Properties of the Leech Lattice

Austin Roberts
University of Puget Sound

April 14, 2006

Abstract

This paper catalogues and describes the properties of the Leech lattice and gives a basic introduction to the fields where it emerges. Topics include sphere packing, error-correcting codes, and simple groups, along with some related topics such as kissing numbers and designs. The focus is primarily geometric and combinatorial. The discussion is aimed towards an advanced undergraduate student though it is understood to be more meaningful with some prior exposure to the covered topics.

1 Introduction

This paper catalogues and describes the properties of the Leech lattice and gives a basic introduction to the fields where it emerges. Topics include sphere packing, error-correcting codes, and simple groups, along with some related topics such as kissing numbers and designs. The discussion is aimed towards an advanced undergraduate student, though it is understood to be more meaningful with some prior knowledge of the covered topics.

The Leech lattice is a remarkable mathematical object. For all of the time and thought that went in to its creation, it is a surprisingly simple geometric object, that happens to be of profound importance in mathematics. The topic is made all the more interesting with an understanding of how recently much of it has come about. The discovery of the Leech lattice was heavily dependent on error-correcting codes, which were not established until the late 1940's, and by the late 1970's J. H. Conway had found three new simple groups within the automorphism group of the lattice. This paper also includes work as recent as 2004.

It is difficult to encompass all of this work in a narrative fashion. There is no simple choice of where to begin because each topic is dependent on another for proof techniques and explanations. This paper chooses to begin by presenting the Leech lattice in one of its purest forms, as a particularly nice generator matrix. Though at first unmotivated, all of the necessary information about the Leech lattice lies in this 24×24 matrix, and so we take the liberty of investigating it before understanding how it was discovered.

Lastly, it should be remembered that almost all fields discussed are the topics of ongoing work. All problems associated with sphere packing have proven very difficult, as have many of those associated with coding. Simple groups, although totally enumerated, continue to be the source for much ongoing work in group theory. We are in the middle of exciting work. The results contained here are milestones, but also stepping stones. We are thus discussing matters of importance and wide application that are all the richer for their relevance.

$$\left[\begin{array}{cccccccc|cccccccc|cccccccc}
8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 2 & 2 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 \\
-3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right]$$

A matrix representation of the Leech lattice (lines included for ease of viewing).

2 Sphere Packing, Kissing, and Covering

In this section we introduce the context in which the Leech lattice was first discovered and describe some of the lattice's basic properties. Some calculations, such as the proof of the Leech lattice's kissing number, are postponed until codes and designs are discussed in Section 3.

2.1 The Sphere Packing Problem

When Leech first discovered his lattice, he was searching for a solution to the sphere packing problem in 24 dimensions. The problem dates back to Thomas Harriot in the late 1590's, more famously to Johaness Kepler in the beginning of the 17th century, and eventually to a review that Gauss wrote in 1831. It asks, is there a denser arrangement of equally sized spheres than the standard way of stacking oranges? This arrangement, known as the *face-centered cubic lattice* (fcc lattice), was not proven to be optimal until 1998 (see [14] for the current proof);

however, the heavy dependence of this proof on computers is still controversial. The modern version of the problem is generalized to n dimensions. The goal of sphere packing is to find the packing, in a given number dimensions, which achieves the highest possible density Δ, defined as the proportion of space taken up by spheres. Though the formal definition of density is rarely used, we provide it here along with a definition of radius.

Definition 1 (Radius) *Given a set of points P in $\mathbb{R}^n$, the* packing radius *of P is*

$$\rho = \min(\{\tfrac{1}{2} \cdot \text{dist}(p_i, p_j) \,|\, p_i, p_j \in P, i \neq j\})$$

where dist *is the standard Euclidean distance between two points.*

It is important to notice that the packing radius, and in fact, all other properties are entirely determined by the sphere centers. We will assume that ρ is positive and will often use the term *arrangement*, instead of set, to imply that $\rho \neq 0$.

Definition 2 (Density) *Given a arrangement of points P in $\mathbb{R}^n$ with packing radius ρ, the* packing density *of P is*

$$\Delta(P) = \underset{p_i \in P}{\text{ave}} \left(\frac{(\text{vol}(\{x \in \mathbb{R}^n \,|\, \text{dist}(x, p_i) \leq \rho\})}{\text{vol}(\{x \in \mathbb{R}^n \,|\, \text{dist}(x, p_i) \leq \text{dist}(x, p_j) \; for\, all \; j \neq i\})} \right)$$

where ave *is the average over a set and* vol *is the n-dimensional volume.*

In practice, finding the volume of the broad sets in the definition of Δ is often bypassed by taking advantage of symmetries within an arrangement rather than considering all of n-dimensional space.

The process of arranging spheres in n dimensions is less than intuitive, but we may begin to understand by looking in lower dimensions. The sphere packing problem takes place in Euclidean space, $\mathbb{R}^n$ and so we define a sphere as the set of points within a given distance from a central point. In the 1-dimensional case a 1-sphere is merely a line segment within the Euclidean space consisting of a single line (see Fig.1).

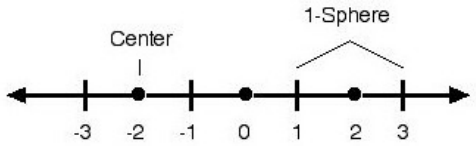


Figure 1: The optimal packing in one dimension

If we give our spheres a radius of one unit and place the center of the spheres on the even integers of a number line marking off the distances of E^1, then it is easy to see that we can cover the entire space, achieving 100% density. The scale of this arrangement, as with all arrangements, is strictly a matter of convenience and causes no difference to the density or other traits that we will examine.

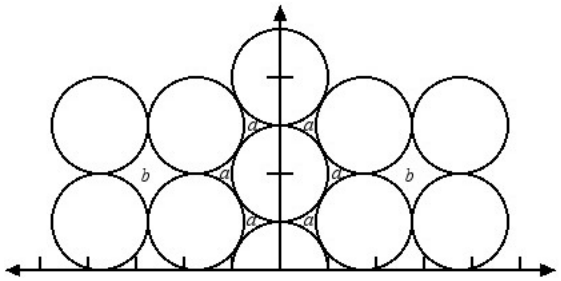


Figure 2: A 2-dimensional packing, shallow and deep holes marked a and b respectively.

The odd numbered coordinates in this example are called *holes*, because they are the points farthest from sphere centers. Points at an absolute maximum distance from the nearest center are termed *deep holes* and those at only local maximums are termed *shallow holes* (see Fig. 2).

In two dimensions, the optimal sphere packing is known as the hexagonal lattice (see Fig. 3).

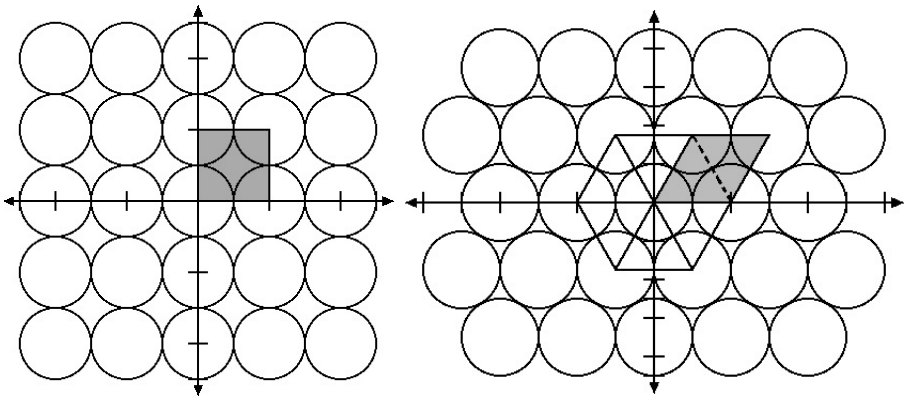


Figure 3: Lattices with shaded fundamental parallelotopes, hexagonal lattice on right.

Like the Leech lattice or the fcc lattice, it is termed a *lattice* because it satisfies the following definition.

Definition 3 (Lattice) *An arrangement of points P in $\mathbb{R}^n$ is said to be a* lattice *if $(p_i - p_j) \in P$ for all $p_i, p_j \in P$ where subtraction is the standard component-wise vector difference.*

A lattice is simply an arrangement where the origin is a center and given the coordinates of any two centers, u and v, there are also centers at $u + v$ and $u - v$ (the latter is actually sufficient). Given any n-dimensional lattice, it is possible to find n vectors, describing n centers, that generate the entire lattice through all possible combinations of repeated addition and subtraction of these vectors ([28]). Such a set of vectors is termed a *basis* for the lattice. Using different terminology, lattices are integer linear combinations of the n vectors of a basis. In the case of the hexagonal lattice and the fcc lattice, the most apparent bases are

$$\{(2,0),(1,\sqrt{3})\} \text{ and } \{(2,0,0),(1,1,0),(0,1,1)\}.$$

Instead of writing a basis as a set, the vectors are often written as the rows of a matrix. A matrix whose rows are defined by the vectors of a lattice basis is termed a *generator matrix* for that lattice. The hexagonal lattice and the fcc lattice have the generator matrices

$$\begin{bmatrix} 2 & 0 \\ 1 & \sqrt{3} \end{bmatrix} \text{ and } \begin{bmatrix} 2 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Generating matrices are not unique, but for the purposes of sphere packing two matrices that generate the same lattice are considered equivalent. Generator matrices are useful for a number of reasons. In particular, we can use a generator matrix to find the density of its lattice packing.

The set of vectors that can be created by adding the row vectors of a generator matrix, using each vector at most once, forms the vertices of a shape called a *fundamental parallelotope*, or less precisely, a *fundamental region*, a building block that can be repeated, or tiled, over all of $\mathbb{R}^n$ without overlapping (see Fig. 3). Furthermore, the fractions of sphere volumes within the fundamental region will always add up to exactly one whole sphere (the proof of this is simple but tedious). Using this symmetry, the density of a lattice packing simplifies to the volume of a sphere divided by the volume of the fundamental parallelotope.

For an n-dimensional lattice L_n with generator matrix G, the volume of the fundamental parallelotope is equal to the determinant of G ([9]). The volume of an n-dimensional sphere of radius 1 is denoted V_n, and the volume of a sphere of radius ρ is

$$\rho^n V_n.$$

The density of an n-dimensional lattice packing L_n with generator matrix G is thus

$$\Delta(L_n) = \frac{\text{The Volume of a Sphere}}{\text{The Volume of a Fundamental Region}} = \frac{\rho^n V_n}{\det(G)}$$

It can be shown by induction on n that

$$V_n = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)} = \frac{\pi^{n/2}}{(n/2)!} = \frac{2^n \pi^{((n-1)/2))!}}{n!}$$

where Γ is the gamma function, the first expression holds for all n, the second is easier to use with even n, and the last is easiest to use with odd n.

We can demonstrate this process by calculating the density of the Leech lattice, denoted Λ_{24}, based on the generator matrix G given in the introduction. By inspection, we find that the minimum length between sphere centers is $4\sqrt{2}$ (this will be shown in Section 3.3), giving each sphere a radius of $2\sqrt{2}$, so we need only insert $2\sqrt{2}$ and our particular G into the density equation:

$$\Delta(\Lambda_{24}) \;=\; \frac{(2\sqrt{2})^{24}\pi^{n/2}}{(n/2)!\det(G)} \;=\; \frac{\pi^{12}}{12!} \;\approx\; 0.001930$$

This is the highest known density in 24 dimensions and was proven in [7], [8] to be optimal among 24-dimensional lattices.

The density of the Leech lattice can be better understood through its *center density*.

Definition 4 (Center Density) *Given an arrangement of points P in $\mathbb{R}^n$, the* center density *of P is defined as*

$$\delta(P) = \Delta(P)/V_n$$

If we scale a packing so that $\rho = 1$, the center density is equal to the average number of sphere centers per unit volume in $\mathbb{R}^n$. In the case of the Leech lattice, $\delta(\Lambda_{24}) = \Delta(\Lambda_{24})/V_n = 1$, which is the highest center density for any packing of dimension less than 30.

Not only is the Leech lattice an excellent packing in 24 dimensions, it contains copies of excellent packings in lower dimensions as well. To explain these sublattices, we must explain what it means for the Leech lattice to be a *laminated lattice*, denoted as Λ_n in n dimensions. Λ_n is defined inductively as the densest lattice containing Λ_{n-1} in a hyperplane (or a cross-section), where Λ_0 is the point that is $\mathbb{R}^0$. In other words, we can create the laminated lattices by starting with Λ_0, evenly layering copies of it in $\mathbb{R}^1$ to make the perfect one dimensional lattice Λ_1, then layering this lattice in $\mathbb{R}^2$ to make the hexagonal lattice, and so on, choosing the best packing possible in each successive dimension until we get to the Leech lattice and beyond. The densest known lattice packings for $n \leq 10$ and $14 \leq n \leq 24$ are laminated lattices. Thus, the Leech lattice contains all of these best-known lattices as lesser dimensional layers. The specific sequence of laminations is described in [17]-[20]. It should be noted though, that many laminated lattices were discovered and then classified as Λ_n rather than being discovered through a laminating process.

There is another important sequence of lattices, often defined as sections of Λ_{24}, denoted as $K_0, K_1, \ldots, K_{24}$ ([17], [18], and [20]). For $7 \leq n \leq 17$, these are not laminated lattices. The packings K_{11}, K_{12}, and K_{13} are the densest known lattice packings for their dimensions. Thus, the Leech lattice contains all of the densest known lattice packings for $n \leq 24$.

It is important to realize that not all of the densest packings are lattice packings. The densest known packings in dimensions 10, 11, 13, 18, 20, 22, as well as many higher dimensions, are described by non-lattice packings. However, lattice packings share many symmetries that make them easier to work with.

The sphere packing problem in general is unsolved. Packings have only been proven optimal in dimensions one through three; though several upper bounds are known (see [5], [6], [9], [12], and [21]).

2.2 Kissing Numbers

In 1694 Isaac Newton and David Gregory had a famous argument about how many billiard balls could kiss ("contact" to non-billiards-playing mathematicians) a central billiard ball at once.

Newton believed the answer to be 12, as demonstrated by the fcc lattice in Section 2.1, while Gregory thought there might be a way of fitting 13. Newton was eventually proved correct in the nineteenth century (see [16]).

The modern problem is a generalization to n dimensions. It asks, for each natural number n, what is the highest possible kissing number, denoted τ, of an arrangement of n-spheres? Formally, we define the kissing number of an arrangement as follows:

Definition 5 (Kissing Number) *Given an arrangement of points P in $\mathbb{R}^n$ with packing radius ρ, the* kissing number *of p is defined as*

$$\tau(P) = \max_{p_i \in P}(\, |\{p_j \, | \, p_j \in P, \mathrm{dist}(p_i, p_j) = \rho\}| \,)$$

The kissing number increases with each dimension and is not always described by the best sphere packing, though good sphere packings usually have high kissing numbers. It is not necessary for the highest kissing numbers be achieved by lattices, though much more is known about kissing numbers for lattices. In lattices, the kissing number of every sphere is equal since the arrangement around every sphere is identical.

Finding the maximum τ for a given n, like the sphere packing problem, has proven to be quite difficult. There are only five known solutions. In one-dimensional space the answer is obviously two. In two-dimensional space the solution is six, as demonstrated by the hexagonal lattice. In three dimensions the answer, as mentioned before, is 12. It is unknown whether the solution in four dimensions is 24 or 25. Eight dimensions, however, has a somewhat simple solution of 240, as created by the E_8 lattice (see [24], [21], or [10]).

The only other known solution is satisfied by the 196,560 kisses of the 24-dimensional Leech lattice. We will wait until Section 3.5 to verify this number. The kissing number of the Leech lattice is exactly the upper bound given in [24] and thus must be the solution for τ_{24}. Furthermore, it has been proven that Λ_{24} is the only arrangement (up to isometry) to achieve this solution ([1], [11]). It should be noted that these helpful upper bounds were unknown in 1967, when the Leech lattice first appeared in print. Most of the Leech lattice's optimizations were proven decades later.

2.3 The Covering Problem

The covering problem asks, what is the most efficient covering of Euclidean n-space with equally sized overlapping n-spheres? In other words, what arrangement of equally sized n-dimensional spheres can take up all of the space in n-dimensions with the least amount of wasted overlapping. This is called minimizing the *thickness*, Θ, of a covering. To deal with thickness concretely, we introduce the following two definitions.

Definition 6 (Covering Radius) *Given an arrangement of points P in $\mathbb{R}^n$, the* covering radius *of P is defined as*

$$R = \max_{x \in \mathbb{R}^n} \min_{p \in P} \mathrm{dist}(x, p)$$

The covering radius is intentionally defined so that R is the smallest possible radius which still allows the spheres of an arrangement to cover $\mathbb{R}^n$. R is also equal to the distance between a deep hole and the nearest sphere center.

Definition 7 (Thickness) *Given an arrangement of points P in $\mathbb{R}^n$ with covering radius R, the thickness of P is defined as*

$$\Theta(P) = \underset{p_i \in P}{\text{ave}} \left(\frac{(\text{vol}(\{x \in \mathbb{R}^n \mid \text{dist}(x, p_i) \leq R\})}{\text{vol}(\{x \in \mathbb{R}^n \mid \text{dist}(x, p_i) \leq \text{dist}(x, p_j)\ \forall j \neq i\})} \right)$$

The thickness of a covering is defined by the ratio of the sum of the volumes of the spheres to the volume of space. Coverings generally have a certain amount of symmetry that makes the thickness easier to calculate, though it is often still quite difficult. Lattices have a guaranteed symmetry via their bases. For lattices, we can define thickness in the same way as we did density:

$$\Theta(L_n) = \frac{\text{The Volume of a Sphere}}{\text{The Volume of a Fundamental Region}} = \frac{R^n V_n}{\det(G)}$$

To give an idea of the difficulty of this problem, the only coverings that have been proven optimal are in one and two dimensions. The solutions to the first two dimensions are the same as the sphere packing problem, but for three dimensions the *body-centered cubic lattice* (or *bcc* lattice) is a better covering than the face-centered cubic lattice. As with many covering lattices, the bcc lattice is the *dual* of the same dimensional packing lattice.

Definition 8 (Dual) *Given a lattice L_n, the* dual *of L_n is defined by*

$$L_n^* = \{x \in \mathbb{R}^n : x \cdot u \in \mathbb{Z} \quad \text{for all } u \in L_n\}$$

where $x \cdot u$ is the inner product (dot product) of x and u.

For example, the fcc lattice and the bcc lattice, represented by,

$$\begin{bmatrix} 2 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

are duals. Almost all of the thinnest lattice coverings known are the duals of the densest lattice packings known. The only lattices to be both the thinnest known and the densest known for $n \leq 25$ are $\Lambda_0, \Lambda_1, \Lambda_2$ (the hexagonal lattice), $E_8 = \Lambda_8$, and Λ_{24}. In all four cases the lattices, when represented so that $|\det(G)| = 1$, satisfy the definition of being dual with themselves and are termed *self-dual* or *unimodular* (we will assume a rescaling so that $|\det(G)| = 1$ whenever inner products or minimal norms are discussed). The Leech lattice is also an *even* unimodular lattice.

$$\Lambda_{24} = \{x \in \mathbb{R}^n : x \cdot u \in 2\mathbb{Z} \quad \text{for all } u \in \Lambda_{24}\}.$$

This is equivalent to saying that the *minimal norm* of any nonzero vector $x \in \Lambda$, given by $N(x) = x \cdot x$, is a multiple of 2. In fact, the Leech lattice is sometimes termed *doubly even* because the minimal norm of any vector is 4. Not only is Λ_{24} the best covering, it is an exceptionally thin covering in comparison to solutions in other dimensions. The Leech lattice has 23 different types of deep holes at a distance of 4 from the closest center (in our representation). The density is thus

$$\Theta(\Lambda_{24}) = \frac{4^n \pi^{n/2}}{(n/2)!\det(G)} = \frac{2^{12}\pi^{12}}{12!} \approx 7.9035$$

Where the best covering in 23 dimensions has a thickness of about 53.0, the Leech lattice has a thickness of about 7.9. This is nothing short of remarkable!

Because the Leech lattice creates such an efficient covering, it has been used to create the thinnest coverings for higher dimensions. By using the Leech lattice as blocks in n-dimensional generator matrices for large n, [12] constructed coverings with the least known density of

$$\Theta_n \ \leq \ 2^{0.085n}$$

3 Error-Correcting Codes, Designs, and the Creation of the Leech Lattice

The story of the Leech lattice would be a rather short one if it were contained only within the realm of sphere packing. Over the last century a number of topics have become intertwined with sphere packing and are greatly relevant to the study of the Leech lattice. The first of these fields that we will explore is error-correcting codes. It was through error-correcting codes that the Leech lattice was first discovered, and it is through the same codes that we are able to decipher its properties.

3.1 Hamming and the Basics of Error-Correcting Codes

The theory of error-correcting codes is a relatively new one, only emerging in the 1940s when the work of famous mathematicians like Richard Hamming, Claude Shannon, and Marcel Golay redefined digital communication and helped make the computer age possible. The theory concerns itself with the best ways to send a message over noisy channels, where errors and mistakes can occur, while maintaining the accuracy of the message. We will focus on binary codes, made up of strings of 0's and 1's. Each digit will be considered independently modulo 2.

Definition 9 (Binary Code) *A* binary code *of length n is a set of binary strings of length n, called* codewords.

The definition of a code is intentionally broad. It is only within the context of error correction that we will distinguish between 'good' and 'bad' codes.

Error correction is best explained with an example. Over a digital medium we might want to send the message 101. We want to make sure the message is received, so we send it three

times in a row as 101101101. Due to some interference, the message is received incorrectly as 100101110. All three copies can then be compared, and we can keep the values for each of the three digits that occurs most frequently. We correct the errors back to 101101101 and then decode the message as 101. The process can be illustrated as

$$\text{Message} \rightarrow \text{Encoding} \rightarrow \text{Transmission/Errors} \rightarrow \text{Error Correction} \rightarrow \text{Decoding}$$

We can go even further and describe our code with a *generator matrix*:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Generator matrices are used to describe the set of codewords as well as to encode messages. We can use matrix multiplication to encode the three digit message $[x_1\ x_2\ x_3]$ as follows.

$$\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & x_3 & x_1 & x_2 & x_3 & x_1 & x_2 & x_3 \end{bmatrix}$$

This code, call it A, is a very simple type of error-correcting code called a *repetition code*. A has 2^3 codewords defined by the repetitions of the first three digits. The first three digits of a codeword in A are the *message digits* and are followed by six *check digits* making up a 9-block, or 9-vector. A code of length n with k message digits is termed an (n, k) code. We then say that A is a $(9, 3)$ code.

Only certain predetermined binary strings are classified as codewords. In general, we will call a binary string a block. We will measure the difference between two blocks by their *weight* and their *Hamming distance*.

Definition 10 (Weight) *Given any block b, the* weight *of b, denoted* w(b)*, is the number of nonzero digits in b.*

For instance, the weight of 10110 is $w(10110) = 3$.

Definition 11 (Hamming Distance) *Given any two binary blocks b and c the* Hamming distance *between b and c is*

$$D(b, c) = w(b + c)$$

where addition is done component-wise modulo 2.

The Hamming distance, or *distance* for short, is just the number of digits that differ between two blocks. Addition is done on the digits independently of each other, so 011 + 010 = (0+0),(1+1),(1+0) = 001 and $D(011, 010) = w(011 + 010) = w(001) = 1$.

The Hamming distance between two blocks is equal to the distance between their equivalent points in $\mathbf{Z}_2^n$ (see Fig. 4). That is, allowing the digits of the blocks to be the coordinates of the vertices of an n-dimensional unit cube, the Hamming distance from one block to another is

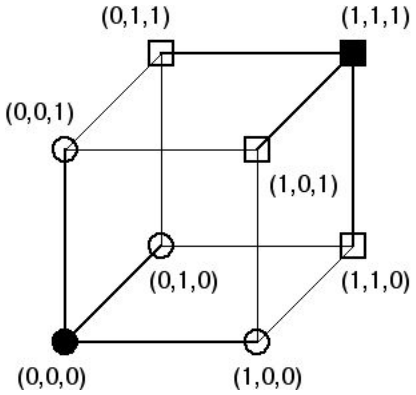


Figure 4: A single error-correcting code on the unit cube.

equal to the distance from one point to another, traveling only through adjacent vertices. The two descriptions will now be used interchangeably.

We are often concerned with the minimum distance between codewords over all pairs, as this will determine how many errors a code can correct. It is easiest to find this number within a *linear code*.

Definition 12 (Linear Code) *A code H is termed* linear *if*

$$(h_1 - h_2) \in H \quad for\, all\ h_1, h_2 \in H$$

where subtraction is the component-wise difference.

As an example, consider the repetition code represented by the two codewords 000 and 111 in Fig. 4. This code, call it B, is linear because the difference of any two codewords will result in a codeword. We may also use the fact that addition and subtraction are equal modulo 2. We can then represent the code with basis vectors just as we did with lattices. By carefully choosing k vectors, we can build all of the codewords of an (n, k) code as the set of all possible sequences of additions of these vectors. Just as with lattices, linear codes can be represented by generator matrices where the set of codewords is equal to the row space of the generator matrix.

In a linear code, the distance from the origin to the nearest codeword is equal to the minimum distance of the entire code. The minimum distance of a linear binary code is equal to the minimum nonzero weight.

The minimum distance of a code defines the number of errors a code can correct. All blocks received are decoded as the codeword closest to them (see Fig. 4). Each error moves the block one unit from the original codeword. If the minimum distance d is even, then $d/2$ errors could make a message equidistant from two different points and impossible to consistently decode correctly. A code with minimum distance d can then consistently correct $(d-1)/2$ errors. To create the most efficient codes, we want to have an odd d, and no blocks more than $(d-1)/2$ away from a codeword so that every block can be decoded correctly. Such codes are called *perfect codes*.

Before further defining perfect codes, we need to define *Hamming spheres*.

Definition 13 (Hamming Sphere) *Given a nonnegative integer r, a* Hamming sphere *of radius r centered on a vertex p, is defined as the set of all vertices x such that $D(p, x) \leq r$.*

If we center equally sized Hamming spheres at each codeword, we see that the number of errors a code corrects is the largest r the spheres can have while remaining disjoint. In Fig. 4, the set of points represented by squares and the set points represented by circles comprise two disjoint Hamming spheres of radius 1.

Definition 14 (Perfect Code) *A code of length n is termed* perfect *if there exists some nonnegative integer r such that all r-spheres centered on the codewords are pairwise disjoint and each n-block lies within a unique r-sphere.*

A received block must be within a unique Hamming sphere of a perfect code. By decoding a received block as the codeword that is at the center of the unique Hamming sphere, a perfect code corrects r errors. With this definition in mind, it is easy to see that finding good codes is akin to finding good sphere packings. While the sphere packings attempt to fill $\mathbb{R}^n$ with spheres as efficiently as possible, error-correcting codes attempt to fill $\mathbb{Z}_2^n$ with Hamming spheres as efficiently as possible. To see their interplay with the Leech lattice, we turn to a special perfect code.

3.2 Golay Codes and the Leech Lattice

In 1949 Marcel Golay published a paper demonstrating how to create several perfect single error-correcting codes. In the same paper he demonstrated a perfect code now called the *binary Golay code, C_{23}*. This remarkable code is a perfect binary 3 error-correcting code in 23 dimensions! A generator matrix of C_{23} is shown below.

$$\left[\begin{array}{cccccccccccc|ccccccccccc} 1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&0\\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1\\ 0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&1&1&1&1\\ 0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&0&0&1&1\\ 0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&1&1&0&1&0&1&0&1\\ 0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&1&0&1&0&0&1\\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&1&1&0&0&1&0&1\\ 0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&0&1&1&1&0&0&1\\ 0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&1&0&1&0&0&1&1\\ 0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&1&1&0&0&1&0&1&1\\ 0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&0&1&1&1&0&1\\ 0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&1&0&0&1&1&1 \end{array}\right]$$

He did not give a proof that his matrix did indeed generate a perfect code, but numerous proofs are now available (see [9]). If we add a parity check digit, giving each row an even number of 1's, we create the extended Golay code, C_{24}, with a minimum weight eight. However, we

will use a more complicated generator matrix of C_{24}, which flows naturally into our matrix representation of the Leech lattice:

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1
\end{bmatrix}$$

Every codeword in C_{24} has a weight of either 0, 8, 12, 16, or 24. Furthermore, the minimum distance between codewords is 8. The later property will be instrumental in our evaluation of the Leech lattice.

3.3 Leech's Construction

Codes are often used to create good sphere packings as we will see in the construction of the Leech lattice using C_{24}. At this time we consider Leech's original construction of his lattice, though we defer any calculations until a discussion of designs in Section 3.4.

Leech's original packing in 24 dimensions simply used C_{24} as a generating matrix for a lattice. He then devised a way of doubling the kissing number, resulting in the Leech lattice. We will follow his construction, prove that it does in fact create a lattice, and then show that it matches the lattices created by our matrix representation of the Leech lattice. The construction goes as follows.

Let each coordinate of a vector be represented in binary, with the first digit being the ones digit, the second being the twos digit, then fours, etc. When picturing these vectors it may help to write vectors with vertical binary representations:

$$\begin{array}{r}
\textit{Eights digit}- \\
\textit{Fours digit}- \\
\textit{Twos digit}- \\
\textit{Ones digit}-
\end{array}
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & \\
0 & 1 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & \\
1, & 1, & 1, & 1, & 1 & \dots
\end{pmatrix} = (9, 5, 1, 1, 1, ...)$$

First, let the ones digit of all the coordinates of a vector be either all 1's or all 0's. That is to say, every vector has all even coordinates or all odd coordinates. Second, let the two's digits of a vector form an element of C_{24}. Lastly, we let there be an even number of 1's in the fours digits of vectors with all even coordinates and an odd number of 1's in the fours digits in vectors of all odd coordinates. All other digits are free. In this way we have incorporated both even and odd copies of C_{24}.

Notice that because all digits above the third are free, we may evaluate a vector's inclusion by its binary value modulo 8. We similarly evaluate negative integers this way (Leech used an equivalent "twos complement" evaluation).

For instance, the vector of all -6 = 2 (mod 8) coordinates is an element of the lattice. For a convenient list of sample vectors in the Leech lattice simply refer to the rows of its generator matrix as well as any sums that can be made from these vectors.

Next we verify that this is indeed a lattice. To do so, we need to show that for any two vectors in the packing, u and v, their difference, $u - v$, is also in the packing. We will begin by showing that $-v$ is in our packing and then prove that $u + v$ is in our packing.

First consider the case where the coordinates of v are all odd. Because of our modulo 8 argument we need only consider the coordinate values 1, 3, 5, or 7. Each of these has an odd additive inverse so $-v$ must also have all odd coordinates. Also via inspection modulo 8, if a coordinate of v has a 1 in the twos digit (as in values 3 or 7), then the same coordinate in $-v$ does not. Since complements in C_{24} are also in C_{24}, the second criterion of inclusion is satisfied. Lastly, the fours digits of v is also the complement of the fours digits in $-v$, which means that there is still an odd number of 1's in the fours digit. Thus $-v$ is an odd vector in our packing.

Now let the coordinates of v be even. We will use similar logic as before. The coordinates are either 0, 2, 4, or 6 (mod 8). A quick inspection shows that $-v$ must also have even values modulo 8. Secondly, if the twos digit of a coordinate is 1, so is the same digit in $-v$. The second criterion is therefore satisfied. Because of our second criterion, we must have an even number of coordinates in v be 2 or 6 (mod 8). These are the only two numbers that change their fours digit in $-v$, so there must still be an even number of 1's in the eights digit. Therefore $-v$ is in our packing, whether even or odd.

Since negatives are always in our packing, we need only show $u+v$ is in our packing to meet the definition of a lattice. It is easy to see that all of the coordinates in $u + v$ are either all even or all odd. If u and v are either both even or a combination of odd and even then there is no affect on the twos digit by addition in the ones digit. Thus, the twos digits are merely adding rows in C_{24} and must still be an element of C_{24}. If u and v are both odd, then a 1 will be added to each of the twos digit from the addition in the ones digit. Since the all 1's vector is an element of C_{24}, the second digit still forms a row of C_{24}. Lastly, all rows in C_{24} have an even number of digits in common, so an even number of ones will be carried to the fours digit, which does not affect its overall parity. It is then apparent that the parity of the fours digits is equal to the parity of the coordinates, satisfying our final criterion.

We can now state that the Leech lattice is indeed a lattice. Furthermore, since the definition allows for any given coordinate to be 8 while leaving the rest as 0's, the Leech lattice is indeed a 24 dimensional lattice.

Finally, we claim that the matrix given in the Introduction is indeed a generator matrix for the Leech lattice. Since every row is an element of the Leech lattice, the lattice generated by the matrix representation must be contained in the Leech lattice. Similarly, all vectors in the Leech lattice can be constructed through linear combinations of row vectors in the generator matrix (the proof of which is left as an instructional exercise for the reader), so the matrix must indeed generate the Leech lattice.

3.4 Designs

Designs were originally studied for the purpose of efficient experimentation, but are now recognized as a specific type of code.

Definition 15 (Design) *Given a set of v elements, termed* points*, a t-(v, k, λ)* design *is a collection of k-subsets, termed* blocks*, such that any set of t points is contained in exactly λ blocks.*

A finite projective plane is an example of a $2-(n^2+n+1, n+1, 1)$ design. The simplest has $n = 2$ and can be represented over the set $\{1, 2, 3, 4, 5, 6, 7\}$ as

$$\{\{1,2,3\},\{3,4,5\},\{5,6,1\},\{1,7,4\},\{2,7,5\},\{3,7,6\},\{2,6,4\}\}$$

or drawn as

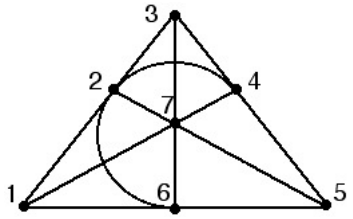


Figure 5: A 7 point projective plane

where any set of two points are on exactly one line. Notice that the curve $\{2, 4, 6\}$ is also a line. The 7 point projective plane forms a $2-(7, 3, 1)$ design. If $\lambda = 1$, as in the projective plane, then we may also call the design an $S(t, k, v)$ *Steiner system* (note the reordering of the variables). The 7 point projective plane is a $S(2, 3, 7)$ Steiner system. Any perfect error-correcting code gives rise to a Steiner system, as we will demonstrate using the binary Golay code.

Let X be the set $\{0, 1, 2, 3, ..., 21, \infty\}$, and associate each of the elements with a coordinate of the binary Golay code. Consider the Hamming spheres of radius 3 around the codewords. Because C_{23} is perfect, any vector with exactly four 1's lies within a unique Hamming sphere. Furthermore, each of these Hamming spheres is centered on a codeword with exactly seven 1's. By letting blocks be the set of indices of the 1's in codewords with weight 7, we form a $S(4, 7, 23)$ Steiner system over X.

$$(1,1,1,1,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1) \leftrightarrow \{0,1,2,3,6,21,\infty\}$$

Since there are $\binom{23}{4}$ possible 4-sets and each block contains $\binom{7}{4}$ possible 4-sets, there are $\binom{23}{4}/\binom{7}{4} = 253$ blocks in this design.

We will show the existence of one more design, which will be of particular use, the $S(5, 8, 24)$ design derived from the extended binary Golay code. Let $\Omega = \{0, 1, 2, ..., 22, \infty\}$ and associate each element with a coordinate of C_{24}. Pick a 5 element subset of Ω, which is then associated

with a binary block of length 24 with five 1's. If we only consider the first 23 coordinates, the vector is in exactly one Hamming sphere (as described before) of a codeword of length 7 or 8 in C_{23}. Any codeword with a 1 in the last digit is naturally associated with a codeword of weight 7 in C_{23} before the parity check digit is added to create C_{24}. We can then define the blocks of the design by the codewords of C_{24}. Thus, the extended Golay code contains (and is completely described by) a $S(5, 8, 24)$ Steiner system. Because we can derive the extended Golay code from the Leech lattice via the lattice's construction, the $S(5, 8, 24)$ Steiner System can also be derived from the structure of the Leech lattice.

We use the connection between $S(5, 8, 24)$ and C_{24} to calculate the number of 8-sets in C_{24}, which will be of use in enumerating the kissing number of the Leech lattice.

There are $\binom{24}{5}$ possible sets of 5 points, and each block contains $\binom{8}{5}$ sets of 5 points. S(5, 8, 24) then has $\binom{24}{5}/\binom{8}{5} = 759$ blocks, which is equal to the number of 8-sets in C_{24}. With this calculation in hand we can focus more directly on the Leech lattice.

3.5 Spherical Codes and Kissing Numbers

There is another type of code that is more related to kissing numbers than sphere packings. These codes are called *spherical codes*.

Definition 16 (Spherical Codes) *A set of points in $\mathbb{R}^n$ that are all on the surface of some n-sphere centered at the origin is termed an* n-dimensional spherical code.

The goal of a spherical code is normally to pack as many points as possible while keeping a minimum angle of separation. For instance, for two spheres to simultaneously touch a central sphere they must be at least 60^o apart. The kissing number problem thus asks how many points can be placed on the surface of an n-sphere while maintaining a minimum angle of 60^o. This number is written as $A(n, \pi/3)$, or generically as $A(n, \phi)$ where ϕ is the minimum angle in radians. Similarly, the maximum angle for a given number of points, M, on a n-sphere is notated by $P(n, M)$.

We will now calculate the kissing number of the Leech lattice. We will use the notational convention (a^m, b^n) to represent a vector with m coordinate values of a and n coordinate values of b. With our definition of the Leech lattice in mind, it is easy to see that the closest possible centers are of the form $(\pm 4^2, 0^{23})$; $(\pm 2^8, 0^{16})$ where the 2's are in the same coordinates as the 1's in a codeword of C_{24} and there are an even number of positive 2's; or $(\pm 3^1, \pm 1^{23})$ where the locations of the 3 and -1's are equal to the location of 1's in a codeword of C_{24}. All of these vectors have a length of $4\sqrt{2}$. Remembering that there are 759 vectors of weight 8 in C_{24}, we can enumerate all of the shortest vectors closest to the origin as follows.

Form	Number
$(2^8, 0^{16})$	759
$(2^6, -2^2, 0^{16})$	$759 \cdot \binom{8}{2} = 21{,}252$
$(2^4, -2^4, 0^{16})$	$759 \cdot \binom{8}{4} = 53{,}130$
$(2^2, -2^6, 0^{16})$	$759 \cdot \binom{8}{2} = 21{,}252$
$(-2^8, 0^{16})$	759
subtotal	$759 \cdot 2^7 = 97,152$
$(4^2, 0^{22})$	$\binom{24}{2} = 276$
$(4, -4, 0^{22})$	$24 \cdot 23 = 552$
$(-4^2, 0^{22})$	$\binom{24}{2} = 276$
subtotal	$4 \cdot \binom{24}{2} = 1,104$

Form	Number
$(1^{23}, 3)$	24
$(1^{16}, -1^7, 3)$	$759 \cdot 8 = 6{,}072$
$(1^{15}, -1^8, -3)$	$759 \cdot 16 = 12{,}114$
$(1^{12}, -1^{11}, 3)$	$2{,}576 \cdot 12 = 30{,}912$
$(1^{11}, -1^{12}, -3)$	$2{,}576 \cdot 12 = 30{,}912$
$(1^8, -1^{15}, 3)$	$759 \cdot 16 = 12{,}114$
$(1^7, -1^{16}, -3)$	$759 \cdot 8 = 6{,}072$
$(-1^{23}, 3)$	24
subtotal	$2^{12} \cdot 24 = 98,304$
Total	196,560

The Leech lattice provides the optimal spherical code/kissing problem solution of $A(24, \pi/3) = 196,560$ as well as the best known value for $P(24, 196560) = \pi/3$.

4 Simple Groups

Group theory is a rich field that has kept mathematicians busy for over 200 years. A group is simply a set with a defined associative operation, closure under that operation, an identity, and inverses. We will take a basic knowledge of group theory for granted, though the section should still be somewhat understandable without. This section is concerned with simple groups and groups created by lattices, particularly the Leech lattice.

Every group contains subgroups. All finite groups can be expressed as the product of *simple groups*. Furthermore this expression of groups in terms of simple groups is unique up to reordering. Simple groups are akin to prime numbers in that they are the basic factors from which other objects are built. This is meant as a brief explanation more than a definition.

Much of the structure of a group can be determined through its expression as a composition of smaller groups. For this reason, the search to find all the simple groups was very important. This project was completed in 1982 [13], after an intensive effort of over 50 years. The body of work dedicated to this proof requires about 15,000 journal pages, and is still the subject of much study and simplification.

The last simple groups to be discovered belong to the family of *sporadic simple groups*. Whereas most simple groups belong to easily classifiable infinite families, such as the cyclic groups of prime order or the alternating groups, the 26 sporadic groups are finite groups that have no obvious structural relationships with other simple groups. This section will focus on sporadic simple groups that can be found in the Leech lattice, three of which were discovered within the Leech lattice.

4.1 Automorphism Groups of Lattices, Designs, and Codes

All lattices can be used to create groups. In particular, every lattice has an *automorphism group.*

Definition 17 (Lattice Automorphism Group) *For a given lattice L_n, the* automorphism group *of L_n, denoted* $\mathrm{Aut}(L_n)$*, is the set of all distance preserving transformations that fix the origin and sends the lattice onto itself. Furthermore, the* order *of Aut(L_n), denoted* $|\mathrm{Aut}(L_n)|$*, is the number of elements in Aut(L_n).*

Though this definition applies specifically to lattices, the notation for automorphism groups will be consistent for all types of automorphism groups and similarly for the order.

As an example, there are 12 elements in $\mathrm{Aut}(\Lambda_2)$, the six rotations of $k\pi/3$ radians where $0 \leq k \leq 5$ and the six possible reflections [see Fig. 3]. The composition of two automorphisms will always be equivalent to one of the twelve automorphisms. This set of automorphisms under the operation of composition forms the group D_6. Notice that we need only consider the set of points closest to the origin. If we know where an automorphism takes the set of points closest to the origin, the distance preserving property of automorphisms determines all other points. There is, however, no comprehensive algorithm for determining the automorphism group of a lattice.

Designs also have automorphism groups.

Definition 18 (Design Automorphism Group) *An* automorphism *of a design D is a permutation of the points of D such that every block of D is taken to a block of D.*

The $S(2,3,7)$ design demonstrated by the seven point projective plane [see Fig. 5] serves as a good example. As noted in Section 3.4, we can represent this design as $\{\{1,2,3\},\{3,4,5\},\{5,6,1\},\{1,7,4\},\{2,7,5\},\{3,7,6\},\{2,6,4\}\}$. The following permutation of elements is an automorphism of the design.

$$1 \to 2,\ 2 \to 4,\ 3 \to 6,\ 4 \to 1,\ 5 \to 5,\ 6 \to 7,\ 7 \to 3$$

or equivalently in cycle notation

$$(1\ 2\ 4)(3\ 6\ 7)(5).$$

Notice that the automorphism takes the block $\{1,2,3\}$ to the block $\{2,4,6\}$. It can be easily checked that the automorphism takes all of the blocks of the design to other blocks.

It is instructive to calculate the order of $\mathrm{Aut}(S(2,3,7))$. After the automophism is applied, we refer to the points in the design after the automorphism as being in the *image* of the automorphism. A first point can be moved to any of the seven points, and the second can be moved to any of the remaining six points in the image. These two points define a block and the image of a third point in that block. The permutation of a fourth point may be chosen from the remaining four points in the image, which then defines the location of the remaining points as elements of blocks. There are therefore $7 \cdot 6 \cdot 4 = 168$ elements in $\mathrm{Aut}(S(2,3,7))$.

A *stabilizer group* is a set of automorphisms that fixes one or more specific points. As the name implies, stabilizer groups are subgroups of automorphism groups. Our demonstrated

automorphism of $S(2,3,7)$ is in the automorphism group that fixes the point 5. Using the same argument as before, the order of any *single point stabilizer group*, a stabilizer group that fixes a single point, of $S(2,3,4)$ is $6 \cdot 4 = 24$. Any type of automorphism group, whether of a lattice, design, etc., can have a stabilizer group by fixing the appropriate elements of the set being permuted.

The automorphism groups of codes are also important.

Definition 19 (Code Automorphism Group) *A permutation of the coordinates of a code that takes all codewords to other codewords is termed an* automorphism. *The set of all automorphisms of a code forms an* automorphism group *under composition of automorphisms.*

The automorphism groups of codes are very much like those of designs. Because of this close relation we will not be dealing directly with automorphism groups of codes, but rather with the automorphism groups of the designs associated with the Golay codes.

Of immediate relevance to us is the automorphism group of the Leach lattice $\cdot 0$, pronounced "dot-oh" (some authors use Co_0 instead of $\cdot 0$). Before we can discuss $\cdot 0$, we must understand its simple subgroup M_{24}, the automorphism group of $S(5,8,24)$.

4.2 The Mathieu Groups

There are multiple Mathieu groups, denoted $M_{24}, M_{23}, M_{22}, M_{12}$, and M_{11}, which represent the automorphism groups of $S(5,8,24), S(4,7,23), S(3,6,22), S(5,6,12)$, and $S(4,5,11)$ respectively. The smaller groups can all be defined as stabilizer groups of the largest. Because we constructed the points and blocks of $S(5,8,24)$ by using the coordinates and codewords of C_{24} respectively (see Section 3.4), we can equivalently define the Mathieu groups as the automorphism group of the binary extended Golay code and its appropriate stabilizers. These five groups were the first sporadic simple groups to be discovered [21],[65]. We will be particularly concerned with M_{24}.

If we let the set of points in $S(5,8,24)$ be $\Omega = \{0,1,2,...,22,\infty\}$, $\mathrm{Aut}(5,8,24) = M_{24}$ is generated by the following permutations of Ω in cycle notation:

$$\begin{aligned}
\alpha &= (\infty)(0\ 1\ 2\ 3\ \ldots\ 22) \\
\beta &= (\infty)(0)(1\ 2\ 4\ 8\ 16\ 9\ 18\ 13\ 3\ 6\ 12)(5\ 10\ 20\ 17\ 11\ 22\ 21\ 19\ 15\ 7\ 14) \\
\gamma &= (0\ \infty)(1\ 22)(2\ 11)(3\ 15)(4\ 17)(5\ 9)(6\ 19)(7\ 13)(8\ 20)(10\ 16)(12\ 21)(14\ 18) \\
\delta &= (\infty)(0)(3)(15)(1\ 18\ 4\ 2\ 6)(5\ 21\ 20\ 10\ 7)(8\ 16\ 13\ 9\ 12)(11\ 19\ 22\ 14\ 17)
\end{aligned}$$

where $\beta = \alpha^5\gamma\alpha^5\gamma\alpha^{14}\gamma\alpha^{18}$.

Again, if each element in Ω is associated with an appropriate coordinate of C_{24}, α, β, γ, and δ generate $\mathrm{Aut}(C_{24})$. We will also associate codewords with subsets of Ω by including elements that are associated with nonzero coordinates of the codeword. For instance

$$(1,1,1,1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1) \leftrightarrow \{0,1,2,3,6,7,22,\infty\}$$

We will often be associating the elements of Ω with the coordinates of the Leech lattice in a similar fashion.

4.3 The Symmetries of ·0

We now begin our analysis of ·0 by describing all possible automorphisms of the Leech lattice and finding a specific maximal subgroup N. Let P represent the set of points in the Leech lattice closest to the origin. Because we are dealing with a lattice $\mathrm{Aut}(P) \cong \mathrm{Aut}(\Lambda_{24})$ as noted in Section 4.1.

By virtue of its construction, any permutation that takes the set of codewords in C_{24} onto itself also takes P onto itself via the same permutation of coordinates. All such permutations are thus automorphisms. Let M be the group formed by the set these automorphisms. M is isomorphic to the automorphism group of $S(5,8,24), M_{24}$. Consequently, ·0 has all of the Mathieu groups as subgroups.

We denote our next automorphism as ϵ_s, where s is a subset of Ω that is associated with any codeword of C_{24} (see Section 4.2). Letting the vector $v = (v_0, v_1, ..., v_{22}, v_\infty)$, define ϵ_s as

$$\epsilon_s(v) = (v_0^*, v_1^*, ..., v_\infty^*) \quad \text{where } v_a^* = \begin{cases} -v_a & \text{if } a \in s \\ v_a & \text{if } a \notin s \end{cases}$$

That is, ϵ_s multiplies each coordinate represented in s by -1. Geometrically, ϵ_s is a reflection about a plane of dimension $|s|$ through the origin.

The set of all possible ϵ_s forms a group which will be denoted as E. It was shown in [11] that E is generated by the permutation $\epsilon = \epsilon_Q$, where $Q = \{0,1,2,3,4,6,8,9,12,13,16,18\}$ (Q is also the set of quadratic residues modulo 23).

The subgroup $N = EM = \{\epsilon\pi | \epsilon \in E, \pi \in M\}$ is maximal in ·0 (see [28]). We may then express N as the symmetries generated by $\alpha, \beta, \gamma, \delta,$ and ϵ [see Appendix A for matrix representations].

We now construct our final symmetry ζ, which lives in ·0 but outside of N. Choose any 4-set T_0 in Ω. T_0 is a subset of 5 8-sets in $C_{24}, T_0 + T_1, T_0 + T_2, ..., T_0 + T_5$, where T_i represents the complement of T_0 in the appropriate 8-set. Furthermore, the T_i's are disjoint, forming a perfect covering of Ω (see [28]).

Letting the vector $v = (v_0, v_1, ..., v_{22}, v_\infty)$, define ζ as

$$\zeta(v) = (v_0', v_1', ..., v_\infty') \quad \text{where } v_a' = v_a - \frac{1}{2}\sum_{b \in T_i} v_b \quad \text{when } a \in T_i$$

That is, for every nonzero coordinate in any T_j, subtract $\frac{1}{2}$ of its value from each coordinate in T_j. The proof that ζ is an automorphism is simple but heavy on computation (the reader is refered to [28]).

The symmetries of N combined with ζ generate all of ·0.

4.4 The Order of ·0

With ·0 defined, it is a largely computational exercise to determine its order. We will discuss the general argument now.

Given any two pairs of points in P, there exists an automorphism in ·0 that will take one pair of points to the other ([9], [28]). That is, ·0 is *doubly transitive*. Letting $\cdot 0_x$ represent the

stabilizer group that fixes a given $x \in P$, and $\cdot 0_{x,y}$ represent the stabilizer group that fixes x and some given $y \in P$ with y orthogonal to x, we have

$$|\cdot 0| = \frac{|\cdot 0|}{|\cdot 0_x|}\frac{|\cdot 0_x|}{|\cdot 0_{x,y}|}|\cdot 0_{x,y}| = [\cdot 0 : \cdot 0_x][\cdot 0_x : \cdot 0_{x,y}]|\cdot 0_{x,y}|.$$

where we use the notation $[G : G_x] = |G|/|G_x|$, for finite G.

We will compute these numbers using the following definition and property. Given $v \in V$ and a group G acting on V we define the *orbit* of v as $\{g(v)|g \in G\}$. In our case, the orbit of $v \in P$ equals $\{p(v)|p \in \mathrm{Aut}(P)\}$. For any given group G, acting on a set containing $x, [G : G_x]$ is equal to the order of the orbit of x. We can rewrite this property as $|G|/|G_x|$ is equal to number of possible permutations of the point x allowed by G.

Because $\cdot 0$ is transitive, any point in P can be taken to any other point by the automorphisms in $\cdot 0$. The order of the orbit of x, which is equal to $[\cdot 0 : \cdot 0_x]$, is simply the number of points adjacent to the origin, or the kissing number, 195,650.

$[\cdot 0_x : \cdot 0_{x,y}]$ can be enumerated as follows, though we refer the reader to [28] or [9] for further justification:

Fix a point x of the form $(4^2, 0^{22})$ with 4's in the ith and jth coordinate and pick a point y of the same form (strictly for convenience) which is orthogonal to x. Orthogonality can most easily defined by the property $x \cdot y = 0$. We now need to find the entire orbit of the point y generated by $\cdot 0_x$. Since $\cdot 0$ is doubly transitive on $P, \cdot 0_x$ can take y to any point in P that is orthogonal to x. We will break the orbit of y into disjoint sets of points orthogonal to x as O_1, O_2, O_3, O_4, and O_5.

Define O_1 as the orbit consisting of the two vectors orthogonal to x formed by taking the negatives of one of the 4's in ith or jth coordinate.

The set of vectors of the form $(\pm 4^2, 0^{22})$ that have 0's in the ith and jth coordinates will be denoted by the orbit O_2. All such vectors are obviously orthogonal to x, so $|O_2| = 4 \cdot \binom{22}{2} = 924$.

The set vectors of the form $(\pm 2^8, 0^{16})$ that have 0's in the ith and jth coordinates will be denoted by the orbit O_3. We first determine how many of the 759 vectors of the form $(2^8, 0^{16})$ have 0's in the ith and j coordinates. Out of the $\binom{24}{2}$ ways of choosing pairs from the 24 coordinate, there are $\binom{16}{2}$ ways of choosing pairs of 0 coordinates in any vector of the form $(2^8, 0^{16})$. This gives $\left(\binom{16}{2}/\binom{24}{2}\right) 759 = 330$ vectors of the form $(2^8, 0^{16})$ with 0's in the ith and jth coordinates. Multiplying by 2^7 choices of signs, we see that there are $2^7 \cdot 330 = 42,240$ vectors in O_3

Now consider O_4, consisting of the vectors of the form $(\pm 2^8, 0^{16})$ where there is a ± 2 in the ith component and a ∓ 2 in the jth component. We first determine how many vectors of the form $(2^8, 0^{16})$ have 2's in the ith and j component. There are $\binom{24}{2}$ ways of choosing 2 coordinates, and each vector contains $\binom{8}{2}$ pairs of 2's. Multiplying, we see that there are $\left(\binom{8}{2}/\binom{24}{2}\right) 759 = 77$ vectors of the form $(2^8, 0^{16})$ with 2's in the ith and jth coordinates. Making sure that the ith and jth coordinates have opposite signs, there are 2^6 choices of sign. This gives $2^6 \cdot 77 = 4,928$ vectors in 0_4.

Lastly we must include the orbit 0_5, with all vectors of the form $(\pm 3, \pm 1^{23})$ where there is a ± 1 in the ith coordinate and a ∓ 1 in the jth coordinate. There are 22 coordinates that the

3 can be in. The number of vectors that have opposite signs in the ith and jth coordinates is the same as the number of codewords in C_{24} that have 1's in only one of the two components, which is half of the 2^{12} codewords in C_{24}. There are thus $2^{11} \cdot 22 = 45,056$ vectors in O_5.

We can now enumerate the orbit of y in the table below.

Orbit	Form	Number
O_1	$(\pm 4, \pm 4, 0^{22})$	2
O_2	$(\pm 4, \mp 4, 0^{22})$	924
O_3	$(\pm 2^8, 0^{16})$	42,240
O_4	$(\pm 2^8, 0^{16})$	4,928
O_5	$(\pm 3, \mp 1^{23})$	45,056
Total	$[\cdot 0_x : \cdot 0_{x,y}]$	93,150

With $[\cdot 0 : \cdot 0_x]$ and $[\cdot 0_x : \cdot 0_{x,y}]$ enumerated, we only need $|\cdot 0_{x,y}|$ to finish computing $|\cdot 0|$.

No two points in P are fixed by ζ, so all permutations in $\cdot 0_{x,y}$ live in N. The order of N is equal to $|E||M_{24}| = 2^{12} \cdot |M_{24}|$. The number of permutions in E that fix a given two points is 2^{10}. The number of permutations in M that fix a given two points is $|M_{22}|$, which is known to be $22 \cdot 21 \cdot 20 \cdot 48$ (see [28]). Therefore $|\cdot 0_{x,y}| = |E_{10}||M_{22}| = 2^{10} \cdot 22 \cdot 21 \cdot 20 \cdot 48 = 2^{17} \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$

We now have all the information we need. Multiplying $[\cdot 0 : \cdot 0_x]$, $[\cdot 0_x : \cdot 0_{x,y}]$, and $|\cdot 0_{x,y}|$ we can thus state that the group $\cdot 0$ generated by the set of symmetries $\alpha, \beta, \gamma, \delta, \epsilon$, and ζ has order

$$2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23 = 8,315,553,613,086,720,000.$$

4.5 A Description of the Sporadic Simple Groups in $\cdot 0$

While $\cdot 0$ is a very large group that contains copies of the sporadic simple groups M_{24}, M_{23}, M_{22}, M_{12}, and M_{11}, it is not simple. If, however, we divide the group in half (taking the quotient of $\cdot 0$ by its two-element center), we create a new simple group denoted, $\cdot 1$. The order of this large sporadic simple group is

$$|\cdot 1| = |\cdot 0|/2 = 2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23 = 4,157,776,806,543,360,000.$$

In addition to $\cdot 1$, two other sporadic simple groups, $\cdot 2$ and $\cdot 3$, were first found in the automorphism group of the Leech lattice. $\cdot 2$ is a group of order

$$|\cdot 2| = |\cdot 1|/196,560 = 42,305,421,312,000,$$

and is formed by the automorphism group of P after fixing any given vector. $\cdot 3$ is a group of order 495,766,656,000 and is formed by the automorphism group of the Leech lattice after fixing a vector in the second shell of the lattice (meaning that the vector is at a distance of $4\sqrt{3}$ from the origin). Both of these simple groups are also subgroups of $\cdot 1$.

There are four other sporadic simple groups that can be found within the Leech lattice. The McLaughlin group (McL) of order 898,128,000 and the Higman-Sims group (HS) of order 44,352,000 can be formed by taking the automorphism group after fixing vectors of length $4\sqrt{5}$ and $4\sqrt{7}$ respectively.

The Suzuki group (Suz) of order 448,345,497,600 and the Hall-Janko group (J_2) of order 604,800 can also be found in the automorphisms of the Leech lattice. These two groups arise from the *complex Leech lattice* and the *quaternionic Leech lattice*. By assigning half of the coordinates of the Leech lattice to be real values and the other half to be imaginary values, the Leech lattice can be described by 12 generator vectors over the complex numbers. Similarly the Leech lattice can be described by 6 generator vectors over the quaternions. By breaking each complex vector back into its two component vectors and each quaternionic vector into its four component vectors the complex and quaternionic Leech lattice become the real Leech lattice. Suz is formed by taking the automorphisms that preserve the complex structure of the Leech lattice, which is equivalent to the automorphism group of the complex Leech lattice, and then factoring by a 6 element quotient group. J_2 can be formed by the automorphisms that, in a similar fashion, preserve the quaternionic structure and then factoring by the center.

Lastly, it should be mentioned that a rather famous sporadic simple group can be constructed using the Leech lattice. The "monster group" or "friendly giant" (F_1 or M) is a group that exists in 196,844 dimensional space and has an of order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

$$= 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

$$\approx 8 \cdot 10^{53}$$

R. L. Greiss originally constructed the monster group in 1981 using using a nonassociative algebra in 196,884 dimensional Euclidean space, but the simplest known construction makes use of the Leech lattice, the Golay code, and the Mathieu groups [9]. Within the monster can be found copies of all but six of the sporadic simple groups. These 6 groups are often referred to as the "pariah."

5 Variations on the Leech Lattice

We conclude our discussion of the Leech lattice by mentioning some related lattices. The complex Leech lattice and the quaternionic Leech lattice were briefly discussed in Section 4.5. There are several other lattices which are best constructed by using properties of the Leech lattice. All of the following lattices have constructions related to the Leech lattices but are not actually sublattices of Λ_{24}.

The even unimodular lattices have many important properties. They have been proven to exist in n-dimensions if and only if n is a multiple of 8. $E_8 = \Lambda_8$ and Λ_{16} are the only such lattices for 8 and 16 dimensions respectively. In 24 dimensions there are 24 even unimodular lattices, the Leech lattice and the 23 *Niemeier lattices*. It is a remarkable property of the Leech lattice that each of the 23 different types of deep holes are in one-to-one correspondence with the 23 Niemeier lattices. We can then catalogue all of the even unimodular lattices in 24 dimensions in the Leech lattice and the lattices generated by the 23 types of deep holes. The Leech lattice also contains copies of E_8 and Λ_{16} (see section 2.1). Thus, the Leech lattice contains copies of all even unimodular lattices of dimension less than or equal to 24.

There are also two important odd unimodular latttices associated with the Λ_{24}. The *shorter Leech lattice*, O_{23}, is defined as the unique 23-dimensional lattice with minimal norm 3 (assuming that all lattices are scaled so that the determinant of their generator matrix is 1). O_{23} is uniquely constructed as follows. Choose any minimal vector, v, in Λ_{24} and define $v^{\perp}$ as the set of all vectors in $\mathbb{R}^{24}$ that are orthogonal to v. We then define O_{23} as the projection of the set of vectors in Λ_{24} that have an even inner product with v onto the 23-dimensional space $v^{\perp}$.

The *odd Leech lattice*, O_{24}, is the unique 24-dimensional lattice with minimal norm 3. O_{24} is generated by the vectors in Λ_{24} with all even coordinates and the all 1's vector. If the -3 in our generator matrix of Λ_{24} is replaced with a 1, the resulting lattice is O_{24}.

6 Conclusion

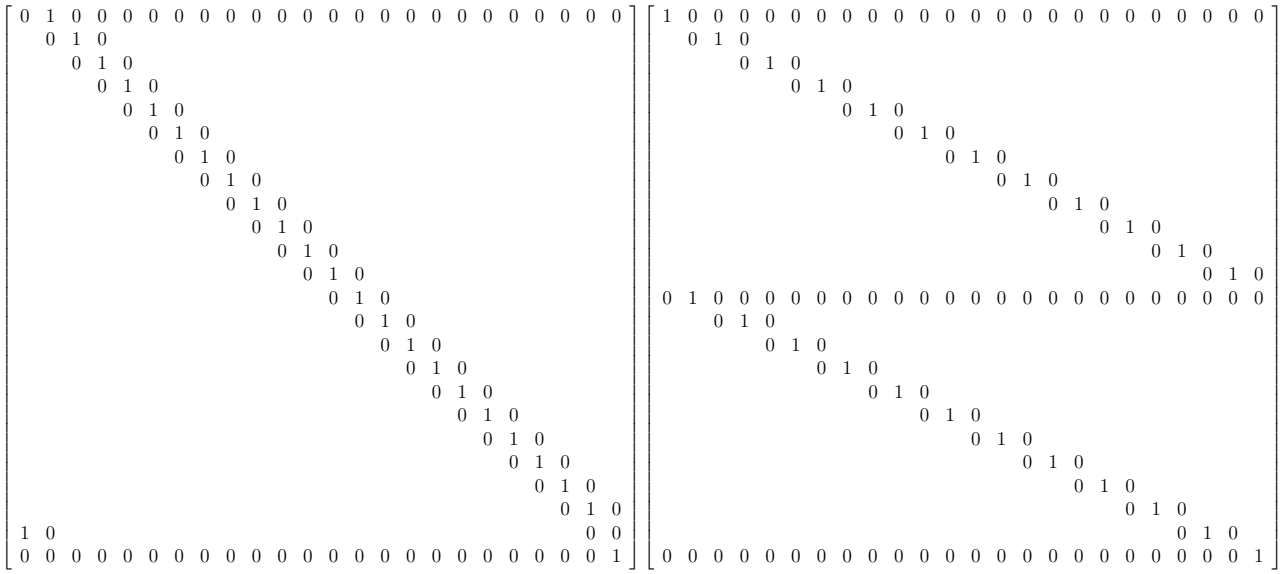
At this point we have touched on many of the important qualities of the Leech lattice. There is, however, far more information available than could be included within a single paper. In fact, any attempt to contain all current knowledge would be futile, as discoveries are constantly being made. Many of the topics covered have emerged within the last century and are still in the process of maturing. There are currently more problems than mathematicians to work on them. The process of cataloguing and disseminating what is known is thus a topic of constant interest. It is in this vein that the paper was written, and in this vein that it will conclude. A table of Leech lattice properties is listed below.

Prominent Properties of Λ_{24}	
Packing Density (Δ)	≈ 0.001930
Center Density (δ)	1
Covering Thickness (Θ)	≈ 0.79035
Kissing Number (τ)	196,560
Modularity	Self-dual, doubly-even unimodular
Sublattices	$\Lambda_n, K_n : 1 \leq n \leq 24$
Imbedded Codes	C_{24}, C_{23}
Imbedded Designs	$S(5,8,24), S(4,7,23), S(3,6,22)$ $S(5,6,12), S(4,5,11)$
Related Lattices	Neiemer lattices, complex Leech lattice, quaternionic Leech lattice, O_{24}, O_{23}
Automorphism Group	$\cdot 0(Co_0)$
Sporadic Simple Subgroups	$\cdot 1(Co_1), \cdot 2(Co_2), \cdot 3(Co_3),$ $M_{24}, M_{23}, M_{22}, M_{12}, M_{11}, HJ, McL$
Related Sporadic Simple Groups	J_2, Suz, F_1(or M, the monster group)
Optimalities	$\Delta(L_{24}), \delta(L_{24}), \Theta(L_{24})$ $\tau_{24} = A(24, \pi/3), P(24, 196560),$

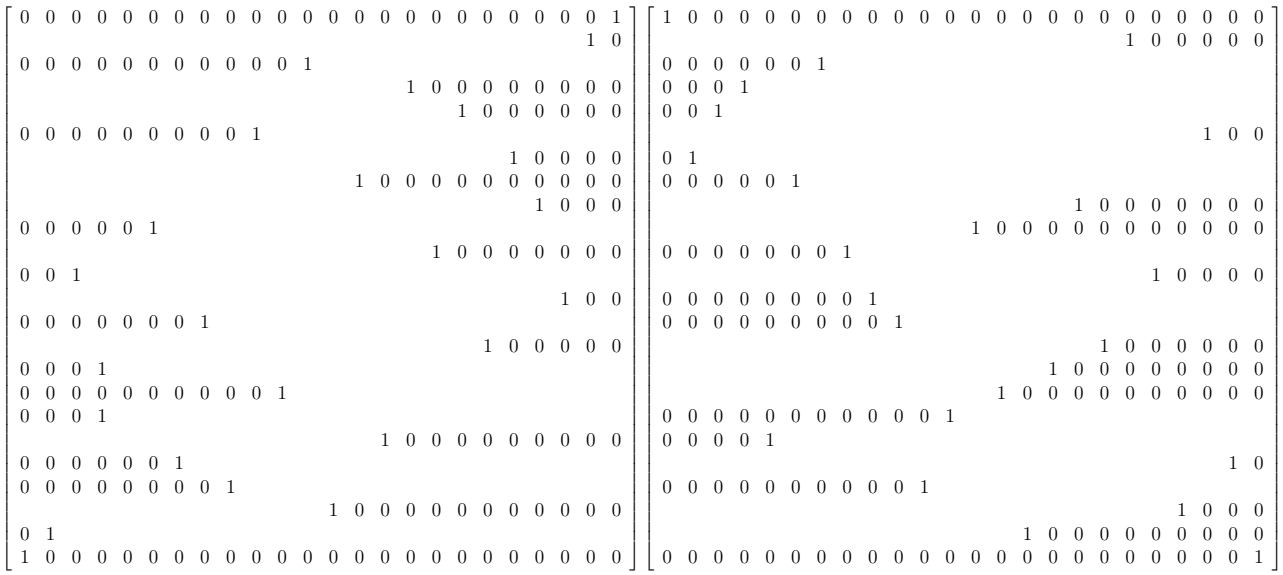
(L_{24} denotes among 24-dimensional lattices.)

7 Appendix A: Matrix Representations of Generator Permutations

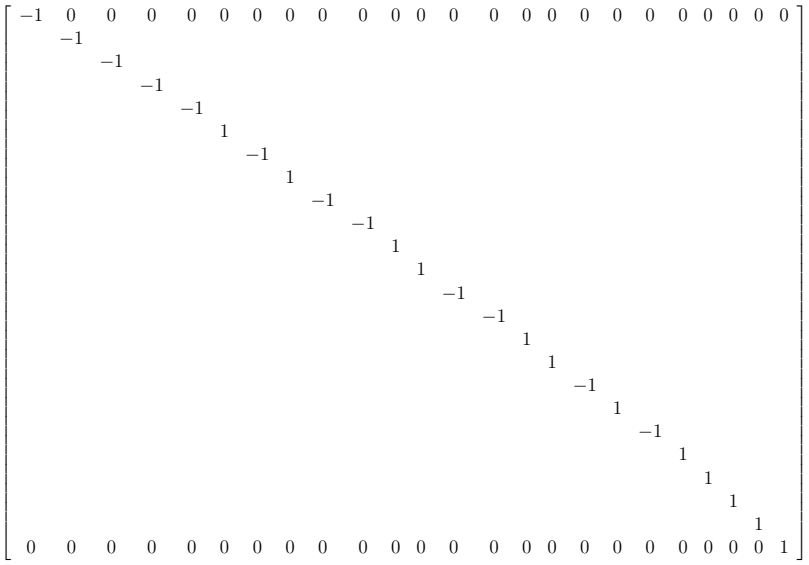
Below are matrix representations of the permutations $\alpha, \beta, \gamma, \delta, and \epsilon$ as given by [28]. All empty entries represent 0's.



Matrix representations for α and β



Matrix representations for γ and δ



Matrix representation for ϵ

References

[1] Banai, E., N. J. A. Sloane. "Uniqueness of Certain Spherical Codes." *Canadian Journal of Mathematics* 33 (1981): 437-449.

[2] Batten, Lynn Margaret. *Combinatorics of Finite Geometries*. New York: Cambridge University Press, 1986

[3] Constantine, Gregory M. *Combinatorial Theory and Statistical Design*. New York: John Wiley & Sons, 1987.

[4] Conway, J. H., et al. *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*. New York: Clarendon Press, 1985.

[5] Cohn, Henry, Noam Elkies. "New Upper Bounds on Sphere Packings I." *Annals of Mathematics* 157 (2003): 689-714.

[6] Cohn, Henry. "New Upper Bounds on Sphere Packings II." *Geometry and Topology* 6 (2002): 329-353.

[7] Cohn, Henry, Abhinav Kumar. *Optimality and Uniqueness of the Leech Lattice Among Lattices*. March 2006 <http://research.microsoft.com/∼cohn/publications.html>.

[8] Cohn, Henry, Abhinav Kumar. "The Densest Lattice in Twenty-Four Dimensions." *Electronic Research Announcements of the American Mathematical Society* 10 (2004), 58-67.

[9] Conway, J. H., N. J. A. Sloane. *Spere Packing, Lattices and Groups*. 3rd ed. New York: Springer, 1998.

[10] Conway, J. H. "The Automorphism group of the 26-Dimensional Even Unimodular Lorentzian Lattice." *Journal of Algebra* 80 (1983): 159-163.

[11] Conway, J. H. "Hexacode and Tetracode- MOG and MINIMOG." *Computational Group Theory*. Ed. M. D. Atkinson. New York: Ac. Press, 1984. 359-364.

[12] Davenport, H. "The Covering of Space by Spheres." *Rend. Circ. Mat. Palermo* 1 (1952): 92-107.

[13] Gallian, J. A. "Classification of Finite Simple Groups Complete." *MAA Focus* 1 (1981): 3, 7.

[14] Hales, Thomas C. *A Proof of the Kepler Conjecture*. 2003 <http://www.math.pitt.edu /∼thales/PUBLICATIONS/>.

[15] Hurley, J. F., A. Rudvalis. "Finite Simple Groups." *American Mathematical Monthly* 84 (1977): 693-714.

[16] Leech, J. "The Problem of Thirteen Spheres." *Mathematika Gazette* 40 (1956): 22-23.

[17] Leech, J. "Some Sphere Packings in Higher Space." *Canadian Journal of Mathematics* 19 (1964): 657-682.

[18] Leech, J. "Notes on Sphere packings." *Canadian Journal of Mathematics* 10 (1967): 251-267.

[19] Leech, J. "Six and Seven Dimensional Nonlattice Sphere Packings." *Canadian Journal of Mathematics* 12 (1969): 151-157.

[20] Leech, J., N. J. A. Sloane. "Sphere Packings and Error-Correcting Codes." *Canadian Journal of Mathematics* 23 (1971): 718-745.

[21] Levenshtein, B. I. "On Bounds for Packing in N-dimensional Euclidean Space." *Doklady Akademii Nauk SSR* 245 (1979): 417-421.

[22] MacWilliams, F. J., N. J. A. Sloane. *The Theory of Error-Correcting Codes*. New York: Elsevier Science Publishers B.V., 1977.

[23] McEliece, Robert J. "The Theory of Information and Coding: A Mathematical Framework for Communication." *Encyclopedia of Mathematics and its Applications*. vol. 3. Reading, Massachusetts: Addison-Wesley Publishing Compony, 1977.

[24] Odlyzko, A. M., N. J. A. Sloane. "New Bounds on the Number of Unit Spheres that can Touch a Unit Sphere in N Dimensions." *Journal of Combinatorial Theory* A26 (1979): 210-214.

[25] Pless, Vera. *Introduction to the Theory of Error-Correcting Codes*. 3rd ed. New York: John Wiley & Sons, 1998.

[26] Schreier, O., "Über die Erweiterung von Gruppen I." *Monatsh. Math. Phys.* 34 (1926): 165-180.

[27] Szpiro, George G. *Kepler's Conjecture: How Some of the Greatest Minds in History Helped Solve One of the Oldest Math Problems in the World*. Hoboken, Jew Jersey: John Wiley & Sons, 2003.

[28] Thompson, Thomas M. *From Error-Correcting Codes through Sphere Packings to Simple Groups*. Washington D.C.: Mathematical Association of America, 1983.

[29] Wallis, W. D. *Combinatorial Designs*. New York: Marcel Dekker, Inc., 1988.

[30] Zador, P. L. *Development and Evaluation of Procedures for Quantizing Multivariate Distributions*. Ph.D, Dissertation, Stanford Univ., 1963.

[31] Zador, P. L. "Asymptotic Quantization Error of Continuous Signals and their Quantization Dimension." *Institute of Electrical and Electronics Engineers, Transactions on Information Theory* 28 (1982): 139-149.