

SPHERE PACKING AND THE GEOMETRY OF NUMBERS

AMBAREESH SHYAM SUNDAR

ABSTRACT. In this paper, we discuss connections between Minkowski's geometry of numbers and the sphere packing problem. We first review existing results in the study of sphere packing, then state some bounds on lattices and lattice packings (with a few proofs). Throughout this discussion, we provide applications of these results to number theory and coding theory.

1. INTRODUCTION

In 1900, David Hilbert published his famous list of 23 open problems in mathematics. The 18th problem consisted of three separate questions, of which the third one asked: “what is the densest sphere packing?”.

Most mathematicians interpreted this to be equivalent to Kepler’s conjecture, which stated the following.

Theorem 1.1. *The densest sphere packing in three dimensions has density $\frac{\pi}{3\sqrt{2}}$.*

Johannes Kepler introduced the conjecture in 1611, but it was not proved until 1998, when Thomas Hales produced a computer-assisted proof that relied on insights provided by László Fejes Tóth. That the sphere packing problem in three dimensions alone took nearly 400 years to solve (longer than Fermat’s Last Theorem!) is a testament to its difficulty.

Before we proceed, we will introduce some terminology to state the sphere packing problem precisely.

Definition 1.2. For some fixed d , let $B(x, r)$ denote the open ball in $\mathbb{R}^d$ centered at x with radius r . Let $\|\cdot\|$ denote the standard Euclidean norm. Let X be a closed discrete subset of $\mathbb{R}^d$ such that for any $x_1, x_2 \in X$, $\|x_1 - x_2\| \geq 2r$; that is, $B(x_1, r)$ and $B(x_2, r)$ do not intersect. Then the set

$$\mathcal{P}_X = \bigcup_{x \in X} B(x, r)$$

is a d -dimensional packing of spheres of radius r .

Definition 1.3. Let $\mathcal{P}_X$ be a d -dimensional sphere packing. The *upper density* of $\mathcal{P}_X$ is defined by

$$\Delta(\mathcal{P}_X) = \limsup_{R \rightarrow \infty} \frac{\mu(\mathcal{P}_X \cap B(0, R))}{\mu(B(0, R))}$$

where μ is the Lebesgue measure on $\mathbb{R}^d$.

The *sphere packing problem* is the problem of finding a packing $\mathcal{P}$ that maximizes $\Delta(\mathcal{P})$.

Using this terminology, Kepler’s conjecture claims that there exists no 3-dimensional packing $\mathcal{P}$ for which $\Delta(\mathcal{P}) > \pi/3\sqrt{2}$.

2. KNOWN RESULTS

The sphere packing problem has only been solved in dimensions 1, 2, 3, 8, and 24.

Dimension 1 is easy: since a sphere in $\mathbb{R}^1$ is just an open interval of length $2r$, we can take $X = 2r\mathbb{Z}$; then $\mathcal{P}_X$ covers all but a countably infinite subset of $\mathbb{R}^1$, which means $\Delta(\mathcal{P}_X) = 1$.

In dimension 2, the problem already becomes nontrivial. Intuition tells us that the most efficient sphere packing is the “honeycomb” packing, and this turns out to be true. In 1940, L. F. Tóth proved the following:

Theorem 2.1. *The densest sphere packing $\mathcal{P}$ in two dimensions has density $\Delta(\mathcal{P}) = \frac{\pi}{2\sqrt{3}}$.*

We show this result using the method outlined in [1]. First, we define a construction known as *Delaunay triangulation*.

Definition 2.2. Let X be a discrete subset of $\mathbb{R}^d$. A *Delaunay triangulation* of X is a set of triangles $D \subseteq \binom{X}{3}$ in $\mathbb{R}^d$ such that:

1. Every element of X is in some triangle $T \in D$.
2. For every triangle $T \in D$, no element of X lies in the interior of the region bounded by the circumcircle of T .

Now we are ready to give the proof.

Proof. We begin by proving two important lemmas.

Lemma A. Let X be a discrete subset of $\mathbb{R}^d$ such that $\mathcal{P}_X$ is a packing of radius r spheres that is saturated (that is, for any $y \in \mathbb{R}^d$, $B(y, r) \cap \mathcal{P}_X \neq \emptyset$), and let D be a Delaunay triangulation of X . Then the largest interior angle θ of any triangle $T \in D$ satisfies

$$\frac{\pi}{3} \leq \theta \leq \frac{2\pi}{3}.$$

Proof. Let the interior angles of $T = \{x, y, z\}$ be $\theta_1 < \theta_2 < \theta$, and assume without loss of generality that the measure of angle z is θ_1 . Then $\theta_1 + \theta_2 + \theta = \pi$.

Clearly it is impossible for θ to be less than $\frac{\pi}{3}$. Assume for the sake of contradiction that $\theta > \frac{2\pi}{3}$. Then $\theta_1 < (\pi - \frac{2\pi}{3})(\frac{1}{2}) = \frac{\pi}{6}$, so $\sin \theta_1 < \frac{1}{2}$. Since $\mathcal{P}_X$ is a packing, $\|x - y\| \geq 2r$. The law of sines tells us that

$$\frac{\|x - y\|}{\sin \theta_1} = 2R$$

where R is the radius of the circumcircle of T . It follows that

$$2R > \frac{2r}{1/2} = 4r \implies R > 2r$$

Since the circumcircle of T contains no points of X other than x , y , and z , the closest points to the circumcenter are x , y , and z . Then, if we let c be the circumcenter, the ball $B(c, r)$ will not intersect $\mathcal{P}_X$ because it is a distance of at least $2r$ away from any other point in X . It follows that $\mathcal{P}_X$ is not saturated — a contradiction. $\square$

Lemma B. The *density* of a triangle $T = \{x, y, z\}$ in a Delaunay triangulation is the ratio

$$\delta(T) = \frac{\mu(B(x, r) \cap T) + \mu(B(y, r) \cap T) + \mu(B(z, r) \cap T)}{\mu(T)},$$

that is, it is the ratio of the volume of the packing that lies inside the triangle to the volume of the triangle itself. If $\mathcal{P}_X$ is a saturated packing with Delaunay triangulation D , then the density of any $T \in D$ is at most $\frac{\pi}{2\sqrt{3}}$.

Proof. From Lemma A, we know that the largest interior angle θ of T lies in the interval $[\frac{\pi}{3}, \frac{2\pi}{3}]$. It follows that $\sin \theta \geq \frac{\sqrt{3}}{2}$. Furthermore, since $\mathcal{P}_X$ is a packing, the distance between any two points in X is at least $2r$. Let the two sides adjacent to θ have lengths a and b . Then the area of T is

$$\mu(T) = \frac{1}{2}ab \sin \theta \geq \frac{1}{2} \cdot (2r) \cdot (2r) \cdot \frac{\sqrt{3}}{2} = r^2 \sqrt{3}$$

It is easy to see that the numerator of $\delta(T)$ is just

$$r^2 \cdot (\theta_1 + \theta_2 + \theta) = r^2 \cdot \frac{\pi}{2}$$

so we have that

$$\delta(T) \leq \frac{r^2 \cdot \pi/2}{r^2 \sqrt{3}} = \frac{\pi}{2\sqrt{3}}$$

as desired. $\square$

The result now follows easily: simply observe that the density of the packing $\mathcal{P}_X$ is bounded above by the supremum of the densities of the triangles in its Delaunay triangulation, which cannot exceed $\frac{\pi}{2\sqrt{3}}$ by Lemma B. Therefore, the honeycomb packing must be optimal. $\square$

Dimension 3 is equivalent to Kepler's conjecture, which we discussed previously. There are two natural ways to construct a maximally dense sphere packing in three dimensions. One is to stack translates of the honeycomb lattice that is optimal in two dimensions; the other is to stack translates of the integer lattice $(2r\mathbb{Z})^2$. The first construction is known as the hexagonal close-packed (HCP) lattice, and the second is known as the face-centered cubic (FCC) lattice. Perhaps surprisingly, both of these constructions give the same packing density, and this density is optimal. Hales' computer-assisted proof aimed to verify that no other packing could surpass this density, and relied on Tóth's discovery that a brute-force search of packings could be conducted by reducing the search space to a specific finite set.

The remaining two results, in dimensions 8 and 24, were proved by Maryna Viazovska in 2016. The densest sphere packing in dimension 8 is given by the E_8 lattice, which is defined as

$$\Lambda = \left\{ x : x \in \mathbb{Z}^8 \cup \left(\mathbb{Z} + \frac{1}{2} \right)^8, \sum_{i \in [8]} x_i \equiv 0 \pmod{2} \right\}$$

and the densest packing in dimension 24 is given by the Leech lattice (whose construction we will discuss later).

It is an interesting fact that all of the above packings are lattice packings. The best possible lattice packings for dimensions 4 through 7 are known, and it is conjectured that these packings are in fact the best possible packings in these dimensions.

3. LATTICES AND QUADRATIC FORMS

In this section, we motivate the study of sphere packings from the perspective of number theory. Given that Minkowski's geometry of numbers, spearheaded by results involving lattices in Euclidean space, had such strong connections to number theory, it is natural to expect that similar connections arise from the study of lattice packings. Indeed, this turns out to be the case.

For notational convenience, we will define $N(v) = \|v\|^2$ for all $v \in \mathbb{R}^d$. Furthermore, if Λ is a lattice, define $\det(\Lambda) = \text{covol}(\Lambda)^2$.

Let Λ be a lattice spanned by vectors $v_1, \dots, v_k \in \mathbb{R}^d$. The Gram matrix of $\{v_1, \dots, v_k\}$ is given by

$$G = V^\top V$$

where V is the matrix whose columns are v_i . It follows that

$$\det(\Lambda) = \det(G).$$

We now construct a relation between lattices and quadratic forms. Any element $x \in \Lambda$ can be written as

$$x = \sum_{i \in [k]} a_i v_i$$

where $a_i \in \mathbb{Z}$. Let $a = (a_1, \dots, a_k)$. Then

$$N(x) = N\left(\sum_{i \in [k]} a_i v_i\right) = \sum_{i, j \in [k]} a_i a_j v_i^\top v_j = a^\top V^\top V a = a^\top G a$$

If we consider $N(x)$ as a function $f(a_1, \dots, a_k)$, then f is a quadratic form (a homogeneous quadratic polynomial). Clearly, any lattice in $\mathbb{R}^d$ corresponds to a single quadratic form.

One natural application of this relation is to the theory of Diophantine equations (in particular, those of degree 2). A classical problem in number theory asks how many ways a given integer n can be written as the sum of four squares. Lagrange's four-square theorem asserts that this number, which we will call $s(n)$, is at least 1 for all n . In 1834, Jacobi proved the following result:

Theorem 3.1. *Let $n \in \mathbb{N}$. Then*

$$s(n) = 8 \sum_{\substack{m|n, \\ 4 \nmid m}} m.$$

We consider an approach to this problem that utilizes the connection between lattices and quadratic forms. It is not difficult to see that

$$f(a) = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

is the quadratic form resulting from the cubic lattice $\mathbb{Z}^4$ with basis equal to the standard basis of $\mathbb{R}^4$. Since $f(a) = N(x)$, to compute $s(n)$ it suffices to count how many $x \in \mathbb{Z}^4$ satisfy $N(x) = n$.

To compute this number, we consider the theta series of the lattice, defined by

$$\Theta(\Lambda; z) = \sum_{x \in \Lambda} q^{N(x)} = \sum_{n \in \mathbb{Z}} s(n) q^n$$

where $q = \exp(\pi i z)$, and the second equality follows from the fact that each x for which $N(x) = n$ adds a q^n term to the sum. Therefore, computing the theta series will allow us to find $s(n)$.

Since $N(x) = x_1^2 + \dots + x_4^2 = N(x_1) + N(x_2) + N(x_3) + N(x_4)$, we have that

$$\Theta(\mathbb{Z}^4; z) = \sum_{x \in \mathbb{Z}^4} q^{N(x_1) + \dots + N(x_4)} = \left(\sum_{x \in \mathbb{Z}} q^{N(x)} \right)^4 = \Theta(\mathbb{Z}; z)^4$$

and evaluating $\Theta(\mathbb{Z}; z)$ shows that

$$\Theta(\mathbb{Z}; z) = \sum_{m \in \mathbb{Z}} q^{m^2} = 1 + 2q + 2q^4 + 2q^9 + \dots$$

which is equal to $\theta(0; z)$, where θ is the Jacobi theta function.

We may then use the properties of this theta series to compute the coefficient of q^m in $\theta(0; z)^4$, which is equal to $s(m)$.

Next, we discuss connections between lattices and unimodular quadratic forms, which are an important object of study in number theory. We begin with some definitions.

Let Λ be a lattice in $\mathbb{R}^d$. The *dual lattice* of Λ is the set

$$\Lambda^* = \{x \in \mathbb{R}^d : \forall y \in \Lambda, x \cdot y \in \mathbb{Z}\}$$

In some sense, the dual of a lattice can be thought of as its inverse.

A lattice Λ generated by vectors $v_1, \dots, v_k \in \mathbb{R}^d$ is called *integral* if every entry of its Gram matrix G is an integer. It is easy to see that a lattice is integral if and only if it is contained within its dual.

A lattice Λ that is both integral and satisfies $\det(\Lambda) = 1$ is called a *unimodular lattice*. Unimodular lattices are exactly those lattices that are dual to themselves, so they are “highly symmetric”. Perhaps surprisingly, both the E_8 lattice and the Leech lattice (which solve the sphere packing problem in dimensions 8 and 24, respectively) are unimodular lattices.

Of course, a unimodular lattice defines a corresponding unimodular quadratic form. A unimodular lattice (and its corresponding quadratic form) is called *even* if all the diagonal entries of its Gram matrix are even. Even unimodular lattices have a variety of applications to coding theory, which we will discuss later. For the moment, we simply state the following interesting fact about even unimodular lattices, whose proof makes use of ideas from the geometry of numbers.

Theorem 3.2. *Even unimodular lattices of rank k exist if and only if $8 \mid k$.*

One might endeavor to enumerate all unimodular lattices of a certain dimension. Indeed, this has been done for dimensions up to at least 25. Notably, there is exactly one even unimodular lattice of dimension 8, the E_8 lattice, and 24 even unimodular

lattices of dimension 24, one of which is the Leech lattice. To verify that these enumerations are accurate, one can use the *Minkowski-Siegel mass formula*. We state the formula only in the case of even unimodular lattices; however, there exist similar results for odd unimodular lattices.

Theorem 3.3. *If Λ is a lattice, and let $\text{Aut}(\Lambda)$ be the group of automorphisms of Λ (where we view Λ as an abelian group). Let $\mathcal{E}_n$ denote the family of even unimodular lattices in n dimensions. Define*

$$M_n = \sum_{\Lambda \in \mathcal{E}_n} \frac{1}{|\text{Aut}(\Lambda)|}.$$

Then

$$M_{8k} = \frac{B_{2k}}{8k} \prod_{j=1}^{4k-1} \frac{B_j}{4j}$$

where B_i is the i -th Bernoulli number.

4. THE MINKOWSKI-HLAWKA THEOREM

Let $\mathcal{P}_X$ be an optimal packing of spheres of radius r in d dimensions. Without loss of generality, we can assume that $\mathcal{P}_X$ is saturated. Then we have the following useful result:

Theorem 4.1. *Let $\mathcal{P}_X$ be a saturated packing of spheres of radius r in d dimensions. Then $\Delta(\mathcal{P}_X) \geq 2^{-d}$.*

Proof. Since $\mathcal{P}_X$ is saturated, for any $y \in \mathbb{R}^d$, y is a distance less than r from some point in $\mathcal{P}_X$, which means it is a distance less than $2r$ from some point in X . Then consider the set

$$\mathcal{P}'_X = \bigcup_{x \in X} B(x, 2r)$$

and observe that $\mathcal{P}'_X = \mathbb{R}^d$. It follows that

$$\begin{aligned} \Delta(\mathcal{P}_X) &= \limsup_{R \rightarrow \infty} \frac{\mu(B(0, R) \cap \mathcal{P}_X)}{\mu(B(0, R))} \\ &= \limsup_{R \rightarrow \infty} \frac{\mu(B(0, R) \cap \mathcal{P}_X)}{\mu(B(0, R) \cap \mathcal{P}'_X)} \\ &\geq \frac{\mu(B(x, r))}{\mu(B(x, 2r))} \\ &= 2^{-d} \end{aligned}$$

as desired. $\square$

This is, however, a very loose bound; 2^{-d} becomes incredibly small as d grows large. Therefore, it is natural to ask whether we can do better. The following theorem due to Minkowski and Hlawka shows that we can; however, the improvement offered is not particularly significant.

Theorem 4.2. *For all $d > 1$, there exists a lattice $X \subset \mathbb{R}^d$ such that $\mathcal{P}_X$ satisfies $\Delta(\mathcal{P}_X) \geq \zeta(d) \cdot 2^{-(d-1)}$, where ζ is the Riemann zeta function.*

The proof of this theorem is somewhat involved, so we omit it for brevity; however, we show the following similar result using a clever probabilistic proof that can be found in [2] (with the notation modified slightly for consistency), and is strongly reminiscent of the derivation of Minkowski's theorem. Note that this theorem is weaker in that it gives a slightly looser bound (although they are asymptotically equivalent, since $\zeta(d) \rightarrow 1$ as $d \rightarrow \infty$), but stronger in that it is applicable to bodies other than spheres.

Theorem 4.3. *Let B be a bounded, convex, centrally symmetric set in $\mathbb{R}^d$. Let Δ be the maximum density of a packing of B in $\mathbb{R}^d$. Then*

$$\Delta > 2^{-(d-1)}.$$

Proof. The key idea is to construct a random lattice and show that it gives a packing with high probability.

Since scaling does not change the density of a packing, we choose an arbitrary $\varepsilon > 0$ and rescale the body B such that $\mu(B) = 2 - \varepsilon$. Denote by B_z the set of points in B whose last coordinate is z . Using a Riemann sum to approximate the measure of B , we obtain that as $\gamma \rightarrow 0$,

$$\sum_{m \in \mathbb{Z}} \mu(B_{m\gamma}) \cdot \gamma \rightarrow \mu(B).$$

Let K be an integer such that

$$\sum_{m \in \mathbb{Z}} \mu(B_{mK^{-(d-1)}}) \cdot K^{-(d-1)} < 2$$

and B lies entirely within $(-\frac{K}{2}, \frac{K}{2})^d$ (such an integer must exist as a consequence of the previous limit).

We define d vectors that determine the fundamental polytope of a lattice in $\mathbb{R}^n$. For $i \in [d-1]$, let v_i be the vector with i -th coordinate equal to K and all other coordinates equal to 0. Then let $z_1, \dots, z_{d-1}$ be chosen uniformly and independently at random from the interval $[0, K) \subset \mathbb{R}$, and define

$$v_d = (z_1, \dots, z_{d-1}, K^{-(d-1)}).$$

Let Λ be the lattice spanned by $\{v_i\}$. Consider an arbitrary $x \in \Lambda$; then as a result of our construction, for $i \in [d-1]$, the coordinate x_i can be written as $m_i z_i + m_d K^{-(d-1)}$, where $m_i, m_d \in \mathbb{Z}$.

Define $\theta(x)$ to be the unique value of $x' \in (-\frac{K}{2}, \frac{K}{2}]$ that satisfies $x - mK = x'$, where $m \in \mathbb{Z}$. That is, θ translates a given coordinate to a coordinate lattice point within the cube that bounds B . For each $m \in \mathbb{Z}$, we define the *bad event* A_m to be the event that there exist $(m_1, \dots, m_{d-1}) \neq \mathbf{0}$ for which

$$m_1 v_1 + \dots + m_{d-1} v_{d-1} + m v_d \in B.$$

We wish to show that the probability that no A_m occurs is greater than 0, or equivalently that B contains no point in the lattice other than the origin.

A_m occurs only if

$$(\theta(mz_1), \dots, \theta(mz_{d-1}), mK^{-(d-1)}) \in B$$

because the $m_i K$ terms vanish when θ is applied. This means it occurs only if

$$(\theta(mz_1), \dots, \theta(mz_{d-1})) \in B_{mK^{-(d-1)}}$$

and since the z_i are distributed uniformly over $[0, K)$, the probability that A_m occurs is

$$\mathbb{P}[A_m] \leq \frac{\mu(B_{mK^{-(d-1)}})}{\mu([0, K)^{d-1})} = \frac{\mu(B_{mK^{-(d-1)}})}{K^{d-1}}$$

Furthermore, note that when $m = 0$, $\mathbb{P}[A_m] = 0$ because any nontrivial choice of $(m_1, \dots, m_{d-1})$ will cause at least one coordinate to have absolute value at least K , and every point of B lies inside $(-\frac{K}{2}, \frac{K}{2})$.

Then the union bound gives that

$$\begin{aligned} \mathbb{P}\left[\bigvee_{m \in \mathbb{Z}} A_m\right] &\leq \sum_{m \in \mathbb{Z}} \mathbb{P}[A_m] \\ &= \mathbb{P}[A_0] + \sum_{m > 0} \mathbb{P}[A_m] + \sum_{m < 0} \mathbb{P}[A_m] \\ &= \sum_{m > 0} \mathbb{P}[A_m] \quad (B \text{ is centrally symmetric}) \\ &\leq \sum_{m > 0} K^{-(d-1)} \mu(B_{mK^{-(d-1)}}) \\ &\leq \frac{1}{2} \cdot \sum_{m \in \mathbb{Z}} K^{-(d-1)} \mu(B_{mK^{-(d-1)}}) \\ &\leq \frac{1}{2} \cdot \mu(B) < 1 \end{aligned}$$

so it follows that there exists a choice of $\{v_i\}$ such that the lattice generated by those $\{v_i\}$ does not intersect B at any point except the origin.

Now it remains only to show that Λ can be turned into a packing. Let $X = 2\Lambda$; we claim that $\mathcal{P} = \{B + x : x \in X\}$ is a packing of copies of B in $\mathbb{R}^d$. Assume for the sake of contradiction that there exists some point $z \in \mathbb{R}^d$ that could be written as

$$z = 2\lambda_1 + b_1 = 2\lambda_2 + b_2$$

where $\lambda_1, \lambda_2 \in \Lambda$, $b_1, b_2 \in B$, and $(\lambda_1, b_1) \neq (\lambda_2, b_2)$. Then

$$\lambda_1 - \lambda_2 = \frac{1}{2}(b_2 - b_1).$$

Since Λ is a lattice (hence an additive group), $\lambda_1 - \lambda_2 \in \Lambda$. Since B is centrally symmetric and $b_1 \in B$, it follows that $-b_1 \in B$; and since B is convex, $\lambda_1 - \lambda_2 = (b_2 + (-b_1))/2$ is also in B . Then $\lambda_1 - \lambda_2 \in B \cap \Lambda$, and by the first part of the proof it follows that $\lambda_1 - \lambda_2 = \mathbf{0}$. This means $\lambda_1 = \lambda_2$ and $b_1 = b_2$ – a contradiction. Therefore $\mathcal{P}$ is a packing. Note that there is a bijection between copies of B in the packing and fundamental polytopes of X . Therefore, the density of the packing is the ratio of the measure of B to the measure of a fundamental polytope of X ; that is,

$$\Delta(\mathcal{P}) = \frac{\mu(B)}{\text{covol}(X)} = \frac{\mu(B)}{\text{covol}(2\Lambda)} = \frac{\mu(B)}{2^d \text{covol}(\Lambda)}$$

and since $\text{covol}(\Lambda) = 1$ (this can be seen by computing the determinant of the matrix V whose columns are v_i by expanding cofactors along the first column), we have that

$$\Delta(\mathcal{P}) = \frac{\mu(B)}{2^d} = \frac{2 - \varepsilon}{2^d}$$

Since the initial choice of $\varepsilon > 0$ was arbitrary, it follows that

$$\Delta \geq \frac{2}{2^d} = 2^{-(d-1)}$$

as desired. $\square$

5. CODING THEORY

We conclude our discussion of sphere packing with a few applications to coding theory.

First, we shall discuss the problem of decoding messages sent over a noisy channel. The setup is simple: we wish to transmit a continuous signal (say, a speaker's voice during a phone call) over some medium (a telephone wire, for example) that may be unreliable, in that it can alter the data sent over it in some nondeterministic way.

The sampling theorem, due to Whittaker, Nyquist, and Shannon, is an important result in digital signal processing which states the following:

Theorem 5.1. *Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be a continuous function whose Fourier transform is 0 outside of the interval $[-M, M]$. Assume $f(t)$ is transmitted over a noiseless channel; then f can be reconstructed perfectly by observing only the values*

$$f\left(\frac{i}{2M}\right) \quad (i \in \mathbb{Z}).$$

We also give the following important definition:

Definition 5.2. The *power* of a signal $f : \mathbb{R} \rightarrow \mathbb{R}$ transmitted over the interval $[0, T]$ is defined as

$$P_f = \frac{1}{T} \int_0^T f(t)^2 dt$$

Consider a signal $g : \mathbb{R} \rightarrow \mathbb{R}^n$ that we wish to transmit over a channel that perturbs its input by applying some noise $\delta = (\delta_1, \dots, \delta_n)$, where each δ_i is sampled independently from $\mathcal{N}(0, \sigma^2)$ (we treat σ^2 as a constant). Assume that the channel only transmits frequencies in the interval $[-M, M]$ (so g will be limited to the same range of frequencies). From the sampling theorem, we know that we can reconstruct g by observing the true value of g at every point in the set $\{i/(2M) : i \in \mathbb{Z}\}$. However, due to the noise added by the channel, we cannot guarantee that the raw values we observe are truthful. Therefore, we construct an error-correcting code that allows us to determine the true value of g at each point in time with high probability. To do this, we add the assumption that our signal takes on values in some finite set $\mathcal{C} \subset \mathbb{R}^d$ of codewords. When a word in $\mathbb{R}^n$ is received, we use minimum distance decoding to associate it to a codeword in $\mathcal{C}$.

Then each codeword transmits $\log_2 |\mathcal{C}|$ bits of information; if this transmission occurs over the interval $[0, T]$, then the average *rate* of information transmission is

$$R_f = \frac{1}{T} \log_2 |\mathcal{C}|$$

bits per second.

The following theorem of Shannon and Hartley gives a sharp upper bound on this transmission rate.

Theorem 5.3. *Let $f : \mathbb{R} \rightarrow \mathbb{R}^n$ be a continuous function transmitted over the interval $[0, T]$ across a medium with additive Gaussian noise with mean 0 and standard deviation σ^2 . Assume that the Fourier transform of f is zero outside of $[-M, M]$, and the power of f is P_f . Then the rate of transmission satisfies the following bound:*

$$R_f \leq R_{\max} = M \log_2 \left(1 + \frac{P_f}{\sigma^2} \right)$$

and for any $\varepsilon, \delta > 0$, there exists a code $\mathcal{C}$ with transmission rate $R_f = R_{\max} - \varepsilon$ and probability of decoding error at most δ .

The proof of this theorem is quite involved, so we do not reproduce it. However, it is natural to think that sphere packing bounds might be helpful in the proof. In particular, we want to construct codes in $\mathbb{R}^n$ such that minimum distance decoding succeeds with high probability. If we associate to each codeword the set of points in $\mathbb{R}^n$ that will be decoded to it, the resulting partition of $\mathbb{R}^n$ is a Voronoi diagram – a natural extension of sphere packing. As such, finding an efficient minimum distance decoding scheme is roughly equivalent to finding a good packing of spheres of radius r (where r is increasing in σ^2) into a larger sphere of radius R (where R is increasing in P_f). Indeed, a very similar idea is used in the proof of the Hamming bound, which gives a similar result for codes over finite sets A^d .

The next application we will consider is binary Golay codes. Marcel Golay introduced these codes in a remarkably short paper published in 1949, but their applications have been far-reaching.

We first describe how to construct the Golay codes. Consider the following two matrices:

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \quad H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

These matrices are parity-check matrices for two Hamming codes $\mathcal{C}_1$ and $\mathcal{C}_2$; that is, some $v \in \mathbb{F}_2^8$ is in $\mathcal{C}_1$ if and only if $H_1 v = 0$, and similarly for $\mathcal{C}_2$. Then the *extended binary Golay code* is the set

$$\mathcal{G} = \{(a + c \mid b + c \mid a + b + c) : a, b \in \mathcal{C}_1, c \in \mathcal{C}_2\}$$

where $\mid$ denotes concatenation of bit strings.

The extended binary Golay code $\mathcal{G}$ is a 12-dimensional subspace of the vector space $\mathbb{F}_2^{24}$ which has a number of interesting and useful properties. For instance, for any $x, y \in \mathcal{G}$, the Hamming distance $H(x, y)$ is at least 8, and therefore $\mathcal{G}$ can detect and correct 3-bit errors. Furthermore, $\mathcal{G}$ is its own dual, where the dual of a code $\mathcal{C} \subseteq A^d$ is defined to be

$$\mathcal{C}^\perp = \{x \in A^d : \langle x, y \rangle = 0 \text{ for all } y \in \mathcal{C}\}$$

Deleting any bit from the extended binary Golay code gives the (regular) binary Golay code $\mathcal{G}'$, which is a 12-dimensional subspace of $\mathbb{F}_2^{23}$ that is a *perfect code* – this means that

$$\bigcup_{x \in \mathcal{G}'} B(x, 3) = \mathbb{F}_2^{23}$$

where $B(x, 3)$ is the set of points whose Hamming distance from x is at most 3. Equivalently, the best possible sphere packing of $\mathbb{F}_2^{23}$ under the Hamming metric has density 1.

Perhaps the most astonishing fact about the extended binary Golay code is that it can be used to construct the Leech lattice (and in fact, the two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ that we defined in the construction of $\mathcal{G}$ can be used to construct the E_8 lattice as well)!

Up to a constant scale factor, the Leech lattice is the lattice Λ consisting of all vectors $x = (x_1, \dots, x_{24}) \in \mathbb{Z}^{24}$ such that the following properties hold:

1. For all $i \in [24]$,

$$\sum_{j \in [24]} x_j \equiv 4x_i \pmod{8}.$$

2. For each $i \in [4]$, the vector $m = (m_1, \dots, m_{24})$ where $m_j = \mathbb{1}\{x_j \equiv i \pmod{4}\}$ is a word in $\mathcal{G}$.

6. CONCLUSION

We hope this has served as a useful introduction to the study of sphere packings and their applications. A majority of modern research on sphere packings, especially in the context of number theory, makes use of the theory of modular forms, which the author is not particularly familiar with; however, we have attempted to motivate the topic in other ways, particularly using combinatorial and geometric applications. The interested reader is encouraged to look at [3] for a much more detailed treatment of many of the topics discussed in this paper.

REFERENCES

1. Chang, H.-C., Wang, L.-C.: A Simple Proof of Thue's Theorem on Circle Packing, <https://arxiv.org/abs/1009.4322>
2. Alon, N., Spencer, J.H.: The probabilistic method. John Wiley & Sons (2016)
3. Conway, J.H., Sloane, N.J.A.: Sphere packings, lattices and groups. Springer Science & Business Media (2013)
4. Viazovska, M.: The sphere packing problem in dimension 8. *Annals of Mathematics*. 185, (2017). <https://doi.org/10.4007/annals.2017.185.3.7>
5. Serre, J.-P.: A course in arithmetic. Springer Science & Business Media (2012)

