# 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 $\ell_2$-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 quite close to a trivial ball-based lower bound and immediately translate to improved 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 improved upper bounds on the Hamming distortion and the error probability of a random linear code over the binary symmetric channel.

## 1. 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 $\mathrm{covol}(L) \neq 1$, one further normalizes by $(\mathrm{covol}(L))^{2/n}$). The NSM is trivially lower

*Date*: June 24, 2025.

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 $\mu_n$, 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 2.5, and an extension for the $p$th moment of a lattice is proved in Theorem C.1. In particular, Theorem 2.5 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 2.6). Prior to this work, the tightest upper bound on the NSM of the "best" lattice in $\mathbb{R}^n$ was $1 + O(\frac{\log n}{n})$ [ZF96]. 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 $\Omega(n)$ [CFR59], this technique is inherently limited, and cannot yield bounds better than $1+O(\frac{\log n}{n})$. We note that not only does Theorem 2.5 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 $n \geq 36$ it attains tighter upper bounds on the NSM than the best known ones, as reported in [AA23].

Furthermore, a canonical upper bound on the NSM of the "best" infinite constellation with a given point density was derived by Zador [Zad82]. To date, it was not known whether or not this bound can be attained by lattices. In Theorem 2.7 we show that for large $n$ there are lattices attaining Zador's upper bound. This can be seen as an evidence that lattice quantizers are as good as any other quantizer, as is essentially postulated in Gersho's conjecture [Ger79].

- The error probability $P_{e,\sigma^2}(L)$ of a lattice $L$ at noise level $\sigma^2$ is defined as the probability that a Gaussian iid noise with zero mean and variance $\sigma^2$ falls outside of the Voronoi cell of $L$. In Theorem 2.8 we prove a novel upper bound on the expected error probability of a random lattice (drawn from $\mu_n$). This bound is numerically shown to be similar to the best known previous upper bound due to [Pol94b, IZF12], 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 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 3.8). In Theorem 3.5 we show that for a random linear code of dimension $k$, the expected Hamming distortion exceeds this lower bound only by a 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 3.11 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 [Pol94a] and Polyanskiy-Poor-Verdú [PPV10].

1.1. **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 $\ell_2$-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 [ORW25, 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

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

By Siegel's summation formula (Minkowski-Hlawka Theorem) [Sie45], we have that if $L$ is drawn from the natural probability distribution $\mu_n$ on the space of unit covolume lattices in $\mathbb{R}^n$, then

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

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.

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.

1.2. **Related work.** 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 [Zam14]. Consequently, characterizing/approximating the optimal NSM $G_n$ at any dimension $n$ is a topic that received considerable attention [FT59, CS82, BS83, CS84, CS85, CS88, ZF96, AE98, LWLC22, AA23, LL24, APKA24, PKAA24, APKA25]. 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 [Rog59], Zamir and Feder [ZF96] deduced 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 optimal normalized second moment $G_n$ is also related to the quantity $b_{2,n}$ defined by Zador [Zad82], which quantifies the "quantization efficiency" [Ger79, Zam14]. 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 $a \to \infty$. 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 [Zad82, Lemma 5]. The resulting quantizer is not a lattice, and to date it was not known if lattices can achieve this upper bound. Our Theorem 2.4 shows that for large $n$ there are indeed lattices that achieve Zador's bound. In fact, a well-known conjecture due

[1] In fact, the 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 [HLR09] and proved in [Mag20].

to Gersho [Ger79] 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 2.4 is perhaps another evidence for the validity of this conjecture. We note that our analysis of $G_n$ involves studying the distribution of the distance between $X \sim \text{Uniform}([-a,a)^n)$ for large $n$, and a lattice $L \subset \mathbb{R}^n$, as characterized by the Voronoi spherical CDF $g_L(r)$. A related random variable was studied in [HLR09], where the distance to the lattice was normalized by the covering radius, such that the normalized value is in $[0,1]$.

The application of lattices as codebooks for reliable communication over the AWGN channel has a rich history, dating back to Blake [Bla71], de Buda [dB75], Conway and Sloane [CS83] and continuing with [For88a, For88b, For89, Pol94b, Loe97, UR98, LSZ02, EZ04, ELZ05, IZF12, OE16], as well as many other works. See also, e.g., [ZSE02, KZ09, NG11, OEN14] and [Zam14, 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 $\mathcal{S} \subset \mathbb{R}^n$ (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 [Pol94b] 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 [Pol94b], and later an equivalent bound was derived in simpler form in [IZF12]. It was shown in [IZF12] that for $\sigma^2$ 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 [Zam14, Chapter 13] for a comprehensive analysis of the error probability of a random lattice. In Theorem 2.8 we prove a different upper bound on the expected error probability of a random lattice. This bound is close to the bound given in [IZF12], 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 [AB15].

The Hamming distortion of linear codes in $\mathbb{F}_2^n$ was first studied by Goblick [Gob63], who proved that such codes can asymptotically attain Shannon's rate-distortion function for a symmetric binary source under

Hamming distortion. In fact, Goblick'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 3, 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 [CHLL97]. 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 by the ball lower bound only by a constant.

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., [Gal68, Pol94a, BF02, PPV10] 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 [SS06, Chapter 1], the new upper bound we derive in Theorem 3.11 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 [Pol94a], which is also equivalent to the RCU bound of [PPV10]. Near capacity our new bound is numerically shown to be tighter than those bounds.

1.3. **Paper structure.** All results regarding lattices are developed in Section 2, whereas all results regarding linear codes are developed in Section 3. 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 2 (or only Section 3).

1.4. **Acknowledgments.** The author is grateful to Uri Erez, Bo'az Klartag, Yury Polyanskiy, Oded Regev and Barak Weiss for many useful discussions. This work was supported by ISF 1641/21.

## 2. Lattices

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

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

where $\|x\|_2 = (\sum_{i=1}^n x_i^2)^{1/2}$ is the $\ell_2$ 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

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

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

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

and its volume is

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

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

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

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

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

where the last equality follows since $L$ has unit covolume.

**Proposition 2.1.** *Let $L \subset \mathbb{R}^n$ be a unit covolume lattice in $\mathbb{R}^n$. Then*

*(1) The packing radius of $L$ is*

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

*(2) The covering radius of $L$ is*

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

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

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

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

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

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

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

**Proposition 2.2.** *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*

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

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

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

*Then*

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

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

2.1. **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

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

is the CDF function for the norm of a random variable uniformly distributed over the Euclidean ball of radius $r_{\text{eff}}$ (such that its volume is the same as that of $\mathcal{V}_L$). Thus, the Euclidean ball provides "inexistence" bounds for the 4 quantities above. Our goal in this paper is

to develop new "existence" bounds for $G_L$ and $P_{e,\sigma^2}$. To that end, we find a CDF $\underline{g}(r)$ for which

$$\mathbb{E}[g_L] \succeq \underline{g}, \tag{15}$$

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 $\pi_L : \mathbb{R}^n \to \mathbb{T}_L$ 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 $Q_L : \mathbb{R}^n \to L$ maps each point in $\mathbb{R}^n$ to $y \in L$, such that $x \in y + \mathcal{V}_L$. Let $m_L : \mathbb{T}_L \to [0,1]$ 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

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

where the last equality holds since, when we identify $\mathcal{V}_L$ with $\mathbb{T}_L$, it holds that $\|\pi_L(x)\|_2 \le \|x\|_2$ 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 [Rog58] and Schmidt [Sch58] in the middle of the previous century up to the recent progress in [ORW22, ORW25]. 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 $\mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$, via the map

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

This identification endows $\mathcal{L}_n$ with a natural probability measure; namely, there is a unique $\mathrm{SL}_n(\mathbb{R})$-invariant Borel probability measure on $\mathcal{L}_n$. Following [ORW22], we will refer to this measure as the *Haar-Siegel measure* and denote it by $\mu_n$. Due to its $\mathrm{SL}_n(\mathbb{R})$-invariance, the measure $\mu_n$ is referred to as the natural measure on the space of lattices in the literature.

**Theorem 2.3.** *For $L \sim \mu_n$ we have*

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

Using the characterization (16), the proof of Theorem 2.3 is an immediate consequence of the derivation in [ORW25, 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 [ORW25, Proof of Proposition 3.6] below.

*Proof of Theorem 2.3.* Observe that for any compact set $\mathcal{K} \subset \mathbb{R}^n$ it holds that

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

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

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

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

$$= \int_{x\in\mathcal{K}} \mathbb{E}\left[\frac{1}{1+|(L\setminus\{0\})\cap(\mathcal{K}-x)|}\right]dx \tag{21}$$

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

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

$$= \frac{|\mathcal{K}|}{1+|\mathcal{K}|}, \tag{24}$$

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

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

as claimed. □

While $\underline{g}_{\text{Jensen}}(r)$ is quite close to $g_{\mathcal{B}}(r)$ 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 $1/|\mathcal{K}|$ [Str11]. On the other hand, recent work [ORW22] showed that the covering radius of a random lattice $L \sim \mu_n$ is $\left(1 + O\left(\frac{\log n}{n}\right)\right) r_{\text{eff}}$ 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 $\mu_n$ on the event that $r_{\text{cov}}(L)$ is small.

In particular, let

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

and define the event

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

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

$$\tilde{\mu}_n \stackrel{\text{def}}{=} \mu_{n|\mathcal{E}_\eta}. \tag{28}$$

Relying on classic results by Rogers [Rog58] and Schmidt [Sch58] and the more recent result [ORW22] on the covering density of a random lattice, we prove the following in Appendix B.

**Theorem 2.4.** *Assume $n \geq 13$, and define $\eta$ 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*

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

$$\geq 1 - \left(e^{-(r/r_{\text{eff}})^n} + 24e^{-\frac{\eta}{2}}\right) \mathbb{1}\left\{ \left(\frac{r}{r_{\text{eff}}}\right)^n < 4n^2\eta \right\}$$

We note that Theorem 2.4 above is the only result in this paper that requires further tools beyond the first moment method.

2.2. **Bounds on the NSM.** We derive two lower bounds on $\mathbb{E}[G_L]$: one for $L \sim \mu_n$ and one for $L \sim \tilde{\mu}_n$.

**Theorem 2.5.** *Let $n$ be an integer and and $L \sim \mu_n$. We have that*

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

*where*

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

Note that for $36 \leq n \leq 48$ this upper bound is smaller than the best known NSM as reported in [AA23, Table 1].

*Proof.* Using Proposition 2.1 part 3, together with Theorem 2.3, we have (using Tonelli's Theorem)

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

$$\leq \int_0^\infty \frac{1}{1 + \left(\frac{r}{{r_{\text{eff}}}^2}\right)^{\frac{n}{2}}} dr \tag{32}$$

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

Finally, recalling that [GR07, Section 3.241] for any $\nu > 0$,

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

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

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

and the claimed result follows. □

It is well-known [CS88] that among all bodies in $\mathbb{R}^n$ of unit volume, the second moment is minimized by $r_{\text{eff}}\mathcal{B}$, and

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

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 2.6.** *Assume $n \geq 8$ and let $L \sim \mu_n$. Then for any $\kappa > 0$*

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

*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

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

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

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

Applying Theorem 2.5 we obtain (for $n \geq 8$, such that $\frac{2}{n} \leq \frac{1}{\pi}$)

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

which yields the claimed result. □

The normalized second moment characterizes the expected squared $\ell_2$ 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 $\ell_p$ distance between $X$ and $L$. In Appendix C we provide the precise definition and extend Theorem 2.5 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 2.7.** *Let $n \geq 13$ be an integer, and $L \sim \tilde{\mu}_n$. We have that*

$$\mathbb{E}[G_L] \leq \frac{1}{nV_n^{\frac{2}{n}}}\left(\Gamma\left(1+\frac{2}{n}\right)\cdot\frac{\gamma\left(\frac{2}{n},\frac{\eta}{2}\right)}{\Gamma\left(\frac{2}{n}\right)} + 60ne^{-\frac{\eta}{2}}\right) \tag{41}$$

*where $\eta$ is defined in* (26)*, $\gamma(\cdot,\cdot)$ is the lower incomplete gamma function, and $\Gamma(\cdot)$ is the Gamma function.*

Note that as $n$ grows, our upper bound above approaches the well-known Zador [Zad82, Lemma 5] upper bound on the smallest MSE a unit-density quantizer can achieve. In particular, Zador's upper bound shows that there exists an infinite constellation $\mathcal{C} \subset \mathbb{R}^n$ with unit density, whose second moment is at most $\frac{1}{nV_n^{\frac{2}{n}}}\Gamma\left(1+\frac{2}{n}\right)$. 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.

*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 2.1 part 3, together with Theorem 2.4, we have (using Tonelli's Theorem)

$$n\mathbb{E}[G_L] = \int_0^\infty \mathbb{E}[1 - g_L(\sqrt{r})]dr \tag{42}$$

$$\leq \int_0^{r_1} e^{-\left(\frac{r}{{r_{\text{eff}}}^2}\right)^{\frac{n}{2}}} + 23 \cdot e^{-\eta/2}dr + \int_{r_1}^{r_2} 24 \cdot e^{-\eta/2}dr \tag{43}$$

$$\leq 24r_2e^{-\eta/2} + \int_0^{r_1} e^{-\left(\frac{r}{{r_{\text{eff}}}^2}\right)^{\frac{n}{2}}} dr. \tag{44}$$

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

$$\int_0^{r_1} e^{-\left(\frac{r}{{r_{\text{eff}}}^2}\right)^{\frac{n}{2}}} dr = \int_0^{r_1} e^{-cr^{\frac{n}{2}}} dr = \frac{2}{nc^{2/n}} \int_0^{cr_1^{n/2}} u^{\frac{2}{n}-1}e^{-u}du \tag{45}$$

$$= {r_{\text{eff}}}^2 \cdot \frac{2}{n} \cdot \gamma\left(\frac{2}{n}, \left(\frac{r_1}{{r_{\text{eff}}}^2}\right)^{\frac{n}{2}}\right) \tag{46}$$

$$= {r_{\text{eff}}}^2 \cdot \frac{2}{n} \cdot \gamma\left(\frac{2}{n}, \frac{\eta}{2}\right). \tag{47}$$

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

$$\int_0^{r_1} e^{-\left(\frac{r}{{r_{\text{eff}}}^2}\right)^{\frac{n}{2}}} dr = V_n^{-\frac{2}{n}}\Gamma\left(1 + \frac{2}{n}\right) \cdot \frac{\gamma\left(\frac{2}{n}, \frac{\eta}{2}\right)}{\Gamma\left(\frac{2}{n}\right)}. \tag{48}$$

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

$$24r_2 \leq 24\left(4n^2\eta\right)^{\frac{2}{n}} {r_{\text{eff}}}^2 \leq 60{r_{\text{eff}}}^2 = 60V_n^{-\frac{2}{n}}, \quad \forall n \geq 13. \tag{49}$$

This establishes our claimed result. □

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

$$P_e(L, \sigma^2) = \Pr(\sigma Z \notin \mathcal{V}_L) = 1 - \Pr(\sigma Z \in \mathcal{V}_L) = 1 - \mu_{\sigma^2}(\mathcal{V}_L). \tag{50}$$

Clearly,

$$\mu_{\sigma^2}(\mathcal{V}_L) \leq \mu_{\sigma^2}(r_{\text{eff}}\mathcal{B}), \tag{51}$$

and similarly

$$P_e(L, \sigma^2) \geq P^{\text{SP}}(\sigma^2) \stackrel{\text{def}}{=} 1 - \mu_{\sigma^2}(r_{\text{eff}}\mathcal{B}). \tag{52}$$

We prove the following.

**Theorem 2.8.** *Let $n$ be an integer, let $W \sim \chi^2_{n+2}$ be a chi-squared random variable with $n+2$ degrees of freedom, and let*

$$X_W \stackrel{\text{def}}{=} \left( \frac{\sqrt{\sigma^2 W}}{r_{\text{eff}}} \right)^n . \tag{53}$$

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

$$\mathbb{E}_{\mu_n}[P_e(L,\sigma^2)] \le P^{\text{SP}}(\sigma^2) + \mathbb{E}\left[ \frac{\min\{X_W, X_W^{-1}\}}{1+X_W} \right]. \tag{54}$$

*Proof.* By Proposition 2.2, for any unit-covolume $L \subset \mathbb{R}^n$ we have that

$$\Delta(L,\sigma^2) \stackrel{\text{def}}{=} \mu_{\sigma^2}(r_{\text{eff}}\mathcal{B}) - \mu_{\sigma^2}(\mathcal{V}_L) \tag{55}$$

$$= \mathbb{E}\left[ \frac{1}{\left(\frac{\sqrt{\sigma^2 W}}{r_{\text{eff}}}\right)^n} \left( g_{\mathcal{B}}(\sqrt{\sigma^2 W}) - g_L(\sqrt{\sigma^2 W}) \right) \right] \tag{56}$$

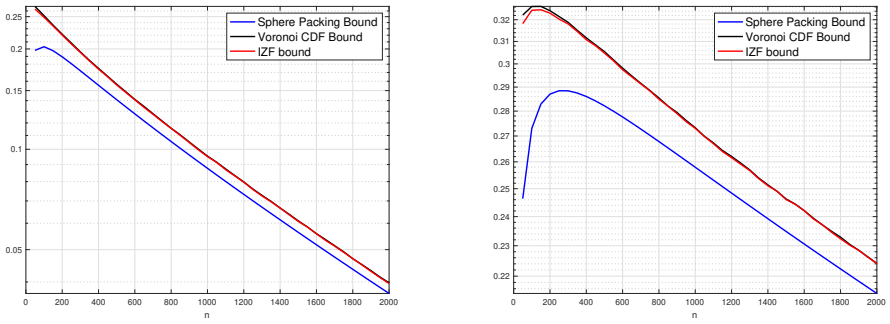
$$= \mathbb{E}\left[ \frac{1}{X_W} \left( g_{\mathcal{B}}\left( r_{\text{eff}} X_W^{1/n} \right) - g_L\left( r_{\text{eff}} X_W^{1/n} \right) \right) \right]. \tag{57}$$

Consequently,

$$\begin{aligned}
\mathbb{E}[P_e(L,\sigma^2)] &= P^{\text{SP}}(\sigma^2) + \left( \mathbb{E}[P_e(L,\sigma^2)] - P^{\text{SP}}(\sigma^2) \right) \\
&= P^{\text{SP}}(\sigma^2) + \left( \mu_{\sigma^2}(r_{\text{eff}}\mathcal{B}) - \mathbb{E}[\mu_{\sigma^2}(\mathcal{V}_L)] \right) \\
&= P^{\text{SP}}(\sigma^2) + \mathbb{E}_{\mu_n}[\Delta(L,\sigma^2)] \\
&= P^{\text{SP}}(\sigma^2) + \mathbb{E}_W\left[ \frac{1}{X_W} \left( g_{\mathcal{B}}\left( r_{\text{eff}} X_W^{1/n} \right) - \mathbb{E}_{\mu_n}\left[ g_L\left( r_{\text{eff}} X_W^{1/n} \right) \right] \right) \right] \\
&= P^{\text{SP}}(\sigma^2) + \mathbb{E}_W\left[ \frac{1}{X_W} \left( \min\{X_W, 1\} - \mathbb{E}_{\mu_n}\left[ g_L\left( r_{\text{eff}} X_W^{1/n} \right) \right] \right) \right] \qquad (58) \\
&\le P^{\text{SP}}(\sigma^2) + \mathbb{E}_W\left[ \frac{1}{X_W} \left( \min\{X_W, 1\} - \frac{X_W}{1+X_W} \right) \right], \qquad (59)
\end{aligned}$$

where in (58) we used $g_{\mathcal{B}}\left( r_{\text{eff}} X_W^{1/n} \right) = \min\{X_W, 1\}$ which follows from (14), and (59) follows from Theorem 2.3. This establishes (54). □

One can also use Theorem 2.4 to derive an upper bound on $\mathbb{E}_{\tilde{\mu}_n}[P_e(L,\sigma^2)]$. However, such bound is not useful for most values of $n$ and $\sigma^2$ due to the $e^{-\eta/2}$ term in $\underline{g}_{\text{covering}}(r)$.




(A) $\sigma^2 = \frac{0.95}{2\pi e}$ (B) $\sigma^2 = \frac{0.98}{2\pi e}$

FIGURE 1. Computation of the sphere packing lower bound, the $P_e^{\mathrm{MLB}}(\sigma^2)$ bound from [IZF12, Theorem 2], and the new upper bound from Theorem 2.8. The bounds are plotted for $\sigma^2 = \frac{0.95}{2\pi e}$ and $\sigma^2 = \frac{0.98}{2\pi e}$.

**Remark 2.9.** *Let $\tilde{Z} \sim \chi^2_n$ 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* [Pol94b] *and Ingber, Zamir, and Feder* [IZF12, Theorem 2]*, see also* [Zam14, Chapter 13.4]*, is the bound*

$$\mathbb{E}_{\mu_n}[P_e(L,\sigma^2)] \le P_e^{\mathrm{MLB}}(\sigma^2) \stackrel{\mathrm{def}}{=} \mathbb{E}\left[\min\left\{\left(\frac{\sigma^2\tilde{Z}}{{r_{\mathrm{eff}}}^2}\right)^{\frac{n}{2}}, 1\right\}\right] = P^{\mathrm{SP}}(\sigma^2) + \mathbb{E}[X_{\tilde{Z}}\mathbb{1}\{X_{\tilde{Z}} \le 1\}], \quad (60)$$

*where*

$$X_{\tilde{Z}} \stackrel{\mathrm{def}}{=} \left(\frac{\sqrt{\sigma^2\tilde{Z}}}{r_{\mathrm{eff}}}\right)^n. \quad (61)$$

*The bound we obtained in Theorem 2.8, is quite similar to $P_e^{\mathrm{MLB}}(\sigma^2)$. An analytic comparison seems non-trivial. In Figure 1 we evaluate the two bounds numerically, along with $P^{\mathrm{SP}}(\sigma^2)$ 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.*

## 3. LINEAR CODES

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

$$\mathcal{V}_{\mathcal{C}} \stackrel{\mathrm{def}}{=} \{x \in \mathbb{F}_2^n \ : \ d_H(x,0) \le d_H(x,y) \ \forall y \in \mathcal{C} \setminus \{0\}\}, \quad (62)$$

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

$$Q_\mathcal{C}(r) \stackrel{\text{def}}{=} \Pr(|U_\mathcal{C}| \le r), \quad r = 0, 1, \ldots, n. \tag{63}$$

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

$$\mathcal{S}_{n,r} \stackrel{\text{def}}{=} \left\{x \in \mathbb{F}_2^n \ : \ |x| = r\right\}, \tag{64}$$

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

$$\mathcal{B}_{n,r} \stackrel{\text{def}}{=} \left\{x \in \mathbb{F}_2^n \ : \ |x| \le r\right\}. \tag{65}$$

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

$$V_{n,r} = |\mathcal{B}_{n,r}| = \sum_{j=0}^{r} \binom{n}{j}. \tag{66}$$

Note that

$$Q_\mathcal{C}(r) = \frac{1}{|\mathcal{V}_\mathcal{C}|} \left|\mathcal{B}_{n,r} \cap \mathcal{V}_\mathcal{C}\right| = 2^{k-n} \left|\mathcal{B}_{n,r} \cap \mathcal{V}_\mathcal{C}\right|. \tag{67}$$

**Proposition 3.1.** *Let $\mathcal{C} \subset \mathbb{F}_2^n$ be a linear code of dimension $0 \le k \le n$. Then*

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

$$r_{\text{pack}}(\mathcal{C}) = \max\left\{r \in 0, 1, \ldots, n \ : \ Q_\mathcal{C}(r) = 2^{k-n} V_{n,r}\right\} \tag{68}$$

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

$$r_{\text{cov}}(\mathcal{C}) = \min\left\{r \in 0, 1, \ldots, n \ : \ Q_\mathcal{C}(r) = 1\right\} \tag{69}$$

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

$$D_\mathcal{C} \stackrel{\text{def}}{=} \frac{\mathbb{E}|U_\mathcal{C}|}{n} = \frac{1}{n} \sum_{r=0}^{n} 1 - Q_\mathcal{C}(r). \tag{70}$$

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

$$\begin{aligned} P_e(\mathcal{C}, p) &= \Pr(Z \notin \mathcal{V}_{\mathcal{C}}) \\ &= 1 - 2^{n-k}\left(\frac{p}{1-p}\cdot p^n + \frac{1-2p}{1-p}\mathbb{E}\left[\frac{Q_{\mathcal{C}}(|Z|)}{\binom{n}{|Z|}}\right]\right), \end{aligned} \tag{71}$$

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

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

**Proposition 3.2.** *Let $\mathcal{K} \subset \mathbb{F}_2^n$ be a subset, and for $U_{\mathcal{K}} \sim \mathrm{Uniform}(\mathcal{K})$ define*

$$Q_{\mathcal{K}}(r) = \Pr(|U_{\mathcal{K}}| \le r) = \frac{|\mathcal{K} \cap \mathcal{B}_{n,r}|}{|\mathcal{K}|}. \tag{72}$$

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

$$\mu_p(\mathcal{K}) \stackrel{\mathrm{def}}{=} \Pr(Z \in \mathcal{K}) = |\mathcal{K}|\left(\frac{p}{1-p}\cdot p^n + \frac{1-2p}{1-p}\mathbb{E}\left[\frac{Q_{\mathcal{K}}(|Z|)}{\binom{n}{|Z|}}\right]\right), \tag{73}$$

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

3.1. **Estimates for the expected Voronoi spherical CDF.** For $k \in \{1, \ldots, n\}$, let the discrete Grassmannian $\mathrm{Gr}_{n,k}(\mathbb{F}_2)$ 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 $\mathcal{C} \in \mathrm{Gr}_{n,k}(\mathbb{F}_2)$, and let $\pi_{\mathcal{C}} : \mathbb{F}_2^n \to \mathbb{T}_{\mathcal{C}}$ 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 of the quotient map as $\pi_{\mathcal{C}}(x) = x - f_{\mathcal{C}}(x)$, where $f_{\mathcal{C}}(x) : \mathbb{F}_2^n \to \mathcal{C}$ 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 $m_{\mathcal{C}} : \mathbb{T}_{\mathcal{C}} \to [0, 1]$ denote the normalized counting measure (uniform distribution) on $\mathbb{T}_{\mathcal{C}}$. Namely, for any $\mathcal{A} \subset \mathbb{T}_{\mathcal{C}}$ we have

$$m_{\mathcal{C}}(\mathcal{A}) \stackrel{\mathrm{def}}{=} \frac{|\mathcal{A}|}{|\mathbb{T}_{\mathcal{C}}|} = 2^{k-n}|\mathcal{A}|. \tag{74}$$

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

$$m_{\mathcal{C}}(\pi_{\mathcal{C}}(\mathcal{K})) = \sum_{x \in \mathcal{K}} \frac{2^{k-n}}{|(x + \mathcal{C}) \cap \mathcal{K}|} = \sum_{x \in \mathcal{K}} \frac{2^{k-n}}{1 + |(\mathcal{C} \setminus \{0\}) \cap (\mathcal{K} - x)|}. \tag{75}$$

Furthermore, observe that

$$Q_{\mathcal{C}}(r) = \Pr(|U_{\mathcal{C}}| \le r) = 2^{k-n}|\mathcal{B}_{n,r} \cap \mathcal{V}_{\mathcal{C}}| = m_{\mathcal{C}}(\pi_{\mathcal{C}}(\mathcal{B}_{n,r})), \tag{76}$$

where the last equality holds since, when we identify $\mathcal{V}_{\mathcal{C}}$ with $\mathbb{T}_{\mathcal{C}}$, it holds that $|\pi_{\mathcal{C}}(x)| \le |x|$ 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 3.3.** *Let $\mathcal{C}$ be a random code drawn uniformly over $\mathrm{Gr}_{n,k}(\mathbb{F}_2)$. Then, for any $\mathcal{K} \in \mathbb{F}_2^n$ we have that*

$$\mathbb{E}[m_{\mathcal{C}}(\pi_{\mathcal{C}}(\mathcal{K}))] \ge \frac{2^{k-n}|\mathcal{K}|}{1 + 2^{k-n}|\mathcal{K}|}. \tag{77}$$

*In particular,*

$$\mathbb{E}_{\mathcal{C}}[Q_{\mathcal{C}}(r)] \ge \frac{2^{k-n}V_{n,r}}{1 + 2^{k-n}V_{n,r}}. \tag{78}$$

*Proof.* Starting from (75), and using Jensen's inequality with the convexity of $t \mapsto \frac{1}{1+t}$, we obtain

$$\mathbb{E}[m_{\mathcal{C}}(\pi_{\mathcal{C}}(\mathcal{K}))] = \mathbb{E}\left[\sum_{x \in \mathcal{K}} \frac{2^{k-n}}{1 + |(\mathcal{C} \setminus \{0\}) \cap (\mathcal{K} - x)|}\right] \tag{79}$$

$$\ge \sum_{x \in \mathcal{K}} \frac{2^{k-n}}{1 + \mathbb{E}[|(\mathcal{C} \setminus \{0\}) \cap (\mathcal{K} - x)|]}. \tag{80}$$

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

$$\mathbb{E}[|(\mathcal{C} \setminus \{0\}) \cap (\mathcal{K} - x)|] = \frac{2^k - 1}{2^n - 1}(|\mathcal{K}| - 1) < 2^{k-n}|\mathcal{K}|. \tag{81}$$

Thus,

$$\mathbb{E}[m_{\mathcal{C}}(\pi_{\mathcal{C}}(\mathcal{K}))] \ge \sum_{x \in \mathcal{K}} \frac{2^{k-n}}{1 + 2^{k-n}|\mathcal{K}|} = \frac{2^{k-n}|\mathcal{K}|}{1 + 2^{k-n}|\mathcal{K}|}, \tag{82}$$

establishing (77). Combining (76) with (77) applied with $\mathcal{K} = \mathcal{B}_{n,r}$, we obtain

$$\mathbb{E}[Q_{\mathcal{C}}(r)] = \mathbb{E}[\Pr(|U_{\mathcal{C}}| \le r)] \ge \frac{2^{k-n}|\mathcal{B}_{n,r}|}{1 + 2^{k-n}|\mathcal{B}_{n,r}|} = \frac{2^{k-n}V_{n,r}}{1 + 2^{k-n}V_{n,r}}, \tag{83}$$

which establishes (78). □

3.2. **Hamming distortion of a linear code.** As a straightforward consequence of Proposition 3.1 and of Theorem 3.3 we obtain the following.

**Theorem 3.4.** *Let $\mathcal{C}$ be a random code drawn uniformly over $\mathrm{Gr}_{n,k}(\mathbb{F}_2)$. Then,*

$$\mathbb{E}[D_{\mathcal{C}}] \leq \frac{1}{n}\sum_{r=0}^{n-1}\frac{1}{1+2^{k-n}V_{n,r}}. \tag{84}$$

*Proof.* Combining part 3 of Proposition 3.1 and (78) of Theorem 3.3, we obtain

$$\mathbb{E}[D_{\mathcal{C}}] = \frac{1}{n}\sum_{r=0}^{n-1}\mathbb{E}[1-Q_{\mathcal{C}}(r)] \tag{85}$$

$$\leq \frac{1}{n}\sum_{r=0}^{n-1}1-\frac{2^{k-n}V_{n,r}}{1+2^{k-n}V_{n,r}} \tag{86}$$

$$= \frac{1}{n}\sum_{r=0}^{n-1}\frac{1}{1+2^{k-n}V_{n,r}}, \tag{87}$$

as claimed. □

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 $r_{\text{eff}}$ in lexicographic order (there is no significance to which $|\mathcal{K}| - V_{n,r_{\text{eff}}-1}$ vectors of Hamming weight $r_{\text{eff}}$ 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

$$r_{\text{eff}}(n,k) \stackrel{\text{def}}{=} \min\{r \ : \ 2^{n-k}\leq V_{n,r}\}, \tag{88}$$

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

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

$$D_{\mathcal{C}} \geq D^*_{n,k} = \frac{1}{n}\mathbb{E}|U_{\bar{\mathcal{B}}^{n,k}}|. \tag{89}$$

See Lemma 3.8 below for a more general statement. Defining $Q_{\bar{\mathcal{B}}^{n,k}}(r)$ as in (72), we also have that

$$Q_{\bar{\mathcal{B}}^{n,k}}(r) = \min\{2^{k-n}V_{n,r}, 1\}, \tag{90}$$

and therefore, using item 3 of Proposition 3.1, that holds for any set, not just a Voronoi region, we have

$$D^*_{n,k} = \frac{1}{n} \sum_{r=0}^{r_{\text{eff}}(n,k)-1} 1 - 2^{k-n} V_{n,r}. \tag{91}$$

Combining this with Theorem 3.4 we obtain

$$\Delta(n,k) \stackrel{\text{def}}{=} n(\mathbb{E}[D_{\mathcal{C}}] - D^*_{n,k}) \tag{92}$$

$$= \sum_{r=0}^{r_{\text{eff}}(n,k)-1} \frac{x_r^2}{1+x_r} + \sum_{r=r_{\text{eff}}(n,k)}^{n-1} \frac{1}{1+x_r}, \tag{93}$$

where

$$x_r = x_{r,n,k} \stackrel{\text{def}}{=} 2^{k-n} V_{n,r}. \tag{94}$$

We prove the following result in Appendix D.

**Theorem 3.5.** *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 3.6.** *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 $D_C$ is minimized by $\mathcal{C} = \{0\ldots0, 1\ldots1\}$ (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 3.7.** *A related quantity to $D_{\mathcal{C}}$ is the covering radius $r_{\text{cov}}(\mathcal{C})$. In particular, $nD_{\mathcal{C}} \le r_{\text{cov}}(\mathcal{C})$. For any code, the covering radius is at least $r_{\text{eff}}(n,k)$, and there exist codes with covering radius $r_{\text{eff}}(n,k) + O(\log n)$ [CHLL97]. 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 3.5 is significantly tighter as it bounds this gap by a constant.*

3.2.1. *Lossy compression of binary symmetric source under Hamming distortion.* Let $X \sim \text{Ber}^{\otimes n}(1/2)$, and let $0 \le R \le 1$. An $(n, R, D)$ code for $X$ consists of an encoder[2] $f : \mathbb{F}_2^n \to [\lfloor 2^{nR} \rfloor]$. and a decoder $g : [\lfloor 2^{nR} \rfloor] \to \mathbb{F}_2^n$, such that

$$\frac{1}{n}\mathbb{E}[d_H(X, g(f(X))] \le D. \tag{95}$$

[2]For $x > 1$ we write $\lfloor x \rfloor$ to denote the largest integer smaller than $x$, and $[\lfloor x \rfloor] = \{1, \ldots, \lfloor x \rfloor\}$.

Denote

$$D_n(R) = \min\{D \ : \ \exists(n, R, D) - \text{code}\}. \tag{96}$$

It is well-known [CT12, PW25] that

$$D(R) \leq D_n(R) < D(R) + O\left(\frac{\log n}{n}\right). \tag{97}$$

where

$$D(R) = 1 - h_2^{-1}(R), \tag{98}$$

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, [ZYW97, Theorem 1] shows that

$$D_n(R) = D(R) - D'(R)\frac{\log n}{2\log n} + o\left(\frac{\log n}{n}\right) \tag{99}$$

The following claim is essentially[3] stated in [Gob63, eq. 4.6-4.7], and for completeness of exposition we provide a proof in Appendix D.

**Lemma 3.8.** *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 3.5, we have the following.

**Theorem 3.9.** *Let $0 \leq k \leq n$ be an integer, and $R = \frac{k}{n} > \alpha > 0$. Then*

$$D_n(R) = D^*_{n,k} + O_\alpha\left(\frac{1}{n}\right), \tag{100}$$

*and this is achievable using a linear code.*

*Proof.* The lower bound $D_n(R) \geq D^*_{n,k}$ follows from Lemma 3.8. 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 3.5, 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. □

[3]Our definition of $D^*_{n,k}$ corresponds to the average distortion of a quasi-ball with size $2^{n-k}$, whereas Goblick 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 $2^{n-k}$.

**Remark 3.10.** *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* [KV16],[PW25, Ex. V3]

$$\begin{aligned} n\mathbb{E}[D] &\le \sum_{r=0}^{n} \left(1 - 2^{-n} V_{n,r}\right)^{2^k} \le \sum_{r=0}^{n} \left(1 - 2^{k-n} V_{n,r}\right) \\ &\le \sum_{r=0}^{n} \frac{1}{1 + 2^{k-n} V_{n,r}}, \end{aligned} \tag{101}$$

*where the last bound is the bound from Theorem 3.4. However, the first inequality 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.*

3.3. **Error probability of a linear code.** Let $p \in (0, 1/2)$ and let $Z \sim \mathrm{Ber}^{\otimes n}(p)$. For a set $\mathcal{K} \subset \mathbb{F}_2^n$ let

$$\mu_p(\mathcal{K}) \stackrel{\mathrm{def}}{=} \Pr(Z \in \mathcal{K}) = (1-p)^n \sum_{x \in \mathcal{K}} \left(\frac{p}{1-p}\right)^{|x|}. \tag{102}$$

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

$$\mu_p(\mathcal{V}_{\mathcal{C}}) \le \mu_p(\bar{\mathcal{B}}^{n,k}). \tag{103}$$

Let $X \sim \mathrm{Uniform}(\mathcal{C})$ 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

$$P_e(\mathcal{C}, p) = 1 - \mu_p(\mathcal{V}_{\mathcal{C}}). \tag{104}$$

Clearly,

$$P_e(\mathcal{C}, p) \ge P_e(\bar{\mathcal{B}}^{n,k}, p) = 1 - \mu_p(\bar{\mathcal{B}}^{n,k}) \stackrel{\mathrm{def}}{=} P_{n,k}^{\mathrm{SP}}(p), \tag{105}$$

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

**Theorem 3.11.** *Let $\mathcal{C}$ be a random code drawn uniformly over $\mathrm{Gr}_{n,k}(\mathbb{F}_2)$. Then, for any $p \in (0, 1/2)$ we have that*

$$\mathbb{E}[P_e(\mathcal{C}, p)] \le P_{n,k}^{\mathrm{SP}}(p) + \frac{1-2p}{1-p} \mathbb{E}\left[\frac{V_{n,W}}{\binom{n}{W}} \cdot \frac{\min\{x_W, x_W^{-1}\}}{1 + x_W}\right] \tag{106}$$

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

*Proof.* We have

$$\begin{aligned}\mathbb{E}[P_e(\mathcal{C},p)] &= P^{\mathrm{SP}}_{n,k}(p) + \left(\mathbb{E}[P_e(\mathcal{C},p)] - P^{\mathrm{SP}}_{n,k}(p)\right) \\ &= P^{\mathrm{SP}}_{n,k} + \left(\mu_p(\bar{\mathcal{B}}^{n,k}) - \mathbb{E}[\mu_p(\mathcal{V}_{\mathcal{C}})]\right). \end{aligned} \tag{107}$$

By Proposition 3.2 and (90), we have that

$$\mu_p(\bar{\mathcal{B}}^{n,k}) = 2^{n-k}\left(\frac{p}{1-p}\cdot p^n + \frac{1-2p}{1-p}\mathbb{E}\left[\frac{\min\{2^{k-n}V_{n,|Z|},1\}}{\binom{n}{|Z|}}\right]\right). \tag{108}$$

Similarly, by Proposition 3.2 (or part 4 of Proposition 3.1) together with Theorem 3.3, we obtain that for $\mathcal{C}\sim \mathrm{Uniform}(\mathrm{Gr}_{n,k}(\mathbb{F}_2))$

$$\mathbb{E}[\mu_p(\mathcal{V}_{\mathcal{C}})] \geq 2^{n-k}\left(\frac{p}{1-p}\cdot p^n + \frac{1-2p}{1-p}\mathbb{E}\left[\frac{2^{k-n}V_{n,|Z|}}{\binom{n}{|Z|}\left(1+2^{k-n}V_{n,|Z|}\right)}\right]\right). \tag{109}$$

Consequently, we obtain

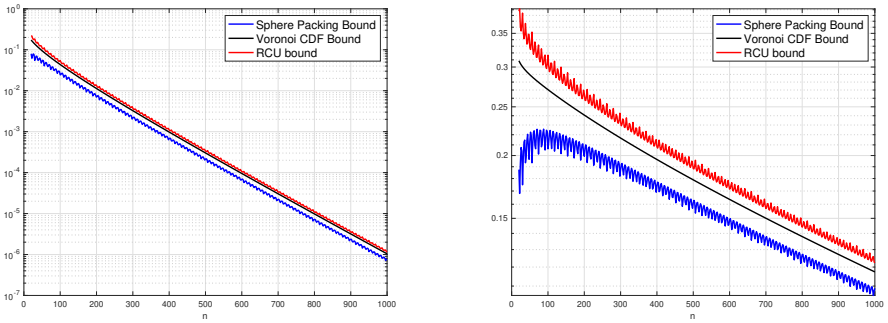
$$\begin{aligned}\Delta^p_{n,k} &\stackrel{\mathrm{def}}{=} \mu_p(\bar{\mathcal{B}}^{n,k}) - \mathbb{E}[\mu_p(\mathcal{V}_{\mathcal{C}})] \\ &\leq \frac{1-2p}{1-p}2^{n-k}\mathbb{E}\left[\frac{1}{\binom{n}{|Z|}}\left(\min\{x_{|Z|},1\} - \frac{x_{|Z|}}{1+x_{|Z|}}\right)\right] \\ &= \frac{1-2p}{1-p}2^{n-k}\mathbb{E}\left[\frac{1}{\binom{n}{|Z|}}\left(\frac{\min\{x^2_{|Z|},1\}}{1+x_{|Z|}}\right)\right] \\ &= \frac{1-2p}{1-p}2^{n-k}\mathbb{E}\left[\frac{1}{\binom{n}{|Z|}}\left(\frac{\min\{2^{k-n}V_{n,|Z|}\cdot x_{|Z|}, 2^{k-n}V_{n,|Z|}\cdot x^{-1}_{|Z|}\}}{1+x_{|Z|}}\right)\right] \\ &= \frac{1-2p}{1-p}\mathbb{E}\left[\frac{V_{n,|Z|}}{\binom{n}{|Z|}}\cdot\frac{\min\{x_{|Z|},x^{-1}_{|Z|}\}}{1+x_{|Z|}}\right]. \end{aligned} \tag{110}$$

Substituting this into (107) established the claim. □

**Remark 3.12.** *The benchmark upper bound to date for the binary symmetric channel is the so-called random coding upper bound (RCU bound) from* [Pol94a] *and* [PPV10, Theorem 33]*, which implies that for a random linear code*

$$\mathbb{E}[P_e(\mathcal{C},p)] \leq \mathrm{RCU}(n,k,p) \stackrel{\mathrm{def}}{=} \mathbb{E}\left[\min\left\{1, 2^{k-n}V_{n,W}\right\}\right]. \tag{111}$$

*It is not straightforward to compare the upper bound from Theorem 3.11 and the RCU bound. However, numerically it seems that the new bound from Theorem 3.11 does dominate the RCU bound. See Figure 2 for a numeric demonstration.*




(A) $p = 0.07$ (B) $p = 0.1$

FIGURE 2. Computation of the sphere packing lower bound, the RCU bound from [PPV10, Theorem 33], and the new upper bound from Theorem 3.11. The bounds are plotted for $p = 0.07$ and $p = 0.1$, even values of $n$ and $k = n/2$.

## APPENDIX A. PROOFS OF CLAIMS FOR LATTICES

*Proof of Proposition 2.1.* The first item follows since

$$r_{\text{pack}}(L) = \sup\{r \ : \ r\mathcal{B} \subset \mathcal{V}_L\} = \sup\left\{r \ : \ g_L(r) = \left(\frac{r}{r_{\text{eff}}}\right)^n\right\}, \quad (112)$$

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

$$r_{\text{cov}}(L) = \sup_{x\in\mathbb{R}^n} \min_{y\in L} \|x-y\|_2 = \sup_{x\in\mathcal{V}_L} \|x\|_2. \quad (113)$$

For the third item, we write

$$\mathbb{E}\|U_L\|^2 = \int_{r=0}^{\infty} \Pr(\|U_L\|^2 > r)dr = \int_{r=0}^{\infty} 1 - \Pr(\|U_L\| \le \sqrt{r})dr. \quad (114)$$

The fourth item follows directly from Proposition 3.2. □

*Proof of Proposition 2.2.* 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

$$\mu_{\sigma^2}(\mathcal{K}) = C_n \cdot |\mathcal{K}| \cdot \mathbb{E}\left[e^{-\frac{\|U\|_2^2}{2\sigma^2}}\right] \tag{115}$$

$$= C_n \cdot |\mathcal{K}| \cdot \int_0^\infty \Pr\left(e^{-\frac{\|U\|_2^2}{2\sigma^2}} \geq r\right) dr \tag{116}$$

$$= C_n \cdot |\mathcal{K}| \cdot \int_0^1 \Pr\left(\|U\|_2 \leq \left(2\sigma^2 \log\left(\frac{1}{r}\right)\right)^{\frac{1}{2}}\right) dr \tag{117}$$

$$= C_n \cdot V_n {r_{\text{eff}}}^n \cdot \int_0^1 \Pr\left(\|U\|_2 \leq \left(2\sigma^2 \log\left(\frac{1}{r}\right)\right)^{\frac{1}{2}}\right) dr \tag{118}$$

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

$$\mu_{\sigma^2}(\mathcal{K}) = C_n \cdot V_n {r_{\text{eff}}}^n \cdot \int_0^\infty \frac{1}{2} e^{-\frac{w}{2}} \Pr\left(\|U\|_2 \leq \sqrt{\sigma^2 w}\right) dw \tag{119}$$

$$= C_n \cdot V_n {r_{\text{eff}}}^n \cdot 2^{\frac{n}{2}}\Gamma\left(1+\frac{n}{2}\right) \cdot \int_0^\infty \frac{w^{\frac{n+2}{2}-1}e^{-\frac{w}{2}}}{2^{\frac{n+2}{2}}\Gamma\left(\frac{n+2}{2}\right)} \frac{\Pr\left(\|U\|_2 \leq \sqrt{\sigma^2 w}\right)}{w^{\frac{n}{2}}} dw \tag{120}$$

$$= C_n \cdot V_n \cdot 2^{\frac{n}{2}}\Gamma\left(1+\frac{n}{2}\right) \cdot \mathbb{E}\left[\frac{\Pr\left(\|U\|_2 \leq \sqrt{\sigma^2 W}\right)}{\left(\frac{W}{{r_{\text{eff}}}^2}\right)^{\frac{n}{2}}}\right]. \tag{121}$$

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

$$C_n \cdot V_{2,n} \cdot 2^{\frac{n}{2}}\Gamma\left(1+\frac{n}{2}\right) = \frac{1}{(\sigma^2)^{\frac{n}{2}}}. \tag{122}$$

Substituting this into (121), establishes the claim. □

## Appendix B. Proof of Theorem 2.4

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

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

equivalently, $\varepsilon(J, L)$ is the density of points in $\mathbb{R}^n$ not covered by $L+J$. Also recall the definition of $\eta$ from (26). With these notations, the following is a corollary of [Sch58] (see also [Rog58], where a similar

bound was shown for larger $\eta$, but with a large constant $c_{\mathrm{Rog}}$ instead of the constant 7 below):

**Theorem B.1** (Corollary of Theorem 4 of [Sch58])**.** *For all $n > 13$ and for every Borel measurable $J \subset \mathbb{R}^n$ with*

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

*and bounded diameter we have*

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

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

$$e^{-V}(3/4)^{n/2}e^{4V} \leq e^{-\eta}, \quad e^{-V}V^{n-1}n^{-n+1}e^{V+n} \leq e^{-\eta}, \tag{123}$$

and consequently for $|R|$ defined in [Sch58, eq. (3)], we have $e^{-V}|R| < 7e^{-\eta}$.

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

$$\varepsilon(J, L) = \lim_{a\to\infty} \frac{1}{a^n} \int_{x\in\mathrm{CUBE}(a)} \mathbb{1}\{|L \cap (x + J)| = \emptyset\}dx. \tag{124}$$

Consequently, by the bounded convergence theorem

$$\mathbb{E}_{\mu_n}[\varepsilon(J, L)] = \lim_{a\to\infty} \frac{1}{a^n} \int_{x\in\mathrm{CUBE}(a)} \mathbb{E}_{\mu_n}[\mathbb{1}\{|L \cap (x + J)| = \emptyset\}]dx \tag{125}$$

$$= \lim_{a\to\infty} \frac{1}{a^n} \int_{x\in\mathrm{CUBE}(a)} \mu_n\left\{L \in \mathcal{L}_n \ : \ L \text{ is } (x + J) - \text{admissible}\right\} dx \tag{126}$$

$$= \lim_{a\to\infty} \frac{1}{a^n} \int_{x\in\mathrm{CUBE}(a)} e^{-V}(1 - R)dx \tag{127}$$

$$\in e^{-V} \pm 7e^{-\eta}, \tag{128}$$

where in (127) we have applied [Sch58, Theorem 4], and in the last step we used the fact that $e^{-V}|R| \leq 7e^{-\eta}$ provided that $|J| \leq \eta$. □

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

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

$$\mathbb{E}[g_L(r)] \geq 1 - e^{-(r/r_{\mathrm{eff}})^n} - 7 \cdot e^{-\eta}. \tag{129}$$

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*

$$\mu_n\left(\left\{L \in \mathcal{L}_n \ : \ \varepsilon(J, L) > e^{-\eta/2}\right\}\right) \leq 8e^{-\eta/2} \tag{130}$$

Tracking down the constants in [ORW22, Theorem 1.2], gives the following.

**Theorem B.4** (Special case of Theorem 1.2 from [ORW22])**.** *For*

$$\mathcal{E}_\eta = \{L \in \mathcal{L}_n \ : \ r_{\mathrm{cov}}(L) \leq 4n^2\eta\} \tag{131}$$

*and $L \sim \mu_n$, we have*

$$\Pr(L \notin \mathcal{E}_\eta) \leq 16e^{-\eta/2}. \tag{132}$$

To obtain this result we apply the proof of [ORW22, Theorem 1.2], with $V = \eta$, and $n < p < 2n$, using Corollary B.3 instead of [ORW22, 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 $p^2V = p^2\eta < 4n^2\eta$ 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 2.4. Recall that $\mu_n$ is the Haar-Siegel probability distribution, and $\tilde{\mu}_n = \mu_{n|\mathcal{E}_\eta}$. For all $r > 0$, we have

$$\begin{aligned}
\mathbb{E}_{\mu_n}[g_L(r)] &= \Pr(L \in \mathcal{E}_\eta)\mathbb{E}[g_L(r)|L \in \mathcal{E}_\eta] + \Pr(L \notin \mathcal{E}_\eta)\mathbb{E}[g_L(r)|L \notin \mathcal{E}_\eta] \\
&= \Pr(L \in \mathcal{E}_\eta)\mathbb{E}_{\tilde{\mu}_n}[g_L(r)] + \Pr(L \notin \mathcal{E}_\eta)\mathbb{E}[g_L(r)|L \notin \mathcal{E}_\eta] \\
&\leq \mathbb{E}_{\tilde{\mu}_n}[g_L(r)] + \Pr(L \notin \mathcal{E}_\eta). \qquad (133)
\end{aligned}$$

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

$$\begin{aligned}
\mathbb{E}_{\tilde{\mu}_n}[g_L(r)] &\geq 1 - e^{-(r/r_{\mathrm{eff}})^n} - 7 \cdot e^{-\eta} - 16e^{-\eta/2} \qquad (134) \\
&\geq 1 - e^{-(r/r_{\mathrm{eff}})^n} - 23 \cdot e^{-\eta/2}. \qquad (135)
\end{aligned}$$

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 $(r/r_{\mathrm{eff}})^n \geq \eta/2$. Finally, by definition of $\tilde{\mu}_n$ we have that for $(r/r_{\mathrm{eff}})^n > 4n^2\eta$ it holds that $g_L(r) = 1$ with probability 1 for $L \sim \tilde{\mu}_n$. This establishes the claimed result.

## Appendix C. Normalized $p$th Moment

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

$$\mathcal{V}_L^{(p)} \stackrel{\text{def}}{=} \{x \in \mathbb{R}^n \ : \ \|x\|_p \leq \|x-y\|_p, \ \forall y \in L \setminus \{0\}\}, \tag{136}$$

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 $\pi_L : \mathbb{R}^n \to \mathbb{T}_L$ 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

$$G_L^{(p)} \stackrel{\text{def}}{=} \frac{\mathbb{E}(\|U_L\|_p^p)}{n} \tag{137}$$

Let

$$\mathcal{B}^{(p)} \stackrel{\text{def}}{=} \{x \in \mathbb{R}^n \ : \ \|x\|_p \leq 1\} \tag{138}$$

be the unit closed ball with respect to $\|\cdot\|_p$, ans let $V_{p,n}$ be its volume. The main result of this section, is the following extension of Theorem 2.5.

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

$$\mathbb{E}[G_L^{(p)}] \leq \frac{1}{n{V_{p,n}}^{p/n}} \cdot \frac{1}{\text{sinc}(p/n)}. \tag{139}$$

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

$$\mathbb{E}\|U_L\|_p^p = \int_0^\infty \Pr(\|U_L\|_p^p > r)dr = \int_0^\infty \Pr(\|U_L\|_p > r^{1/p})dr. \tag{140}$$

We further have that

$$\Pr(\|U_L\|_p > r^{1/p}) = 1 - \Pr(\|U_L\|_p \leq r^{1/p}), \tag{141}$$

and that

$$\Pr(\|U_L\|_p \leq r^{1/p}) = |r^{1/p}\mathcal{B}^{(p)} \cap \mathcal{V}_L^{(p)}| = m_L(\pi_L(r^{1/p}\mathcal{B}^{(p)})), \tag{142}$$

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

We have therefore obtained that

$$\mathbb{E}\|U_L\|_p^p = \int_0^\infty 1 - m_L(\pi_L(r^{1/p}\mathcal{B}^{(p)}))dr. \tag{143}$$

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

$$\mathbb{E}\|U_L\|_p^p = \int_0^\infty 1 - \mathbb{E}[m_L(\pi_L(r^{1/p}\mathcal{B}^{(p)}))]dr. \tag{144}$$

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

$$\mathbb{E}[m_L(\pi_L(r^{1/p}\mathcal{B}^{(p)}))] \geq \frac{|r^{1/p}\mathcal{B}^{(p)}|}{1+|r^{1/p}\mathcal{B}^{(p)}|} = \frac{r^{n/p}V_{p,n}}{1+r^{n/p}V_{p,n}}, \tag{145}$$

and therefore

$$\mathbb{E}\|U_L\|_p^p \leq \int_0^\infty \frac{1}{1+(r{V_{p,n}}^{p/n})^{n/p}}dr \tag{146}$$

$$= \frac{1}{{V_{p,n}}^{p/n}} \int_0^\infty \frac{1}{1+t^{n/p}}dt. \tag{147}$$

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

$$\int_0^\infty \frac{1}{1+t^\nu}dt = \frac{\pi/\nu}{\sin(\pi/\nu)} = \frac{1}{\operatorname{sinc}(1/\nu)}, \tag{148}$$

and we obtain that

$$\mathbb{E}\|U_L\|_p^p \leq \frac{1}{{V_{p,n}}^{p/n}} \cdot \frac{1}{\operatorname{sinc}(p/n)}, \tag{149}$$

establishing the claimed result. □

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

$$G_L^{(p)} \geq G_{n,p}^* \stackrel{\text{def}}{=} \frac{1}{(n+p){V_{p,n}}^{p/n}}. \tag{150}$$

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 (140), noting that

$$\Pr(\|U_S\|_p^p \geq r) = \begin{cases} 1 - r^{n/p}V_{p,n} & 0 \leq r \leq r_{\text{eff}}^p \\ 0 & r > r_{\text{eff}}^p \end{cases}. \tag{151}$$

The following is the analogue of Lemma 2.6 for general $p > 0$.

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

$$\Pr\left(G_L^{(p)} > (1+\kappa)G_{n,p}^*\right) \leq \frac{2p}{\kappa n}. \tag{152}$$

*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

$$\Pr\left(G_L^{(p)} \geq (1+\kappa)G_{n,p}^*\right) = \Pr(Y \geq \kappa) \leq \frac{\mathbb{E}[Y]}{\kappa}. \tag{153}$$

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

$$\frac{1}{\operatorname{sinc}(x)} \leq \frac{\pi x}{\pi x(1-\frac{(\pi x)^2}{6})} \leq 1 + \frac{1}{5}(\pi x)^2 < 1 + 2x^2. \tag{154}$$

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

$$\begin{aligned}\mathbb{E}[Y] &\leq \frac{n+p}{n}\frac{1}{\operatorname{sinc}(p/n)} - 1 \leq \left(1+\frac{p}{n}\right)\left(1+2\left(\frac{p}{n}\right)^2\right) - 1 \\ &= \frac{p}{n} + 2\frac{p^2}{n^2} + 2\frac{p^3}{n^3} < 2\frac{p}{n},\end{aligned} \tag{155}$$

which yields the claimed result. □

## Appendix D. Proofs of claims for linear codes

*Proof of Proposition 3.1.* The first item follows since

$$r_{\text{pack}}(\mathcal{C}) = \max\{r \ : \ \mathcal{B}_{n,r} \subset \mathcal{V}_{\mathcal{C}}\} = \max\{r \ : \ Q_{\mathcal{C}}(r) = 2^{k-n}V_{n,r}\}, \tag{156}$$

where in the second equality we have used (67). The second item follows since

$$r_{\text{cov}}(\mathcal{C}) = \max_{x\in\mathbb{F}_2^n}\min_{y\in\mathcal{C}} d_H(x,y) = \max_{x\in\mathcal{V}_{\mathcal{C}}}|x|. \tag{157}$$

For the third item, we write

$$\mathbb{E}|U_L| = \sum_{r=0}^{n}\Pr(|U_{\mathcal{C}}| > r) = \sum_{r=0}^{n} 1 - \Pr(|U_{\mathcal{C}}| \leq r) = \sum_{r=0}^{n} 1 - Q_{\mathcal{C}}(r). \tag{158}$$

The fourth item follows directly from Proposition 3.2. □

*Proof of Proposition 3.2.* 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

$$\Pr(Z \in \mathcal{K}) = \sum_{r=0}^{n} \Pr\left(Z \in (\mathcal{K} \cap \mathcal{S}_{n,r})\right) \tag{159}$$

$$= \sum_{r=0}^{n} \varphi_p(r) \left|\mathcal{K} \cap \mathcal{S}_{n,r}\right| \tag{160}$$

$$= \sum_{r=0}^{n} \varphi_p(r) \left(\left|\mathcal{K} \cap \mathcal{B}_{n,r}\right| - \left|\mathcal{K} \cap \mathcal{B}_{n,r-1}\right|\right) \tag{161}$$

$$= \varphi_p(n) \left|\mathcal{K} \cap \mathcal{B}_{n,n}\right| + \sum_{r=0}^{n-1} (\varphi_p(r) - \varphi_p(r+1)) \left|\mathcal{K} \cap \mathcal{B}_{n,r}\right| \tag{162}$$

$$= \left(\frac{p}{1-p} + \frac{1-2p}{1-p}\right) \varphi_p(n) \left|\mathcal{K} \cap \mathcal{B}_{n,n}\right| + \frac{1-2p}{1-p} \sum_{r=0}^{n-1} \varphi_p(r) \left|\mathcal{K} \cap \mathcal{B}_{n,r}\right| \tag{163}$$

$$= |\mathcal{K}| \cdot \frac{p}{1-p} \cdot p^n + \frac{1-2p}{1-p} \sum_{r=0}^{n} \varphi_p(r) \left|\mathcal{K} \cap \mathcal{B}_{n,r}\right| \tag{164}$$

$$= |\mathcal{K}| \cdot \frac{p}{1-p} \cdot p^n + |\mathcal{K}| \cdot \frac{1-2p}{1-p} \sum_{r=0}^{n} \binom{n}{r} p^r (1-p)^{n-r} \frac{\left|\mathcal{K} \cap \mathcal{B}_{n,r}\right| / |\mathcal{K}|}{\binom{n}{r}} \tag{165}$$

$$= |\mathcal{K}| \left(\frac{p}{1-p} \cdot p^n + \frac{1-2p}{1-p} \sum_{r=0}^{n} \binom{n}{r} p^r (1-p)^{n-r} \frac{Q_{\mathcal{K}}(r)}{\binom{n}{r}}\right) \tag{166}$$

$$= |\mathcal{K}| \left(\frac{p}{1-p} \cdot p^n + \frac{1-2p}{1-p} \mathbb{E}\left[\frac{Q_{\mathcal{K}}(|Z|)}{\binom{n}{|Z|}}\right]\right), \tag{167}$$

as claimed. □

*Proof of Theorem 3.5.* Let $m < n/2 - 1$ be a positive integer, and denote

$$\beta_m = \frac{n-m}{m+1} > 1. \tag{168}$$

We claim that

$$\gamma_r = \frac{\binom{n}{r+1}}{V_{n,r}} \geq \beta_m - 1, \quad \forall 0 \leq r \leq m. \tag{169}$$

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

$$\gamma_r = \frac{\binom{n}{r+1}}{V_{n,r}} = \frac{\binom{n}{r+1}}{\binom{n}{r} + V_{n,r-1}} = \frac{\binom{n}{r+1}}{\binom{n}{r}\left(1 + \frac{1}{\gamma_{r-1}}\right)} \tag{170}$$

$$= \frac{n-r}{r+1}\frac{\gamma_{r-1}}{1+\gamma_{r-1}} \ge \beta_m \cdot \frac{\gamma_{r-1}}{1+\gamma_{r-1}} \ge 1 - \beta_m, \tag{171}$$

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 (169), we have that

$$\frac{x_{r+1}}{x_r} = \frac{V_{n,r+1}}{V_{n,r}} = 1 + \frac{\binom{n}{r+1}}{V_{n,r}} = 1 + \gamma_r \ge \beta_m, \quad \forall 0 < r \le m. \tag{172}$$

By (93), for any $r_{\text{eff}}(n,k) < m < n/2 - 1$ we can write

$$\Delta(n,k) \stackrel{\text{def}}{=} S_1 + S_{2a} + S_{2b}, \tag{173}$$

where

$$S_1 = \sum_{r=0}^{r_{\text{eff}}(n,k)-1} \frac{x_r^2}{1+x_r} \le \sum_{r=0}^{r_{\text{eff}}(n,k)-1} x_r \tag{174}$$

$$S_{2a} = \sum_{r=r_{\text{eff}}(n,k)}^{m} \frac{1}{1+x_r} \le \sum_{r=r_{\text{eff}}(n,k)}^{m} x_r^{-1} \tag{175}$$

$$S_{2b} = \sum_{r=1+m}^{n} \frac{1}{1+x_r} \le n \cdot x_m^{-1}. \tag{176}$$

Note that by definition of $r_{\text{eff}}(n,k)$, we have that $x_r < 1$ for all $r \le r_{\text{eff}}(n,k) - 1$, and that $x_r \ge 1$ for all $r \ge r_{\text{eff}}(n,k)$. By (172) we therefore have

$$x_r \le \beta_m^{-(r_{\text{eff}}(n,k)-1-r)}, \quad \forall 0 \le r \le r_{\text{eff}}(n,k) - 1, \tag{177}$$

$$x_r^{-1} \le \beta_m^{-(r-r_{\text{eff}}(n,k))}, \quad \forall r_{\text{eff}}(n,k) \le r \le m. \tag{178}$$

It therefore follows that

$$S_1 \leq \sum_{r=0}^{r_{\text{eff}}(n,k)-1} x_r \leq \sum_{r=0}^{r_{\text{eff}}(n,k)-1} \beta_m^{-(r_{\text{eff}}(n,k)-r)} < \sum_{j=0}^{\infty} \beta_m^{-j} = \frac{1}{1-\beta_m^{-1}} \tag{179}$$

$$S_{2a} \leq \sum_{r=r_{\text{eff}}(n,k)}^{m} x_r^{-1} \leq \sum_{r=r_{\text{eff}}(n,k)}^{m} \beta_m^{-(r-r_{\text{eff}}(n,k))} < \sum_{j=1}^{\infty} \beta_m^{-j} \leq \frac{1}{1-\beta_m^{-1}}. \tag{180}$$

Thus,

$$\Delta(n,k) \leq 2\frac{\beta_m}{\beta_m - 1} + n \cdot \beta_m^{-(m-r_{\text{eff}}(n,k))}. \tag{181}$$

Take $m = \left\lceil \frac{n}{2}\left(h_2^{-1}(1-\alpha)+\frac{1}{2}\right)\right\rceil$,cwhere $h_2(p) = -p\log_2(p) - (1-p)\log_2(1-p)$, 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 (181), we obtain

$$\Delta(n,k) \leq 2\frac{1-\kappa}{1-2\kappa} + 1, \tag{182}$$

as claimed. □

*Proof of Lemma 3.8.* Let $X \sim \text{Ber}^{\otimes n}(1/2)$ and let $\mathcal{C} = \{c_1, \ldots, c_{2^k}\} \subset \{0,1\}^n$ be the codebook corresponding to the image of the decoder $g(\cdot)$. Define the random variable

$$Y = d_H(X, \mathcal{C}) = \min_{c \in \mathcal{C}} d_H(X, c). \tag{183}$$

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

$$D = \mathbb{E}[Y] = \sum_{y=0}^{n} \Pr(Y > y) = \sum_{y=0}^{n} 1 - \Pr(Y \leq y). \tag{184}$$

Let

$$\mathcal{A}_y = \{x \in \mathbb{F}_2^n \ : \ d(x, \mathcal{C}) \leq y\}. \tag{185}$$

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,

$$\Pr(Y \leq y) = \Pr(X \in \mathcal{A}_y) = 2^{-n}|\mathcal{A}_y| \leq \min\{2^{k-n}V_{n,y}, 1\}. \tag{186}$$

Substituting this into (184), and recalling (91), yields the claimed result. □

## References


[AA23] E. Agrell and B. Allen, *On the best lattice quantizers*, IEEE Transactions on Information Theory **69** (2023), no. 12, 7650–7658.

[AB15] V. Anantharam and F. Baccelli, *Capacity and error exponents of stationary point processes under random additive displacements*, Advances in Applied Probability **47** (2015), no. 1, 1–26.

[AE98] E. Agrell and T. Eriksson, *Optimization of lattices for quantization*, IEEE Transactions on Information Theory **44** (1998), no. 5, 1814–1828.

[APKA24] E. Agrell, D. Pook-Kolb, and B. Allen, *Glued lattices are better quantizers than $K_{12}$*, IEEE Transactions on Information Theory (2024).

[APKA25] E. Agrell, D. Pook-Kolb, and B. Allen, *Optimization and identification of lattice quantizers*, IEEE Transactions on Information Theory (2025).

[BF02] A. Barg and G D. Forney, *Random codes: Minimum distances and error exponents*, IEEE Transactions on Information Theory **48** (2002), no. 9, 2568–2573.

[Bla71] I. F Blake, *The Leech lattice as a code for the Gaussian channel*, Information and control **19** (1971), no. 1, 66–74.

[BS83] E. Barnes and N. Sloane, *The optimal lattice quantizer in three dimensions*, SIAM Journal on Algebraic Discrete Methods **4** (1983), no. 1, 30–41.

[CFR59] H. S. M. Coxeter, L. Few, and C. A. Rogers, *Covering space with equal spheres*, Mathematika **6** (1959), 147–157. MR124821

[CHLL97] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes*, Vol. 54, Elsevier, 1997.

[CS82] J. Conway and N. Sloane, *Voronoi regions of lattices, second moments of polytopes, and quantization*, IEEE Transactions on Information Theory **28** (1982), no. 2, 211–226.

[CS83] J. Conway and N. Sloane, *A fast encoding method for lattice codes and quantizers*, IEEE Transactions on Information Theory **29** (1983), no. 6, 820–824.

[CS84] J. H Conway and N. J. Sloane, *On the Voronoi regions of certain lattices*, SIAM Journal on Algebraic Discrete Methods **5** (1984), no. 3, 294–305.

[CS85] J. Conway and N. Sloane, *A lower bound on the average error of vector quantizers (corresp.)*, IEEE Transactions on Information Theory **31** (1985), no. 1, 106–109.

[CS88] J. H. Conway and N. J. A. Sloane, *Sphere packing, lattices and groups*, Grundlehren de mathemtische wissenschaften, vol. 290, Springer, 1988.

[CT12] T. M Cover and J. A Thomas, *Elements of information theory*, John Wiley & Sons, 2012.

[dB75] R. de Buda, *The upper error bound of a new near-optimal code*, IEEE Trans. Inform. Theory **IT-21** (1975), 441–445.

[ELZ05] U. Erez, S. Litsyn, and R. Zamir, *Lattices which are good for (almost) everything*, IEEE Trans. Inform. Theory **51** (2005), no. 10, 3401–3416. MR2236418

[EZ04] U. Erez and R. Zamir, *Achieving 1/2 log (1+ SNR) on the AWGN channel with lattice encoding and decoding*, IEEE Transactions on Information Theory **50** (2004), no. 10, 2293–2314.

[For88a] G D. Forney, *Coset codes. i. introduction and geometrical classification*, IEEE Transactions on Information Theory **34** (1988), no. 5, 1123–1151.

[For88b] G D. Forney, *Coset codes. ii. binary lattices and related codes*, IEEE Transactions on Information Theory **34** (1988), no. 5, 1152–1187.

[For89] G. D. Forney, *Multidimensional constellations. ii. Voronoi constellations*, IEEE Journal on Selected Areas in Communications **7** (1989), no. 6, 941–958.

[FT59] L Fejes Toth, *Sur la représentation d'une population infinie par un nombre fini d'éléments*, Acta Mathematica Hungarica **10** (1959), no. 3-4, 299–304.

[Gal68] R. G Gallager, *Information theory and reliable communication*, Vol. 588, Springer, 1968.

[Ger79] A. Gersho, *Asymptotically optimal block quantization*, IEEE Transactions on information theory **25** (1979), no. 4, 373–380.

[Gob63] T. J. Goblick, *Coding for a discrete information source with a distortion measure*, Ph.D. Thesis, 1963.

[GR07] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, Academic press, 2007.

[HLR09] I. Haviv, V. Lyubashevsky, and O. Regev, *A note on the distribution of the distance from a lattice*, Discrete & Computational Geometry **41** (2009), no. 1, 162–176.

[IZF12] A. Ingber, R. Zamir, and M. Feder, *Finite-dimensional infinite constellations*, IEEE transactions on information theory **59** (2012), no. 3, 1630–1656.

[KV16] V. Kostina and S. Verdú, *Nonasymptotic noisy lossy source coding*, IEEE Transactions on Information Theory **62** (2016), no. 11, 6111–6123.

[KZ09] Y. Kochman and R. Zamir, *Joint Wyner–Ziv/dirty-paper coding by modulo-lattice modulation*, IEEE Transactions on Information Theory **55** (2009), no. 11, 4878–4889.

[LL24] C. W. Ling and C. T. Li, *Rejection-sampled universal quantization for smaller quantization errors*, arXiv preprint arXiv:2402.03030 (2024).

[Loe97] H.-A. Loeliger, *Averaging bounds for lattices and linear codes*, IEEE Trans. Inform. Theory **43** (1997), no. 6, 1767–1773. MR1481036

[LSZ02] T. Linder, C Schlegal, and K. Zeger, *Corrected proof of de buda's theorem (lattice channel codes)*, IEEE transactions on information theory **39** (2002), no. 5, 1735–1737.

[LWLC22] S. Lyu, Z. Wang, C. Ling, and H. Chen, *Better lattice quantizers constructed from complex integers*, IEEE Transactions on Communications **70** (2022), no. 12, 7932–7940.

[Mag20] A. Magazinov, *A proof of a conjecture by Haviv, Lyubashevsky and Regev on the second moment of a lattice Voronoi cell*, Advances in Geometry **20** (2020), no. 1, 117–120.

[NG11] B. Nazer and M. Gastpar, *Compute-and-forward: Harnessing interference through structured codes*, IEEE Transactions on Information Theory **57** (2011), no. 10, 6463–6486.

[OE16] O. Ordentlich and U. Erez, *A simple proof for the existence of "good" pairs of nested lattices*, IEEE Transactions on Information Theory **62** (2016), no. 8, 4439–4453.

[OEN14] O. Ordentlich, U. Erez, and B. Nazer, *The approximate sum capacity of the symmetric Gaussian k-user interference channel*, IEEE Transactions on Information Theory **60** (2014), no. 6, 3450–3482.

[ORW22] O. Ordentlich, O. Regev, and B. Weiss, *New bounds on the density of lattice coverings*, Journal of the American Mathematical Society **35** (2022), no. 1, 295–308.

[ORW25] O. Ordentlich, O. Regev, and B. Weiss, *Bounds on the density of smooth lattice coverings*, Journal d'Analyse Mathématique (2025), 1–26.

[PKAA24] D. Pook-Kolb, E. Agrell, and B. Allen, *Parametric lattices are better quantizers in dimensions 13 and 14*, arXiv preprint arXiv:2411.19250 (2024).

[Pol94a] G. Poltyrev, *Bounds on the decoding error probability of binary linear codes via their spectra*, IEEE Transactions on Information Theory **40** (1994), no. 4, 1284–1292.

[Pol94b] G. Poltyrev, *On coding without restrictions for the AWGN channel*, IEEE Transactions on Information Theory **40** (1994), no. 2, 409–417.

[PPV10] Y. Polyanskiy, H V. Poor, and S. Verdú, *Channel coding rate in the finite blocklength regime*, IEEE Transactions on Information Theory **56** (2010), no. 5, 2307–2359.

[PW25] Y. Polyanskiy and Y. Wu, *Information theory: From coding to learning*, Cambridge university press, 2025.

[Rog58] C. A. Rogers, *Lattice covering of space: The Minkowski-Hlawka theorem*, Proc. London Math. Soc. (3) **8** (1958), 447–465. MR0096639

[Rog59] C. A. Rogers, *Lattice coverings of space*, Mathematika **6** (1959), 33–39. MR124820

[Sch58] W. M. Schmidt, *The measure of the set of admissible lattices*, Proc. Amer. Math. Soc. **9** (1958), 390–403. MR96638

[Sie45] C. L. Siegel, *A mean value theorem in geometry of numbers*, Ann. of Math. (2) **46** (1945), 340–347. MR0012093 (6,257b)

[SS06] I. Sason and S. Shamai, *Performance analysis of linear codes under maximum-likelihood decoding: A tutorial*, Foundations and Trends® in Communications and Information Theory **3** (2006), no. 1–2, 1–222.

[Str11] A. Strömbergsson, *On the probability of a random lattice avoiding a large convex set*, Proc. Lond. Math. Soc. (3) **103** (2011), no. 6, 950–1006. MR2861748

[UR98] R. Urbanke and B. Rimoldi, *Lattice codes can achieve capacity on the AWGN channel*, IEEE transactions on Information Theory **44** (1998), no. 1, 273–278.

[Zad82] P. Zador, *Asymptotic quantization error of continuous signals and the quantization dimension*, IEEE Transactions on Information Theory **28** (1982), no. 2, 139–149.

[Zam14] R. Zamir, *Lattice coding for signals and networks*, Cambridge University Press, Cambridge, 2014.

[ZF96] R. Zamir and M. Feder, *On lattice quantization noise*, IEEE Transactions on Information Theory **42** (1996), no. 4, 1152–1159.

[ZSE02] R. Zamir, S. Shamai, and U. Erez, *Nested linear/lattice codes for structured multiterminal binning*, IEEE Transactions on Information Theory **48** (2002), no. 6, 1250–1276.

[ZYW97] Z. Zhang, E.-h. Yang, and V. K. Wei, *The redundancy of source coding with a fidelity criterion. 1. known statistics*, IEEE Transactions on Information Theory **43** (1997), no. 1, 71–91.

School of Computer Science and Engineering, Hebrew University