb{E}_{\mu_n}[\varepsilon(J, L)] \quad (148)$$

$$= \lim_{a \rightarrow \infty} \frac{1}{a^n} \int_{x \in \text{CUBE}(a)} \mathbb{E}_{\mu_n}[\mathbb{1}\{|L \cap (x+J)| = \emptyset\}] dx \quad (149)$$

$$= \lim_{a \rightarrow \infty} \frac{1}{a^n} \int_{x \in \text{CUBE}(a)} \mu_n\{L \in \mathcal{L}_n : L \text{ is } (x+J) - \text{admissible}\} dx \quad (150)$$

$$= \lim_{a \rightarrow \infty} \frac{1}{a^n} \int_{x \in \text{CUBE}(a)} e^{-V} (1 - R) dx \quad (151)$$

$$\in e^{-V} \pm 7e^{-\eta}, \quad (152)$$

where in (151) we have applied [65, Theorem 4], and in the last step we used the fact that $e^{-V}|R| \leq 7e^{-\eta}$ provided that $|J| \leq \eta$. $\square$

Applying Theorem B.1 with $J = r\mathcal{B}$, whose volume is $|J| = (r/r_{\text{eff}})^n$, we obtain the following.

Corollary B.2. Assume $(r/r_{\text{eff}})^n \leq \eta$. Then, for $L \sim \mu_n$ we have

$$\mathbb{E}[g_L(r)] \geq 1 - e^{-(r/r_{\text{eff}})^n} - 7 \cdot e^{-\eta}. \quad (153)$$

Also, a straightforward application of Markov's inequality gives the following Corollary of Theorem B.1.

Corollary B.3. For J with volume $|J| = \eta$, we have

$$\mu_n\left(\left\{L \in \mathcal{L}_n : \varepsilon(J, L) > e^{-\eta/2}\right\}\right) \leq 8e^{-\eta/2} \quad (154)$$

Tracking down the constants in [66, Theorem 1.2], gives the following.

Theorem B.4 (Special case of Theorem 1.2 from [66]). For

$$\mathcal{E}_\eta = \{L \in \mathcal{L}_n : r_{\text{cov}}(L) \leq 4n^2\eta\} \quad (155)$$

and $L \sim \mu_n$, we have

$$\Pr(L \notin \mathcal{E}_\eta) \leq 16e^{-\eta/2}. \quad (156)$$

To obtain this result we apply the proof of [66, Theorem 1.2], with $V = \eta$, and $n < p < 2n$, using Corollary B.3 instead of [66, Corollary 2.4]. Note also that for $n \geq 13$ we have that $V = \eta > 2 \ln 2$. This gives that the covering density of L is smaller or equal to $p^2 V = p^2 \eta < 4n^2 \eta$ with probability at least

$$1 - \left(8e^{-V/2} + e^{2n/p} e^{-V/2}\right) \geq 1 - 16e^{-V/2} = 1 - 16e^{-\eta/2}.$$

With this, we are ready to prove Theorem II.4. Recall that μ_n is the Haar-Siegel probability distribution, and $\tilde{\mu}_n = \mu_n|_{\mathcal{E}_\eta}$. For all $r > 0$, we have

$$\begin{aligned} \mathbb{E}_{\mu_n}[g_L(r)] &= \Pr(L \in \mathcal{E}_\eta) \mathbb{E}[g_L(r) | L \in \mathcal{E}_\eta] + \Pr(L \notin \mathcal{E}_\eta) \mathbb{E}[g_L(r) | L \notin \mathcal{E}_\eta] \\ &= \Pr(L \in \mathcal{E}_\eta) \mathbb{E}_{\tilde{\mu}_n}[g_L(r)] + \Pr(L \notin \mathcal{E}_\eta) \mathbb{E}[g_L(r) | L \notin \mathcal{E}_\eta] \end{aligned} \quad (157)$$

$$\leq \mathbb{E}_{\tilde{\mu}_n}[g_L(r)] + \Pr(L \notin \mathcal{E}_\eta). \quad (158)$$

$$\leq \mathbb{E}_{\tilde{\mu}_n}[g_L(r)] + \Pr(L \notin \mathcal{E}_\eta). \quad (159)$$

Rearranging and applying Corollary B.2 and Theorem B.4, we obtain that for $(r/r_{\text{eff}})^n \leq \eta/2$

$$\mathbb{E}_{\tilde{\mu}_n}[g_L(r)] \geq 1 - e^{-(r/r_{\text{eff}})^n} - 7 \cdot e^{-\eta} - 16e^{-\eta/2} \quad (160)$$

$$\geq 1 - e^{-(r/r_{\text{eff}})^n} - 23 \cdot e^{-\eta/2}. \quad (161)$$

By monotonicity of $r \mapsto g_L(r)$, we have that $\mathbb{E}_{\tilde{\mu}_n}[g_L(r)] \geq 1 - 24e^{-\eta/2}$ for $(r/r_{\text{eff}})^n \geq \eta/2$. Finally, by definition of $\tilde{\mu}_n$ we have that for $(r/r_{\text{eff}})^n > 4n^2\eta$ it holds that $g_L(r) = 1$ with probability 1 for $L \sim \tilde{\mu}_n$. This establishes the claimed result.

APPENDIX C

PROOF OF LEMMA II.9

We will show that

$$\log \frac{\bar{G}_n^{\text{Zador}}}{\underline{G}_n^{\text{CS}}} = O\left(\frac{\log^2 n}{n^2}\right), \quad (162)$$

from which the claimed result immediately follows.

We use the standard asymptotic expansions for large z , small ε and large n [77, 6.141, 6.133] [78, Chapter 6.3]

$$\log \Gamma(z) = \left(z - \frac{1}{2}\right) \log z - z + \frac{1}{2} \log(2\pi) + O(z^{-1}), \quad (163)$$

$$\log \Gamma(1 + \varepsilon) = -\gamma \varepsilon + O(\varepsilon^2), \quad (164)$$

$$H_{n+2} = \log n + \gamma + O(n^{-1}). \quad (165)$$

Here γ is the Euler–Mascheroni constant.

We start by expanding $\log \bar{G}_n^{\text{Zador}}$. By definition of V_n in (4), we have

$$\log \bar{G}_n^{\text{Zador}} = -\log(n\pi) + \frac{2}{n} \log \Gamma\left(1 + \frac{n}{2}\right) + \log \Gamma\left(1 + \frac{2}{n}\right). \quad (166)$$

Applying (163) with $z = 1 + \frac{n}{2} = \frac{n}{2} \left(1 + \frac{2}{n}\right)$ and (164) with $\varepsilon = \frac{2}{n}$ yields after some straightforward algebra

$$\frac{2}{n} \log \Gamma\left(1 + \frac{n}{2}\right) = \left(\log \frac{n}{2} - 1\right) + \frac{\log(\pi n)}{n} + O(n^{-2}), \quad (167)$$

$$\log \Gamma\left(1 + \frac{2}{n}\right) = \frac{-2\gamma}{n} + O(n^{-2}), \quad (168)$$

so that

$$\log \bar{G}_n^{\text{Zador}} = -\log(2\pi) - 1 + \frac{\log(\pi n) - 2\gamma}{n} + O(n^{-2}). \quad (169)$$

We proceed to expand $\log \underline{G}_n^{\text{CS}}$. Inserting (54) into (53), and using $\log(1 + \frac{31}{12n} + O(n^{-2})) = O(n^{-1})$ gives

$$\begin{aligned} \log \underline{G}_n^{\text{CS}} &= \log\left(\frac{n+3-2H_{n+2}}{4n(n+1)}\right) + \frac{\log(n+1)}{n} \\ &\quad + \frac{4}{n} \log(n!) + \frac{2}{n} \log f_n(n) \end{aligned} \quad (170)$$

$$\begin{aligned} &= \log\left(\frac{n+3-2H_{n+2}}{4n(n+1)}\right) + \log\left(\frac{2e}{\pi n}\right) + \frac{2}{n} \log(n!) \\ &\quad + \frac{2 \log(n+1)}{n} - \frac{\log 2 + 2}{n} + O(n^{-2}). \end{aligned} \quad (171)$$

Applying (165), we obtain

$$\frac{n+3-2H_{n+2}}{n+1} = \frac{n+1-2(H_{n+2}-1)}{n+1} \quad (172)$$

$$= 1 - \frac{2(H_{n+2}-1)}{n+1} \quad (173)$$

$$= 1 - 2 \frac{\log(n) + (\gamma - 1) + O(n^{-1})}{n+1} \quad (174)$$

$$= 1 - \frac{2 \log n + 2(\gamma - 1)}{n} + O\left(\frac{\log n}{n^2}\right) \quad (175)$$

and consequently

$$\begin{aligned} &\log \frac{n+3-2H_{n+2}}{4n(n+1)} \\ &= -\log(4n) \\ &\quad + \log\left(1 - \frac{2 \log n + 2(\gamma - 1)}{n} + O\left(\frac{\log n}{n^2}\right)\right) \\ &= -\log(4n) \\ &\quad - \frac{2 \log n + 2(\gamma - 1)}{n} - \frac{2 \log^2(n)}{n} + O\left(\frac{\log(n)}{n^2}\right) \end{aligned} \quad (176)$$

Recalling that $n! = \Gamma(1+n)$ and applying (163) at integer $z = n+1$ (which is just Stirling's approximation) we obtain

$$\frac{2}{n} \log(n!) = 2 \log(n) - 2 + \frac{\log(2\pi n)}{n} + O(n^{-2}). \quad (178)$$

Substituting (177) and (178) into (171) gives (after careful algebra)

$$\begin{aligned} \log \underline{G}_n^{\text{CS}} &= -\log(2\pi) - 1 + \frac{\log(\pi n) - 2\gamma}{n} \\ &\quad - \frac{2 \log^2 n}{n^2} + O\left(\frac{\log n}{n^2}\right). \end{aligned} \quad (179)$$

Combining (169) with (179) gives

$$\log \frac{\bar{G}_n^{\text{Zador}}}{\underline{G}_n^{\text{CS}}} = \frac{2 \log^2 n + O(\log n)}{n^2} = O\left(\frac{\log^2 n}{n^2}\right), \quad (180)$$

as claimed.

APPENDIX D

NORMALIZED p TH MOMENT

Let $p > 0$ be a real number. For a unit covolume lattice $L \subset \mathbb{R}^n$ and the ℓ_p norm $\|\cdot\|_p$ on $\mathbb{R}^n$, we define the p -Voronoi region as

$$\mathcal{V}_L^{(p)} \stackrel{\text{def}}{=} \{x \in \mathbb{R}^n : \|x\|_p \leq \|x - y\|_p, \forall y \in L \setminus \{0\}\}, \quad (181)$$

where ties are broken in a systematic manner, such that $\mathcal{V}_L^{(p)}$ is a fundamental cell of L . Let $\mathbb{T}_L \stackrel{\text{def}}{=} \mathbb{R}^n/L$ be the quotient torus, which is isomorphic to $\mathcal{V}_L^{(p)}$, and let m_L be the Haar probability measure on $\mathbb{T}_L$, and $\pi_L : \mathbb{R}^n \rightarrow \mathbb{T}_L$ be the quotient map.

Let $U_L^{(p)} = U_L \sim \text{Uniform}(\mathcal{V}_L^{(p)})$. We define the normalized p th moment of L as

$$G_L^{(p)} \stackrel{\text{def}}{=} \frac{\mathbb{E}(\|U_L\|_p^p)}{n} \quad (182)$$

Let

$$\mathcal{B}^{(p)} \stackrel{\text{def}}{=} \{x \in \mathbb{R}^n : \|x\|_p \leq 1\} \quad (183)$$

be the unit closed ball with respect to $\|\cdot\|_p$, and let $V_{p,n}$ be its volume. The main result of this section, is the following extension of Theorem II.5.

Theorem D.1. *Let n be an integer and $p > 0$, and $L \sim \mu_n$. We have that*

$$\mathbb{E}[G_L^{(p)}] \leq \frac{1}{nV_{p,n}^{p/n}} \cdot \frac{1}{\text{sinc}(p/n)}. \quad (184)$$

Proof. Fix a unit covolume lattice $L \subset \mathbb{R}^n$. Since $\|U_L\|_p$ is a non-negative random variable, we have that

$$\mathbb{E}\|U_L\|_p^p = \int_0^\infty \Pr(\|U_L\|_p^p > r) dr \quad (185)$$

$$= \int_0^\infty \Pr(\|U_L\|_p > r^{1/p}) dr. \quad (186)$$

We further have that

$$\Pr(\|U_L\|_p > r^{1/p}) = 1 - \Pr(\|U_L\|_p \leq r^{1/p}), \quad (187)$$

and that

$$\Pr(\|U_L\|_p \leq r^{1/p}) = |r^{1/p}\mathcal{B}^{(p)} \cap \mathcal{V}_L^{(p)}| = m_L(\pi_L(r^{1/p}\mathcal{B}^{(p)})), \quad (188)$$

where the justification of the last equality is similar to that of (16).

We have therefore obtained that

$$\mathbb{E}\|U_L\|_p^p = \int_0^\infty 1 - m_L(\pi_L(r^{1/p}\mathcal{B}^{(p)})) dr. \quad (189)$$

Now, further averaging with respect to $L \sim \mu_n$ and using Tonelli's Theorem, we get

$$\mathbb{E}\|U_L\|_p^p = \int_0^\infty 1 - \mathbb{E}[m_L(\pi_L(r^{1/p}\mathcal{B}^{(p)}))] dr. \quad (190)$$

Using (24) applied with $\mathcal{K} = r^{1/p}\mathcal{B}^{(p)}$, we have that

$$\mathbb{E}[m_L(\pi_L(r^{1/p}\mathcal{B}^{(p)}))] \geq \frac{|r^{1/p}\mathcal{B}^{(p)}|}{1 + |r^{1/p}\mathcal{B}^{(p)}|} = \frac{r^{n/p}V_{p,n}}{1 + r^{n/p}V_{p,n}}, \quad (191)$$

and therefore

$$\mathbb{E}\|U_L\|_p^p \leq \int_0^\infty \frac{1}{1 + (rV_{p,n}^{p/n})^{n/p}} dr \quad (192)$$

$$= \frac{1}{V_{p,n}^{p/n}} \int_0^\infty \frac{1}{1 + t^{n/p}} dt. \quad (193)$$

Finally, using (34) we have that for any $\nu > 0$,

$$\int_0^\infty \frac{1}{1 + t^\nu} dt = \frac{\pi/\nu}{\sin(\pi/\nu)} = \frac{1}{\text{sinc}(1/\nu)}, \quad (194)$$

and we obtain that

$$\mathbb{E}\|U_L\|_p^p \leq \frac{1}{V_{p,n}^{p/n}} \cdot \frac{1}{\text{sinc}(p/n)}, \quad (195)$$

establishing the claimed result. $\square$

To put this result in context, it is easy to see that for any unit covolume lattice $L \subset \mathbb{R}^n$ it holds that

$$G_L^{(p)} \geq G_{n,p}^* \stackrel{\text{def}}{=} \frac{1}{(n+p)V_{p,n}^{p/n}}. \quad (196)$$

This follows by setting $S = r_{\text{eff}}\mathcal{B}^{(p)}$, where $r_{\text{eff}} = \frac{1}{V_{p,n}^{1/n}}$ is chosen so that $|S| = 1 = |\mathcal{V}_L^{(p)}|$, and computing $\mathbb{E}\|U_S\|_p^p$ for $U_S \sim \text{Uniform}(S)$. Clearly, $\mathbb{E}\|U_L\|_p^p \geq \mathbb{E}\|U_S\|_p^p$, and $\mathbb{E}\|U_S\|_p^p$ can be computed as in (186), noting that

$$\Pr(\|U_S\|_p^p \geq r) = \begin{cases} 1 - r^{n/p}V_{p,n} & 0 \leq r \leq r_{\text{eff}}^p \\ 0 & r > r_{\text{eff}}^p \end{cases}. \quad (197)$$

The following is the analogue of Lemma II.6 for general $p > 0$.

Lemma D.2. *Let $p > 0$ and $n \geq 4p$ be an integer. Then, for $L \sim \mu_n$*

$$\Pr(G_L^{(p)} > (1 + \kappa)G_{n,p}^*) \leq \frac{2p}{\kappa n}. \quad (198)$$

Proof. Define the random variable $Y = \frac{G_L^{(p)}}{G_{n,p}^*} - 1$, which is non-negative with probability 1. By Markov's inequality, we have

$$\Pr(G_L^{(p)} \geq (1 + \kappa)G_{n,p}^*) = \Pr(Y \geq \kappa) \leq \frac{\mathbb{E}[Y]}{\kappa}. \quad (199)$$

Using $\sin(x) \geq x(1 - \frac{x^2}{6})$ for $0 < x < 1$, we have that for any $0 < x \leq \frac{1}{\pi}$ it holds that

$$\frac{1}{\text{sinc}(x)} \leq \frac{\pi x}{\pi x(1 - \frac{(\pi x)^2}{6})} \leq 1 + \frac{1}{5}(\pi x)^2 < 1 + 2x^2. \quad (200)$$

Applying Theorem D.1 we obtain (for $n \geq 4p$ such that $\frac{p}{n} < \frac{1}{\pi}$)

$$\mathbb{E}[Y] \leq \frac{n+p}{n} \frac{1}{\text{sinc}(p/n)} - 1 \quad (201)$$

$$\leq \left(1 + \frac{p}{n}\right) \left(1 + 2\left(\frac{p}{n}\right)^2\right) - 1 \quad (202)$$

$$= \frac{p}{n} + 2\frac{p^2}{n^2} + 2\frac{p^3}{n^3} < 2\frac{p}{n}, \quad (203)$$

which yields the claimed result. $\square$

APPENDIX E

PROOFS OF CLAIMS FOR LINEAR CODES

Proof of Proposition III.1. The first item follows since

$$r_{\text{pack}}(\mathcal{C}) = \max\{r : \mathcal{B}_{n,r} \subset \mathcal{V}_{\mathcal{C}}\} \quad (204)$$

$$= \max\{r : Q_{\mathcal{C}}(r) = 2^{k-n}V_{n,r}\}, \quad (205)$$

where in the second equality we have used (80). The second item follows since

$$r_{\text{cov}}(\mathcal{C}) = \max_{x \in \mathbb{F}_2^n} \min_{y \in \mathcal{C}} d_H(x, y) = \max_{x \in \mathcal{V}_{\mathcal{C}}} |x|. \quad (206)$$

For the third item, we write

$$\mathbb{E}|U_L| = \sum_{r=0}^n \Pr(|U_C| > r) \quad (207)$$

$$= \sum_{r=0}^n 1 - \Pr(|U_C| \leq r) \quad (208)$$

$$= \sum_{r=0}^n 1 - Q_C(r). \quad (209)$$

The fourth item follows directly from Proposition III.2. $\square$

Proof of Proposition III.2. Let $\varphi_p(r) = p^r(1-p)^{n-r}$, and not that $\varphi_p(r) - \varphi_p(r+1) = \varphi_p(r) \cdot \frac{1-2p}{1-p}$. We have

$$\Pr(Z \in \mathcal{K}) = \sum_{r=0}^n \Pr(Z \in (\mathcal{K} \cap \mathcal{S}_{n,r})) \quad (210)$$

$$= \sum_{r=0}^n \varphi_p(r) |\mathcal{K} \cap \mathcal{S}_{n,r}| \quad (211)$$

$$= \sum_{r=0}^n \varphi_p(r) (|\mathcal{K} \cap \mathcal{B}_{n,r}| - |\mathcal{K} \cap \mathcal{B}_{n,r-1}|) \quad (212)$$

$$= \varphi_p(n) |\mathcal{K} \cap \mathcal{B}_{n,n}| + \sum_{r=0}^{n-1} (\varphi_p(r) - \varphi_p(r+1)) |\mathcal{K} \cap \mathcal{B}_{n,r}| \quad (213)$$

$$= \left(\frac{p}{1-p} + \frac{1-2p}{1-p} \right) \varphi_p(n) |\mathcal{K} \cap \mathcal{B}_{n,n}| \quad (214)$$

$$+ \frac{1-2p}{1-p} \sum_{r=0}^{n-1} \varphi_p(r) |\mathcal{K} \cap \mathcal{B}_{n,r}| \quad (215)$$

$$= |\mathcal{K}| \cdot \frac{p}{1-p} \cdot p^n + \frac{1-2p}{1-p} \sum_{r=0}^n \varphi_p(r) |\mathcal{K} \cap \mathcal{B}_{n,r}| \quad (216)$$

$$= |\mathcal{K}| \cdot \frac{p}{1-p} \cdot p^n \quad (217)$$

$$+ |\mathcal{K}| \cdot \frac{1-2p}{1-p} \sum_{r=0}^n \binom{n}{r} p^r (1-p)^{n-r} \frac{|\mathcal{K} \cap \mathcal{B}_{n,r}|}{\binom{n}{r}} \quad (218)$$

$$= |\mathcal{K}| \left(\frac{p}{1-p} \cdot p^n + \frac{1-2p}{1-p} \sum_{r=0}^n \binom{n}{r} p^r (1-p)^{n-r} \frac{Q_C(r)}{\binom{n}{r}} \right) \quad (219)$$

$$= |\mathcal{K}| \left(\frac{p}{1-p} \cdot p^n + \frac{1-2p}{1-p} \mathbb{E} \left[\frac{Q_C(|Z|)}{\binom{n}{|Z|}} \right] \right), \quad (220)$$

as claimed. $\square$

Proof of Theorem III.5. Let $m < n/2 - 1$ be a positive integer, and denote

$$\beta_m = \frac{n-m}{m+1} > 1. \quad (221)$$

We claim that

$$\gamma_r = \frac{\binom{n}{r+1}}{V_{n,r}} \geq \beta_m - 1, \quad \forall 0 \leq r \leq m. \quad (222)$$

We show this by induction. For $r = 0$, we have $\gamma_0 = n > \beta_m - 1$. Assume $\gamma_\ell > \beta_m - 1$ for all $0 \leq \ell \leq r-1 < m$. We have that

$$\begin{aligned} \gamma_r &= \frac{\binom{n}{r+1}}{V_{n,r}} = \frac{\binom{n}{r+1}}{\binom{n}{r} + V_{n,r-1}} = \frac{\binom{n}{r+1}}{\binom{n}{r} \left(1 + \frac{1}{\gamma_{r-1}}\right)} \\ &= \frac{n-r}{r+1} \frac{\gamma_{r-1}}{1 + \gamma_{r-1}} \geq \beta_m \cdot \frac{\gamma_{r-1}}{1 + \gamma_{r-1}} \geq 1 - \beta_m, \end{aligned} \quad (223)$$

where the last inequality follows since $t \mapsto \frac{t}{1+t}$ is monotonically increasing, and the induction assumption that $\gamma_{r-1} > 1 - \beta_m$.

Using (220), we have that

$$\frac{x_{r+1}}{x_r} = \frac{V_{n,r+1}}{V_{n,r}} \quad (224)$$

$$= 1 + \frac{\binom{n}{r+1}}{V_{n,r}} \quad (225)$$

$$= 1 + \gamma_r \quad (226)$$

$$\geq \beta_m, \quad \forall 0 < r \leq m. \quad (227)$$

By (108), for any $r_{\text{eff}}(n, k) < m < n/2 - 1$ we can write

$$\Delta(n, k) \stackrel{\text{def}}{=} S_1 + S_{2a} + S_{2b}, \quad (228)$$

where

$$S_1 = \sum_{r=0}^{r_{\text{eff}}(n,k)-1} \frac{x_r^2}{1+x_r} \leq \sum_{r=0}^{r_{\text{eff}}(n,k)-1} x_r \quad (229)$$

$$S_{2a} = \sum_{r=r_{\text{eff}}(n,k)}^m \frac{1}{1+x_r} \leq \sum_{r=r_{\text{eff}}(n,k)}^m x_r^{-1} \quad (230)$$

$$S_{2b} = \sum_{r=1+m}^n \frac{1}{1+x_r} \leq n \cdot x_m^{-1}. \quad (231)$$

Note that by definition of $r_{\text{eff}}(n, k)$, we have that $x_r < 1$ for all $r \leq r_{\text{eff}}(n, k) - 1$, and that $x_r \geq 1$ for all $r \geq r_{\text{eff}}(n, k)$. By (225) we therefore have

$$x_r \leq \beta_m^{-(r_{\text{eff}}(n,k)-1-r)}, \quad \forall 0 \leq r \leq r_{\text{eff}}(n, k) - 1, \quad (232)$$

$$x_r^{-1} \leq \beta_m^{-(r-r_{\text{eff}}(n,k))}, \quad \forall r_{\text{eff}}(n, k) \leq r \leq m. \quad (233)$$

It therefore follows that

$$\begin{aligned} S_1 &\leq \sum_{r=0}^{r_{\text{eff}}(n,k)-1} x_r \leq \sum_{r=0}^{r_{\text{eff}}(n,k)-1} \beta_m^{-(r_{\text{eff}}(n,k)-r)} < \sum_{j=0}^{\infty} \beta_m^{-j} \\ &= \frac{1}{1 - \beta_m^{-1}} \end{aligned} \quad (234)$$

$$\begin{aligned} S_{2a} &\leq \sum_{r=r_{\text{eff}}(n,k)}^m x_r^{-1} \leq \sum_{r=r_{\text{eff}}(n,k)}^m \beta_m^{-(r-r_{\text{eff}}(n,k))} < \sum_{j=1}^{\infty} \beta_m^{-j} \\ &\leq \frac{1}{1 - \beta_m^{-1}}. \end{aligned} \quad (235)$$

Thus,

$$\Delta(n, k) \leq 2 \frac{\beta_m}{\beta_m - 1} + n \cdot \beta_m^{-(m-r_{\text{eff}}(n,k))}. \quad (236)$$

Take $m = \lceil \frac{n}{2} (h_2^{-1}(1-\alpha) + \frac{1}{2}) \rceil$, where $h_2(p) = -p \log_2(p) - (1-p) \log_2(1-p)$, and $h_2^{-1}(\cdot)$ is its inverse

restricted to $[0, 1/2]$. We may assume without loss of generality that n is large enough such that $\kappa \stackrel{\text{def}}{=} \frac{m+1}{n} < 1/2$, so that $\beta_m \geq \frac{1-\kappa}{\kappa} > 1$, and $m - r_{\text{eff}}(n, k) > \left\lceil \frac{\log n}{\log \beta_m} \right\rceil$. Substituting this into (234), we obtain

$$\Delta(n, k) \leq 2 \frac{1-\kappa}{1-2\kappa} + 1, \quad (235)$$

as claimed. $\square$

Proof of Lemma III.8. Let $X \sim \text{Ber}^{\otimes n}(1/2)$ and let $\mathcal{C} = \{c_1, \dots, c_{2^k}\} \subset \{0, 1\}^n$ be the codebook corresponding to the image of the decoder $g(\cdot)$. Define the random variable

$$Y = d_H(X, \mathcal{C}) = \min_{c \in \mathcal{C}} d_H(X, c). \quad (236)$$

Since given $\mathcal{C}$ the optimal encoder f maps each X to the nearest point in $\mathcal{C}$, we have that the average distortion of the code is at least

$$D = \mathbb{E}[Y] = \sum_{y=0}^n \Pr(Y > y) = \sum_{y=0}^n 1 - \Pr(Y \leq y). \quad (237)$$

Let

$$\mathcal{A}_y = \{x \in \mathbb{F}_2^n : d(x, \mathcal{C}) \leq y\}. \quad (238)$$

We clearly have that $\mathcal{A}_y \subset \cup_{c \in \mathcal{C}} \{c + B_{n,y}\}$, and therefore $|\mathcal{A}_y| \leq \min\{|\mathcal{C}| \cdot V_{n,y}, 2^n\}$, and consequently,

$$\Pr(Y \leq y) = \Pr(X \in \mathcal{A}_y) = 2^{-n} |\mathcal{A}_y| \leq \min\{2^{k-n} V_{n,y}, 1\}. \quad (239)$$

Substituting this into (237), and recalling (106), yields the claimed result. $\square$

REFERENCES

- [1] R. Zamir and M. Feder, "On lattice quantization noise," *IEEE Transactions on Information Theory*, vol. 42, no. 4, pp. 1152–1159, 1996.
- [2] H. S. M. Coxeter, L. Few, and C. A. Rogers, "Covering space with equal spheres," *Mathematika*, vol. 6, pp. 147–157, 1959. [Online]. Available: <https://doi.org/10.1112/S0025579300002059>
- [3] E. Agrell and B. Allen, "On the best lattice quantizers," *IEEE Transactions on Information Theory*, vol. 69, no. 12, pp. 7650–7658, 2023.
- [4] P. Zador, "Asymptotic quantization error of continuous signals and the quantization dimension," *IEEE Transactions on Information Theory*, vol. 28, no. 2, pp. 139–149, 1982.
- [5] J. Conway and N. Sloane, "A lower bound on the average error of vector quantizers (corresp.)," *IEEE Transactions on Information Theory*, vol. 31, no. 1, pp. 106–109, 1985.
- [6] A. Gersho, "Asymptotically optimal block quantization," *IEEE Transactions on information theory*, vol. 25, no. 4, pp. 373–380, 1979.
- [7] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 409–417, 1994.
- [8] A. Ingber, R. Zamir, and M. Feder, "Finite-dimensional infinite constellations," *IEEE transactions on information theory*, vol. 59, no. 3, pp. 1630–1656, 2012.
- [9] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Transactions on Information Theory*, vol. 40, no. 4, pp. 1284–1292, 1994.
- [10] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2307–2359, 2010.
- [11] O. Ordentlich, O. Regev, and B. Weiss, "Bounds on the density of smooth lattice coverings," *Journal d'Analyse Mathématique*, pp. 1–26, 2025.
- [12] C. L. Siegel, "A mean value theorem in geometry of numbers," *Ann. of Math. (2)*, vol. 46, pp. 340–347, 1945.
- [13] F. A. Hamprecht, E. Agrell, and J. Cawse, "Exploring a space of materials: Spatial sampling design and subset selection," in *Experimental Design for Combinatorial and High Throughput Materials Development*. Wiley New York, NY, USA, 2003.
- [14] S. Torquato, B. Lu, and J. Rubinstein, "Nearest-neighbor distribution functions in many-body systems," *Physical Review A*, vol. 41, no. 4, p. 2059, 1990.
- [15] S. Torquato, "Reformulation of the covering and quantizer problems as ground states of interacting particles," *Physical Review E—Statistical, Nonlinear, and Soft Matter Physics*, vol. 82, no. 5, p. 056109, 2010.
- [16] S. Torquato and F. Stillinger, "Exactly solvable disordered sphere-packing model in arbitrary-dimensional euclidean spaces," *Physical Review E—Statistical, Nonlinear, and Soft Matter Physics*, vol. 73, no. 3, p. 031106, 2006.
- [17] I. Haviv, V. Lyubashevsky, and O. Regev, "A note on the distribution of the distance from a lattice," *Discrete & Computational Geometry*, vol. 41, no. 1, pp. 162–176, 2009.
- [18] R. Zamir, *Lattice Coding for Signals and Networks*. Cambridge: Cambridge University Press, 2014.
- [19] L. Fejes Toth, "Sur la représentation d'une population infinie par un nombre fini d'éléments," *Acta Mathematica Hungarica*, vol. 10, no. 3–4, pp. 299–304, 1959.
- [20] J. Conway and N. Sloane, "Voronoi regions of lattices, second moments of polytopes, and quantization," *IEEE Transactions on Information Theory*, vol. 28, no. 2, pp. 211–226, 1982.
- [21] E. Barnes and N. Sloane, "The optimal lattice quantizer in three dimensions," *SIAM Journal on Algebraic Discrete Methods*, vol. 4, no. 1, pp. 30–41, 1983.
- [22] J. H. Conway and N. J. Sloane, "On the Voronoi regions of certain lattices," *SIAM Journal on Algebraic Discrete Methods*, vol. 5, no. 3, pp. 294–305, 1984.
- [23] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., ser. Grundlehren der mathematischen Wissenschaften. New York: Springer-Verlag, 1999, vol. 290.
- [24] E. Agrell and T. Eriksson, "Optimization of lattices for quantization," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1814–1828, 1998.
- [25] S. Lyu, Z. Wang, C. Ling, and H. Chen, "Better lattice quantizers constructed from complex integers," *IEEE Transactions on Communications*, vol. 70, no. 12, pp. 7932–7940, 2022.
- [26] C. W. Ling and C. T. Li, "Rejection-sampled universal quantization for smaller quantization errors," *arXiv preprint arXiv:2402.03030*, 2024.
- [27] E. Agrell, D. Pook-Kolb, and B. Allen, "Glued lattices are better quantizers than K_{12} ," *IEEE Transactions on Information Theory*, 2024.
- [28] D. Pook-Kolb, E. Agrell, and B. Allen, "Parametric lattices are better quantizers in dimensions 13 and 14," *arXiv preprint arXiv:2411.19250*, 2024.
- [29] E. Agrell, D. Pook-Kolb, and B. Allen, "Optimization and identification of lattice quantizers," *IEEE Transactions on Information Theory*, 2025.
- [30] P. Autissier, "Un lemme matriciel effectif," *Mathematische Zeitschrift*, vol. 273, pp. 355–361, 2013.
- [31] A. Magazinov, "A proof of a conjecture by Haviv, Lyubashevsky and Regev on the second moment of a lattice Voronoi cell," *Advances in Geometry*, vol. 20, no. 1, pp. 117–120, 2020.
- [32] C. A. Rogers, "Lattice coverings of space," *Mathematika*, vol. 6, pp. 33–39, 1959. [Online]. Available: <https://doi.org/10.1112/S002557930000190X>
- [33] I. F. Blake, "The Leech lattice as a code for the Gaussian channel," *Information and control*, vol. 19, no. 1, pp. 66–74, 1971.
- [34] R. de Buda, "The upper error bound of a new near-optimal code," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 441–445, 1975. [Online]. Available: <https://doi.org/10.1109/tit.1975.1055409>
- [35] J. Conway and N. Sloane, "A fast encoding method for lattice codes and quantizers," *IEEE Transactions on Information Theory*, vol. 29, no. 6, pp. 820–824, 1983.
- [36] G. D. Forney, "Coset codes. i. introduction and geometrical classification," *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1123–1151, 1988.
- [37] —, "Coset codes. ii. binary lattices and related codes," *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1152–1187, 1988.
- [38] G. Forney, "Multidimensional constellations. ii. Voronoi constellations," *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 6, pp. 941–958, 1989.
- [39] H.-A. Loeliger, "Averaging bounds for lattices and linear codes," *IEEE Trans. Inform. Theory*, vol. 43, no. 6, pp. 1767–1773, 1997. [Online]. Available: <https://doi.org/10.1109/18.641543>

- [40] R. Urbanke and B. Rimoldi, "Lattice codes can achieve capacity on the AWGN channel," *IEEE transactions on Information Theory*, vol. 44, no. 1, pp. 273–278, 1998.
- [41] T. Linder, C. Schlegel, and K. Zeger, "Corrected proof of de buda's theorem (lattice channel codes)," *IEEE transactions on information theory*, vol. 39, no. 5, pp. 1735–1737, 2002.
- [42] U. Erez and R. Zamir, "Achieving $1/2 \log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2293–2314, 2004.
- [43] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. Inform. Theory*, vol. 51, no. 10, pp. 3401–3416, 2005. [Online]. Available: <https://doi.org/10.1109/TIT.2005.855591>
- [44] C. Swannack, U. Erez, and G. W. Wornell, "Reflecting on the awgn error exponent," in *43rd Annual Allerton Conference on Communication, Control, and Computing*, Allerton House, Monticello, Illinois, 2005.
- [45] T. Liu, P. Moulin, and R. Koetter, "On error exponents of modulo lattice additive noise channels," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 454–471, 2006.
- [46] O. Ordentlich and U. Erez, "A simple proof for the existence of "good" pairs of nested lattices," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4439–4453, 2016.
- [47] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1250–1276, 2002.
- [48] Y. Kochman and R. Zamir, "Joint Wyner–Ziv/dirty-paper coding by modulo-lattice modulation," *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 4878–4889, 2009.
- [49] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463–6486, 2011.
- [50] O. Ordentlich, U. Erez, and B. Nazer, "The approximate sum capacity of the symmetric Gaussian k -user interference channel," *IEEE Transactions on Information Theory*, vol. 60, no. 6, pp. 3450–3482, 2014.
- [51] A. Ingber and R. Zamir, "Expurgated infinite constellations at finite dimensions," in *2012 IEEE International Symposium on Information Theory Proceedings*, 2012, pp. 130–134.
- [52] V. Anantharam and F. Baccelli, "Capacity and error exponents of stationary point processes under random additive displacements," *Advances in Applied Probability*, vol. 47, no. 1, pp. 1–26, 2015.
- [53] T. J. Goblick, "Coding for a discrete information source with a distortion measure," Ph.D. dissertation, Massachusetts Institute of Technology, 1963.
- [54] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes*. Elsevier, 1997, vol. 54.
- [55] A. Viterbi and J. Omura, "Trellis encoding of memoryless discrete-time sources with a fidelity criterion," *IEEE Transactions on Information Theory*, vol. 20, no. 3, pp. 325–332, 1974.
- [56] Y. Matsunaga and H. Yamamoto, "A coding theorem for lossy data compression by ldpc codes," *IEEE Transactions on Information Theory*, vol. 49, no. 9, pp. 2225–2229, 2003.
- [57] M. J. Wainwright, E. Maneva, and E. Martinian, "Lossy source compression using low-density generator matrix codes: Analysis and algorithms," *IEEE Transactions on Information theory*, vol. 56, no. 3, pp. 1351–1368, 2010.
- [58] S. B. Korada and R. L. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Transactions on Information Theory*, vol. 56, no. 4, pp. 1751–1768, 2010.
- [59] A. Mazumdar, V. Chandar, and G. W. Wornell, "Local recovery in data compression for general sources," in *2015 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2015, pp. 2984–2988.
- [60] R. G. Gallager, *Information theory and reliable communication*. Springer, 1968, vol. 588.
- [61] A. Barg and G. D. Forney, "Random codes: Minimum distances and error exponents," *IEEE Transactions on Information Theory*, vol. 48, no. 9, pp. 2568–2573, 2002.
- [62] I. Sason and S. Shamai, "Performance analysis of linear codes under maximum-likelihood decoding: A tutorial," *Foundations and Trends® in Communications and Information Theory*, vol. 3, no. 1–2, pp. 1–222, 2006.
- [63] B. Allen, "Performance of random template banks," *Physical Review D*, vol. 105, no. 10, p. 102003, 2022.
- [64] C. A. Rogers, "Lattice covering of space: The Minkowski-Hlawka theorem," *Proc. London Math. Soc. (3)*, vol. 8, pp. 447–465, 1958. [Online]. Available: <https://doi.org/10.1112/plms/s3-8.3.447>
- [65] W. M. Schmidt, "The measure of the set of admissible lattices," *Proc. Amer. Math. Soc.*, vol. 9, pp. 390–403, 1958. [Online]. Available: <https://doi.org/10.2307/2032994>
- [66] O. Ordentlich, O. Regev, and B. Weiss, "New bounds on the density of lattice coverings," *Journal of the American Mathematical Society*, vol. 35, no. 1, pp. 295–308, 2022.
- [67] A. Strömbergsson, "On the probability of a random lattice avoiding a large convex set," *Proc. Lond. Math. Soc. (3)*, vol. 103, no. 6, pp. 950–1006, 2011. [Online]. Available: <https://doi.org/10.1112/plms/pdr021>
- [68] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2007.
- [69] C. A. Rogers, "The packing of equal spheres," *Proceedings of the London Mathematical Society*, vol. 3, no. 4, pp. 609–620, 1958.
- [70] C. Rogers, "An asymptotic expansion for certain schläfli functions," *Journal of the London Mathematical Society*, vol. 1, no. 1, pp. 78–80, 1961.
- [71] A. A. Shoom, "Computation of the Schläfli function," *IEEE Transactions on Information Theory*, vol. 71, no. 2, pp. 1481–1486, 2025.
- [72] E. Agrell, *Personal communication*, 2025.
- [73] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 2012.
- [74] Y. Polyanskiy and Y. Wu, *Information theory: From coding to learning*. Cambridge university press, 2025.
- [75] Z. Zhang, E.-h. Yang, and V. Wei, "The redundancy of source coding with a fidelity criterion. 1. known statistics," *IEEE Transactions on Information Theory*, vol. 43, no. 1, pp. 71–91, 1997.
- [76] V. Kostina and S. Verdú, "Nonasymptotic noisy lossy source coding," *IEEE Transactions on Information Theory*, vol. 62, no. 11, pp. 6111–6123, 2016.
- [77] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*. Courier Corporation, 1965, vol. 55.
- [78] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, 2nd ed. Reading, MA: Addison-Wesley, 1994.