ANNALS OF MATHEMATICS

Optimality and uniqueness of the Leech lattice among lattices

By Henry Cohn and Abhinav Kumar

SECOND SERIES, VOL. 170, NO. 3

November, 2009

ANMAAH

Annals of Mathematics, **170** (2009), 1003–1050

Optimality and uniqueness of the Leech lattice among lattices

By HENRY COHN and ABHINAV KUMAR

Dedicated to Oded Schramm (10 December 1961 – 1 September 2008)

Abstract

We prove that the Leech lattice is the unique densest lattice in $\mathbb{R}^{24}$. The proof combines human reasoning with computer verification of the properties of certain explicit polynomials. We furthermore prove that no sphere packing in $\mathbb{R}^{24}$ can exceed the Leech lattice's density by a factor of more than $1 + 1.65 \cdot 10^{-30}$, and we give a new proof that E_8 is the unique densest lattice in $\mathbb{R}^8$.

1. **Introduction**

It is a long-standing open problem in geometry and number theory to find the densest lattice in $\mathbb{R}^n$. Recall that a lattice $\Lambda \subset \mathbb{R}^n$ is a discrete subgroup of rank n; a minimal vector in Λ is a nonzero vector of minimal length. Let $|\Lambda| = \mathrm{vol}(\mathbb{R}^n/\Lambda)$ denote the covolume of Λ, i.e., the volume of a fundamental parallelotope or the absolute value of the determinant of a basis of Λ. If r is the minimal vector length of Λ, then spheres of radius $r/2$ centered at the points of Λ do not overlap except tangentially. This construction yields a sphere packing of density

$$\frac{\pi^{n/2}}{(n/2)!}\left(\frac{r}{2}\right)^n \frac{1}{|\Lambda|},$$

since the volume of a unit ball in $\mathbb{R}^n$ is $\pi^{n/2}/(n/2)!$, where for odd n we define $(n/2)! = \Gamma(n/2+1)$. The densest lattice in $\mathbb{R}^n$ is the lattice for which this quantity is maximized.

There might be several distinct densest lattices in the same dimension. For example, the greatest density known in $\mathbb{R}^{25}$ is achieved by at least 23 distinct

Kumar was supported by a summer internship in the Theory Group at Microsoft Research and by a Putnam graduate fellowship at Harvard University.

lattices, although they are not known to be optimal. (See pages xix and 178 of [CS99] for the details.) We will speak of "the densest lattice" because it sounds more natural.

The problem of finding the densest lattice is a special case of the sphere packing problem, but there is no reason to believe that the densest sphere packing should come from a lattice. In particular, in $\mathbb{R}^{10}$ the densest packing known is the Best packing P_{10c}, which is not a lattice packing (see [CS99, p. 140]). It conjectured that lattices are suboptimal in all sufficiently high dimensions. However, many of the most interesting packings in low dimensions are lattice packings, and lattices have strong connections with other fields such as number theory. For example, the Hermite constant γ_n is defined to be the smallest constant such that for every positive-definite quadratic form $Q(x_1, \dots, x_n)$ of determinant D, there is a nonzero vector $(v_1, \dots, v_n) \in \mathbb{Z}^n$ such that $Q(v_1, \dots, v_n) \le \gamma_n D^{1/n}$. Finding the maximum density of a lattice packing in $\mathbb{R}^n$ is equivalent to computing γ_n.

The densest lattice in $\mathbb{R}^n$ is known for $n \le 8$: the answers are the root lattices A_1, A_2, A_3, D_4, D_5, E_6, E_7, and E_8. For $n = 3$ this is due to Gauss [Gau31], for $4 \le n \le 5$ to Korkine and Zolotareff [KZ73], [KZ77], and for $6 \le n \le 8$ to Blichfeldt [Bli35]. However, before the present paper no further cases had been solved since 1935. In 1946 Chaundy claimed to have dealt with $n = 9$ and $n = 10$, but his paper [Cha46] implicitly assumes that a densest lattice in $\mathbb{R}^n$ must contain one in $\mathbb{R}^{n-1}$ as a cross section. That is known to be false (see [CS82]), so the paper appears irreparably flawed.

In each of the solved cases, the optimal lattice is furthermore known to be unique, up to scaling and isometries. This was proved simultaneously with the optimality for $n \le 5$, for $n = 6$ it was proved by Barnes [Bar57], and for $6 \le n \le 8$ it was proved by Vetčinkin [Vet80].

In this paper we deal with $n = 24$ (the theorem numbering is as it will appear later in the paper):

THEOREM 9.3. *The Leech lattice is the unique densest lattice in* $\mathbb{R}^{24}$, *up to scaling and isometries of* $\mathbb{R}^{24}$.

In terms of the Hermite constant, $\gamma_{24} = 4$. We also give a new proof for E_8:

THEOREM 11.7 (Blichfeldt, Vetčinkin). *The* E_8 *root lattice is the unique densest lattice in* $\mathbb{R}^8$, *up to scaling and isometries of* $\mathbb{R}^8$.

Our work is motivated by the paper [CE03] by Cohn and Elkies (see also [Coh02]), which proves upper bounds for the sphere packing density. In particular, the main theorem in [CE03] is an analogue for sphere packing of the linear programming bounds for error-correcting codes: given a function satisfying certain linear inequalities one can deduce a density bound. It is not known how to choose the function to optimize the bound, but in $\mathbb{R}^8$ and $\mathbb{R}^{24}$ one can come exceedingly close to the densities of E_8 and the Leech lattice, respectively. This observation, together with analogies with error-correcting codes and spherical codes, led Cohn and Elkies to conjecture that their bound is sharp in $\mathbb{R}^8$ and $\mathbb{R}^{24}$, which would solve the sphere packing problem in those dimensions. While we cannot yet fully carry out that program, in this paper we show how to combine the methods of [CE03] with results on lattices and combinatorics to deal with the special case of lattice packings. We will deal primarily with the Leech lattice, because that case is new and more difficult, but in Section 11 we will discuss E_8.

One might hope to use a relatively simple method. Section 8 of [CE03] shows how to prove that the Leech lattice is the unique densest periodic packing (i.e., union of finitely many translates of a lattice) in $\mathbb{R}^{24}$, if a function from $\mathbb{R}^{24}$ to $\mathbb{R}$ with certain properties exists. Using a computer, one can find functions that very nearly have those properties, and the techniques from Section 8 of [CE03] can then be used straightforwardly to prove an approximate version of the uniqueness result: every lattice that is at least as dense as the Leech lattice must be close to it. It is known (see [Mar03, p. 176]) that the Leech lattice is a strict local optimum for density, among lattices. Thus, if one can show that every denser lattice is sufficiently close, then it proves that the Leech lattice is the unique densest lattice in $\mathbb{R}^{24}$.

Unfortunately, this approach seems completely infeasible if carried out in the most straightforward way. When one naively imitates the techniques from Section 8 of [CE03] in an approximate setting, one loses a tremendous factor in the bounds, and that puts the required computer searches far beyond what we are capable of. In this paper we salvage the approach by using more sophisticated arguments that take advantage of special properties of the Leech lattice. In particular, we make use of three beautiful facts about the Leech lattice: its automorphism group acts transitively on pairs of minimal vectors with the same inner product, its minimal vectors form an association scheme when pairs are grouped according to their inner products, and its minimal vectors form a spherical 11-design. (Note that the second property follows from the first, but our work uses another proof of it, from [DGS77].)

Our proof depends on computer calculations in some places, but they can be carried out relatively quickly, in less than one hour using a personal computer. The calculations are all done using exact arithmetic and are thus rigorous. We have fully documented all of our calculations and made available commented code for use in checking the results or carrying out further investigations. See Appendix A for details.

Appendix B contains very brief introductions to several topics: the Leech lattice, linear programming bounds, spherical designs, and association schemes. For more details, see [CS99]. The expository articles [Elk00a] and [Elk00b] also provide useful background and context, although they do not include everything we need.

2. Outline of proof

We wish to show that the Leech lattice, henceforth denoted by Λ_{24}, is the unique densest sphere packing among all lattices in $\mathbb{R}^{24}$. Let Λ be any lattice in $\mathbb{R}^{24}$ that is at least as dense as Λ_{24}. Without loss of generality, we assume that Λ has covolume 1. Then the restriction on its density simply means its minimal vectors have length at least 2.

We first show, using linear programming bounds, that Λ has exactly 196560 vectors of length approximately 2 (called nearly minimal vectors), and that the next smallest vector length is approximately $\sqrt{6}$.

We rescale those 196560 nearly minimal vectors to lie on the unit sphere. Then they form a spherical code with minimal angle at least φ, where $\cos\varphi$ is very near to (and greater than or equal to) $1/2$. Note that in S^{23} there is a unique spherical code of this size with minimal angle $\pi/3 = \cos^{-1}(1/2)$, and it is the kissing arrangement of Λ_{24}; the spherical code derived from Λ should be a small perturbation of this configuration.

Using linear programming bounds, we show that the inner products of the unit vectors are approximately $0, \pm 1/4, \pm 1/2, \pm 1$. We prove that if pairs of vectors are grouped according to their inner products, then they form an association scheme with the same valencies and intersection numbers as in the case of Λ_{24}, and that it must therefore be the same association scheme. This isomorphism gives us a correspondence between minimal vectors of Λ_{24} and nearly minimal vectors of Λ, such that corresponding inner products are approximately equal.

Using this correspondence, we find a basis of Λ whose Gram matrix is close to the Gram matrix of a basis of Λ_{24}. Finally, from the strict local optimality of the Leech lattice we conclude that Λ must in fact be the Leech lattice.

3. Notation

We begin by recording our normalizations of some special functions (which are always as in [AAR99]), and by defining some notation.

The Laguerre polynomials $L_i^\alpha(z)$ are defined by the initial conditions $L_0^\alpha(z) = 1$ and $L_1^\alpha(z) = 1 + \alpha - z$ and the recurrence

$$iL_i^\alpha(z) = (2i - 1 + \alpha - z)L_{i-1}^\alpha(z) - (i + \alpha - 1)L_{i-2}^\alpha(z)$$

for $i \geq 2$. They are orthogonal polynomials with respect to the measure $e^{-x}x^\alpha\,dx$ on $[0,\infty)$. If $\alpha = n/2 - 1$, then the functions on $\mathbb{R}^n$ given by $x \mapsto e^{-\pi|x|^2}L_i^\alpha(2\pi|x|^2)$ form an orthogonal basis of the radial functions in $L^2(\mathbb{R}^n)$, and they are also eigenfunctions of the Fourier transform with eigenvalue $(-1)^i$ (see (4.20.3) in

[Leb72]). Here we normalize the Fourier transform by

$$\widehat{f}(t) = \int_{\mathbb{R}^n} f(x) e^{2\pi i \langle x,t\rangle}\, dx.$$

Note also that with this normalization of the Fourier transform, the Poisson summation formula states that

$$\sum_{x\in\Lambda} f(x) = \frac{1}{|\Lambda|} \sum_{t\in\Lambda^*} \widehat{f}(t),$$

if $f\colon \mathbb{R}^n \to \mathbb{R}$ is a Schwartz function, $\Lambda \subset \mathbb{R}^n$ is a lattice, and

$$\Lambda^* = \{y \in \mathbb{R}^n : \langle x, y\rangle \in \mathbb{Z} \text{ for all } x \in \Lambda\}$$

is its dual lattice. (See (28) in [Kha91, p. 49].)

The ultraspherical (or Gegenbauer) polynomials $C_i^\lambda(z)$ are defined by the initial conditions $C_0^\lambda(z) = 1$ and $C_1^\lambda(z) = 2\lambda z$ and the recurrence

$$iC_i^\lambda(z) = 2(i+\lambda-1)zC_{i-1}^\lambda(z) - (i+2\lambda-2)C_{i-2}^\lambda(z)$$

for $i \ge 2$. They are orthogonal polynomials with respect to the measure

$$(1-x^2)^{\lambda-1/2}\, dx$$

on $[-1, 1]$. When $\lambda = n/2-1$, that measure is proportional to the projection of the surface measure from S^{n-1} onto an axis, and the ultraspherical polynomials play a fundamental role in the theory of spherical harmonics in $\mathbb{R}^n$. Up to scaling, the ultraspherical polynomial C_i^λ is the same as the Jacobi polynomial $P_i^{(\alpha,\alpha)}$, where $\alpha = \lambda - 1/2$.

Whenever we use Laguerre or ultraspherical polynomials, we will always set $\alpha = \lambda = n/2-1$, where $n = 24$ in the Leech lattice proof and $n = 8$ in the E_8 proof. The term "ultraspherical coefficient" will mean a coefficient in the expansion of a polynomial as a linear combination of ultraspherical polynomials.

Throughout this paper, Λ_{24} will denote the Leech lattice, and Λ will denote any lattice in $\mathbb{R}^{24}$ that is at least as dense and satisfies $|\Lambda| = 1$ (except in §9, where Λ denotes an arbitrary lattice, and in §11, which deals with E_8). We think of Λ as being an optimal lattice, but we will not use that assumption. We do not even need to know *a priori* that a global optimum for density is achieved, although [GL87, §17.5] shows that it is.

Whenever $f\colon \mathbb{R}^n \to \mathbb{R}$ is a radial function and $r \in [0,\infty)$, we will write $f(r)$ for the common value $f(x)$ with $x \in \mathbb{R}^n$ satisfying $|x| = r$.

The surface volume of the unit sphere $S^{n-1} \subset \mathbb{R}^n$ will be denoted by

$$\mathrm{vol}(S^{n-1}) = n\frac{\pi^{n/2}}{(n/2)!}.$$

It is important to keep in mind that $\mathrm{vol}(S^{n-1})$ is not the volume of the enclosed ball.

We will make use of the numerical values

$$\begin{aligned}\varepsilon &= 6.733 \cdot 10^{-27},\\ \mu &= 3.981 \cdot 10^{-13},\\ \nu &= 3.219 \cdot 10^{-12}, \text{ and}\\ \omega &= 1.703 \cdot 10^{-11}\end{aligned}$$

throughout the paper. Each will be defined the first time it is used, but we have collected the values here for easy reference. Note that terminating decimal expansions such as these represent exact rational numbers, not floating point approximations.

4. Nearly minimal vectors

In this section, we show that Λ must have exactly 196560 vectors of length near 2 (this will be made more precise below). The first subsection examines which vector lengths are possible in Λ, and the second then counts the nearly minimal vectors.

4.1. *Restrictions on the lengths of vectors.* Let $f : \mathbb{R}^{24} \to \mathbb{R}$ be a radial Schwartz function with the following properties: $f(0) = \widehat{f}(0) = 1$, $f(x) \leq 0$ for $|x| \geq r$ (for some number r), and $\widehat{f}(t) \geq 0$ for all t. Proposition 3.2 of [CE03] says that if such a function exists, then the sphere packing density in $\mathbb{R}^{24}$ is bounded above by

$$\frac{\pi^{12}}{12!}\left(\frac{r}{2}\right)^{24}.$$

If we could find such a function with $r = 2$, then it would prove that Λ_{24} has the greatest density among all sphere packings in $\mathbb{R}^{24}$, not just lattice packings. Cohn and Elkies conjecture that such a function exists, but the best they achieve in [CE03] is $r \leq 2 \cdot 1.00002946$.

Our proof begins by constructing an explicit function f with

$$r \leq 2\big(1 + 6.851 \cdot 10^{-32}\big).$$

Note that the existence of such a function proves that no sphere packing in $\mathbb{R}^{24}$ can have density greater than $1 + 1.65 \cdot 10^{-30}$ times the density of Λ_{24}.

Unfortunately, the function we construct is extremely complicated (it would take far too much space to write it down here). It consists of a polynomial of degree 803 with rational coefficients, evaluated at $2\pi|x|^2$ and multiplied by $e^{-\pi|x|^2}$. It was constructed by a lengthy computer calculation to optimize the value of r using Newton's method, and even verifying that it has the properties used below requires a computer, although fortunately that is much easier than finding the function. The accompanying computer file `verifyf.txt` includes code to verify all the assertions about f in this subsection of the paper. See Appendix A for details.

We can use techniques similar to those in [CE03] to study the size of the short vectors in Λ. First, we need two lemmas. Set

$$\varepsilon = 6.733 \cdot 10^{-27},$$

and call a nonzero vector in Λ *nearly minimal* if it has length at most $2(1+\varepsilon)$. The reason for this choice of ε will be apparent from Proposition 4.3 below.

Consider what happens if we rescale the nearly minimal vectors so that they all lie on the unit sphere. These vectors determine a spherical code

$$\mathscr{C}_\Lambda = \{u/|u| : u \text{ a nearly minimal vector}\}$$

on the unit sphere S^{23}, and the following lemma bounds its minimal angle. (See Appendix B for background on spherical codes.)

LEMMA 4.1. *If u and v are nearly minimal vectors with $u \neq v$, then the angle φ between u and v satisfies*

$$\cos\varphi \le 1 - \frac{1}{2(1+\varepsilon)^2}.$$

Proof. We have $|u|, |v| \in [2, 2(1+\varepsilon)]$ and $|u-v| \ge 2$. By the law of cosines,

$$\cos\varphi = \frac{|u|^2 + |v|^2 - |u-v|^2}{2|u||v|} \le \frac{|u|^2+|v|^2-4}{2|u||v|}.$$

The bound $(|u|^2+|v|^2-4)/(2|u||v|)$ is convex as a function of $|u|$ and $|v|$ individually, and hence it is maximized at one of the vertices of the square $[2, 2(1+\varepsilon)]^2$. In fact, the maximum occurs when $|u| = |v| = 2(1+\varepsilon)$, in which case the bound becomes

$$1 - \frac{1}{2(1+\varepsilon)^2}. \qquad \square$$

LEMMA 4.2. *There are at most* 196560 *nearly minimal vectors in* Λ.

Proof. This lemma is a straightforward application of the linear programming bounds for spherical codes (see Chapter 9 of [CS99], or Appendix B for a brief summary). Let

$$f_\varepsilon(x) = K_\varepsilon(x+1)\left(x+\frac{1}{2}\right)^2\left(x+\frac{1}{4}\right)^2 x^2 \left(x-\frac{1}{4}\right)^2\left(x - \left(1 - \frac{1}{2(1+\varepsilon)^2}\right)\right),$$

where the constant K_ε is chosen so that f_ε has zeroth ultraspherical coefficient 1. (The normalization is irrelevant for this proof, but it will be important later in the paper, so we use it here for consistency.) If ε were 0, this polynomial would be the one used to solve the kissing problem exactly in $\mathbb{R}^{24}$ (see Chapter 13 of [CS99]). With the current value of ε, the polynomial f_ε has nonnegative ultraspherical coefficients and still proves that there are fewer than 196561 spheres in any spherical code in $\mathbb{R}^{24}$ with minimal angle as in Lemma 4.1. (We check this assertion in the computer file `verifyrest.txt`. In fact, the bound is less than $196560 + 10^{-19}$.) Thus, there can be at most 196560 nearly minimal vectors in Λ. □

In addition to the definition of ε above, set

$$\begin{aligned} \mu &= 3.981 \cdot 10^{-13}, \\ \nu &= 3.219 \cdot 10^{-12}, \text{ and} \\ \omega &= 1.703 \cdot 10^{-11}. \end{aligned}$$

PROPOSITION 4.3. *Every nonzero vector in* Λ *has length in*

$$\big[2, 2(1+\varepsilon)\big) \cup \big(\sqrt{6}(1-\mu), \sqrt{6}(1+\mu)\big) \cup \big(\sqrt{8}(1-\nu), \sqrt{8}(1+\nu)\big) \cup \big(\sqrt{10}(1-\omega), \infty\big).$$

Proof. By the Poisson summation formula,

$$\sum_{x \in \Lambda} f(x) = \sum_{t \in \Lambda^*} \widehat{f}(t).$$

Because Λ is at least as dense as Λ_{24} (and has covolume 1), all nonzero vectors $x \in \Lambda$ satisfy $|x| \geq 2$. Because $r \leq 2(1+\varepsilon)$, by Lemma 4.2 there can be at most 196560 vectors in Λ with $2 \leq |x| \leq r$. Within that range, f is a decreasing function of the radius, and we have

$$196560 f(2) < 1.644104221 \cdot 10^{-30}$$

(recall from §3 that $f(2)$ denotes the common value $f(x)$ with $|x| = 2$).

The key properties of f are $f(0) = \widehat{f}(0) = 1$, $f(x) \leq 0$ for $|x| \geq r$, and $\widehat{f}(t) \geq 0$ for all t. It follows that

$$1 + 1.644104221 \cdot 10^{-30} + \sum_{x \in \mathcal{N}} f(x) \geq 1,$$

where $\mathcal{N}$ is the set of vectors in Λ at which f is negative. No vector in Λ can occur within any region on which f is less than $(1/2)(-1.644104221) \cdot 10^{-30}$; the extra factor of 2 comes from the fact that $f(-x) = f(x)$ since f is a radial function (if $x \in \mathcal{N}$ then $-x \in \mathcal{N}$ as well). That rules out all radii in the set

$$\big[2(1+\varepsilon), \sqrt{6}(1-\mu)\big] \cup \big[\sqrt{6}(1+\mu), \sqrt{8}(1-\nu)\big] \cup \big[\sqrt{8}(1+\nu), \sqrt{10}(1-\omega)\big].$$

In the computer file `verifyf.txt` we prove this by examining the radial derivative of f. □

Much of the rest of the proof would still work if ε, μ, ν, and ω were somewhat larger. The two main places where they must be small are the final inequality (9.4) and the intersection number calculations in Subsection 6.2 (as well as the bounds used there). In each case they could be slightly larger, but not by a factor of 100.

4.2. 196560 *nearly minimal vectors.* We can now show that there are exactly 196560 nearly minimal vectors. We know from Lemma 4.2 that there are at most 196560 of them. For the other direction, a lower bound greater than 196559, we need a new kind of linear programming bound. Recall that we have shown that all nonzero vectors in Λ are either nearly minimal or have lengths greater than $\sqrt{6}(1-\mu)$.

Suppose we knew that all nonzero vectors either have length exactly 2 or at least $\sqrt{6}$. (We will first explain our method under these overly optimistic hypotheses. Lemma 4.4 will then apply it using the actual bounds we have proved.) One might hope to count the nearly minimal vectors using a Schwartz function $g\colon \mathbb{R}^{24} \to \mathbb{R}$ such that $g(x) \le 0$ for $|x| \ge \sqrt{6}$, $\widehat{g}(t) \ge 0$ for all t, and $g(2) > 0$. Given such a function, Poisson summation implies that

$$\sum_{x\in\Lambda} g(x) = \sum_{t\in\Lambda^*} \widehat{g}(t),$$

and hence

$$g(0) + Ng(2) \ge \widehat{g}(0)$$

if there are N minimal vectors. Thus, $N \ge (\widehat{g}(0) - g(0))/g(2)$. We conjecture that g can be chosen so that $(\widehat{g}(0) - g(0))/g(2) = 196560$, which is the largest possible value because the Leech lattice has 196560 minimal vectors. We can construct functions that come quite close to this bound, and will use one of them to prove the following lemma.

LEMMA 4.4. *There are more than* 196559 *nearly minimal vectors in* Λ.

Proof. Define $z_1, \dots, z_{10}$ by $z_i = \lfloor 4\pi(i+1)10^8 \rfloor / 10^8$. In other words, they have the following values:

i	1	2	3	4	5
z_i	25.13274122	37.69911184	50.26548245	62.83185307	75.39822368

i	6	7	8	9	10
z_i	87.96459430	100.53096491	113.09733552	125.66370614	138.23007675

There are unique coefficients $a_1, \dots, a_{37}$ such that

$$1 + \sum_{i=1}^{37} a_i L_i^{11}(x)$$

has a single root at z_2 and a double root at z_i for $i \ge 3$, and

$$1 + \sum_{i=1}^{37} (-1)^i a_i L_i^{11}(x)$$

has a double root at each z_i for $i \ge 1$. Neither polynomial has any other nonnegative roots. (We check this in the computer file `verifyg.txt` using Sturm's theorem, except that we do not check the uniqueness of the coefficients because we do not require it.)

Define $g\colon \mathbb{R}^{24} \to \mathbb{R}$ by

$$g(x) = \left(1 + \sum_{i=1}^{37} a_i L_i^{11}(2\pi|x|^2)\right) e^{-\pi|x|^2}.$$

It follows that

$$\widehat{g}(t) = \left(1 + \sum_{i=1}^{37} (-1)^i a_i L_i^{11}(2\pi|x|^2)\right) e^{-\pi|x|^2}.$$

We have $g(x) \le 0$ for $|x| \ge \sqrt{6}(1-\mu)$, because $z_2 < 2\pi \cdot 6(1-\mu)^2$, the function g changes sign only at z_2, and $g(0) > 0$. For all t, we have $\widehat{g}(t) \ge 0$.

Apply Poisson summation to g, to deduce

$$\sum_{x \in \Lambda} g(x) = \sum_{t \in \Lambda^*} \widehat{g}(t).$$

Applying the two inequalities above shows that

$$g(0) + \sum_{x \in \mathcal{M}} g(x) \ge \widehat{g}(0),$$

where $\mathcal{M}$ is the set of nearly minimal vectors. The function $g(x)$ is positive and a decreasing function of $|x|$ on the interval $[2, 2(1+\varepsilon)]$, so

$$g(0) + |\mathcal{M}| g(2) \ge \widehat{g}(0).$$

However,

$$\frac{\widehat{g}(0) - g(0)}{g(2)} > 196559,$$

so there are more than 196559 nearly minimal vectors. (All these inequalities are checked in `verifyg.txt`.) □

Thus, there must be exactly 196560 nearly minimal vectors, as desired. We conjecture that this method could be used to recover each of the coefficients of the Leech lattice's theta series, but we will not need that for our proof.

5. Inner products in the spherical code

We now continue to study the polynomial

$$f_\varepsilon(x) = K_\varepsilon(x+1)\left(x + \frac{1}{2}\right)^2 \left(x + \frac{1}{4}\right)^2 x^2 \left(x - \frac{1}{4}\right)^2 \left(x - \left(1 - \frac{1}{2(1+\varepsilon)^2}\right)\right)$$

from the previous section.

Note that

$$1 - \frac{1}{2(1+\varepsilon)^2} < \frac{1}{2} + \varepsilon.$$

Thus, all the inner products except 1 in the spherical code $\mathscr{C}_\Lambda$ are at most $1/2+\varepsilon$. We seek bounds for how far from $0, \pm 1/4, \pm 1/2, \pm 1$ they can be. The ± 1 cases must be exact, because of Lemma 4.1 and the fact that $u \in \mathscr{C}_\Lambda$ if and only if $-u \in \mathscr{C}_\Lambda$ (i.e., the code is antipodal).

Because the zeroth ultraspherical coefficient of f_ε is 1, it follows from the usual proof of the linear programming bounds for spherical codes (see Appendix B) that

$$196560 f_\varepsilon(1) + \sum_{x \neq y} f_\varepsilon(\langle x, y\rangle) \geq 196560^2,$$

where the sum is over vectors in the spherical code. Because the four inner products $\langle x, y\rangle$, $\langle -x, -y\rangle$, $\langle y, x\rangle$, and $\langle -y, -x\rangle$ are all equal, and all the terms in the sum are nonpositive, we see that no term in the sum can be less than

$$\frac{196560^2 - 196560 f_\varepsilon(1)}{4},$$

which is approximately $-1.99 \cdot 10^{-15}$.

Now a short calculation implies that all the inner products must be within $6.411 \cdot 10^{-9}$ of one of the numbers $0, \pm 1/4, \pm 1/2, \pm 1$. The exponent is only 9 because f_ε has double roots, and one can stray quite far from a double root without substantially changing the function's value.

In the rest of the paper, we make the following definition: let

$$\sigma = \max_{u,v \in \mathscr{C}_\Lambda} \min\{|\langle u, v\rangle - \alpha| : \alpha \in S\},$$

where $S = \{0, \pm 1/4, \pm 1/2, \pm 1\}$. In other words, σ is the maximum "error" in the inner products. We have just shown that $\sigma \leq 6.411 \cdot 10^{-9}$. We will improve the upper bound for σ substantially, and ultimately we will show $\sigma = 0$.

5.1. *Better bounds for σ.* Recall that we computed in Section 4.1 that vectors of Λ with length close to $\sqrt{6}$ must have length in the interval $\big(\sqrt{6}(1-\mu), \sqrt{6}(1+\mu)\big)$. Therefore if we have nearly minimal vectors u, v with $\langle u, v\rangle \approx 1$ (with error less than 10^{-3}, say), then we see that $|u - v| \approx \sqrt{6}$. Therefore

$$6(1-\mu)^2 \leq \langle u, u\rangle + \langle v, v\rangle - 2\langle u, v\rangle \leq 6(1+\mu)^2.$$

In addition we have

$$4 \leq \langle u, u\rangle \leq 4(1+\varepsilon)^2.$$

Therefore

$$8 - 6(1+\mu)^2 \leq 2\langle u, v\rangle \leq 8(1+\varepsilon)^2 - 6(1-\mu)^2,$$

so

$$\frac{4-3(1+\mu)^2}{4(1+\varepsilon)^2} \leq \left\langle \frac{u}{|u|}, \frac{v}{|v|} \right\rangle \leq (1+\varepsilon)^2 - \frac{3}{4}(1-\mu)^2.$$

Similarly we get for $\langle u, v\rangle \approx 0$ that

$$\frac{1-(1+\nu)^2}{(1+\varepsilon)^2} \leq \left\langle \frac{u}{|u|}, \frac{v}{|v|} \right\rangle \leq (1+\varepsilon)^2 - (1-\nu)^2,$$

and for $\langle u, v\rangle \approx 2$ that

$$\frac{2-(1+\varepsilon)^2}{2(1+\varepsilon)^2} \leq \left\langle \frac{u}{|u|}, \frac{v}{|v|} \right\rangle \leq (1+\varepsilon)^2 - \frac{1}{2}$$

because $2 \leq |u-v| \leq 2(1+\varepsilon)$. Combining these (and if necessary replacing v with $-v$), we find that for $u \neq \pm v$, the inner product $\langle u/|u|, v/|v|\rangle$ differs from an element of $\{0, \pm 1/4, \pm 1/2\}$ by at most $6.43801 \cdot 10^{-12}$. We conclude that the error σ in the inner products is at most $6.43801 \cdot 10^{-12}$.

However, we will be able to get much better bounds in Section 7, once we have shown that the spherical code $\mathscr{C}_\Lambda$ gives us an association scheme.

6. Association schemes

We would like to turn the 196560 points in the spherical code $\mathscr{C}_\Lambda$ into a 6-class association scheme by grouping pairs according to their approximate inner products. (See Appendix B for background on association schemes.) It is not clear that this in fact defines an association scheme, but we will show that it does. Furthermore, we will show that this association scheme is isomorphic to the one derived from Λ_{24}. To achieve this, we show that the intersection numbers are the same as in Λ_{24}. That will also show that it is an association scheme, by showing that the intersection numbers are independent of the pair of points. We use the same techniques as [DGS77], but we need to keep track of error bounds.

6.1. *Spherical design.* First, we show that $\mathscr{C}_\Lambda$ is nearly a spherical 10-design. (See Appendix B for background on spherical designs.) Let

$$C_i(x) = \frac{C_i^{11}(x)}{C_i^{11}(1)} \cdot \frac{\binom{22+i}{22} + \binom{21+i}{22}}{\mathrm{vol}(S^{23})}.$$

The advantage of this normalization of the ultraspherical polynomials is that for every finite subset $\mathscr{C}$ of S^{23},

$$\sum_{x,y\in\mathscr{C}} C_i(\langle x, y\rangle) = \left|\sum_{z\in\mathscr{C}} \mathrm{ev}_i(z)\right|^2,$$

where $\mathrm{ev}_i(z)$ denotes the evaluation at z map in the dual space to the i-th degree spherical harmonics. Although this fact is well known (e.g., it is equivalent to Theorem 9.6.3 in [AAR99]), we will explain it here for completeness, because the correct normalization is important for our application.

LEMMA 6.1. *If $\mathscr{C}$ is a finite subset of S^{23}, then*

$$\sum_{x,y\in\mathscr{C}} C_i(\langle x,y\rangle) = \left|\sum_{z\in\mathscr{C}} \mathrm{ev}_i(z)\right|^2.$$

Proof. Let d be the dimension of the space of spherical harmonics of degree i, and let $S_1,\dots,S_d$ be an orthonormal basis of that space. By Theorem 9.6.3 of [AAR99],

$$\sum_{j=1}^{d} S_j(w)S_j(z) = C_i(\langle w,z\rangle).$$

Let $f=\sum_j a_j S_j$ be any spherical harmonic of degree i. Then

$$\begin{aligned}
(\mathrm{ev}_i(z))(f) &= \sum_{j=1}^{d} a_j S_j(z)\\
&= \sum_{j=1}^{d} S_j(z)\int_{S^{23}} S_j(w)f(w)\,dw\\
&= \int_{S^{23}}\left(\sum_{j=1}^{d} S_j(w)S_j(z)\right) f(w)\,dw\\
&= \int_{S^{23}} C_i(\langle w,z\rangle) f(w)\,dw.
\end{aligned}$$

Thus,

$$\left(\sum_{z\in\mathscr{C}} \mathrm{ev}_i(z)\right)(f) = \int_{S^{23}}\left(\sum_{z\in\mathscr{C}} C_i(\langle w,z\rangle)\right) f(w)\,dw.$$

In other words, applying the element $\sum_{z\in\mathscr{C}} \mathrm{ev}_i(z)$ of the dual space is the same as taking the inner product with

$$w\mapsto \sum_{z\in\mathscr{C}} C_i(\langle w,z\rangle).$$

It follows that

$$\begin{aligned}\left|\sum_{z\in\mathscr{C}} \mathrm{ev}_i(z)\right|^2 &= \int_{S^{23}} \left(\sum_{z\in\mathscr{C}} C_i(\langle w,z\rangle)\right)^2 dw\\ &= \sum_{x,y\in\mathscr{C}} \int_{S^{23}} C_i(\langle w,x\rangle)C_i(\langle w,y\rangle)\,dw\\ &= \sum_{x,y\in\mathscr{C}} (\mathrm{ev}_i(x))(w\mapsto C_i(\langle w,y\rangle))\\ &= \sum_{x,y\in\mathscr{C}} C_i(\langle x,y\rangle),\end{aligned}$$

as desired. □

The following lemma asserts that $\mathscr{C}_\Lambda$ is nearly a spherical 10-design:

LEMMA 6.2. *If* $g\colon S^{23}\to\mathbb{R}$ *is a polynomial of total degree at most* 10, *then*

$$\left|\sum_{z\in\mathscr{C}_\Lambda} g(z) - \frac{196560}{\mathrm{vol}(S^{23})}\int_{S^{23}} g(z)\,dz\right| \le 2.50193\cdot 10^{-5}|g|_2,$$

where $|g|_2$ *denotes the norm on* $L^2(S^{23})$.

Proof. Without loss of generality we may assume that g is a harmonic polynomial (for every polynomial on $\mathbb{R}^{24}$, there is a harmonic polynomial of equal or lesser degree with the same restriction to S^{23}; see equation (5) in [Hel00, p. 17]). We will use the polynomial

$$f_\varepsilon(x) = K_\varepsilon(x+1)\left(x+\frac{1}{2}\right)^2\left(x+\frac{1}{4}\right)^2 x^2\left(x-\frac{1}{4}\right)^2\left(x-\left(1-\frac{1}{2(1+\varepsilon)^2}\right)\right)$$

from earlier in the paper. Recall that f_ε is normalized to have zeroth ultraspherical coefficient 1 (by the standard normalization of the ultraspherical polynomials, not the new normalization C_i). If c_i denotes the coefficient of C_i in f_ε, then

$$\begin{aligned}196560 f_\varepsilon(1) &\ge \sum_{x,y\in\mathscr{C}_\Lambda} f_\varepsilon(\langle x,y\rangle)\\ &= 196560^2 + \sum_{i=1}^{10} c_i \sum_{x,y\in\mathscr{C}} C_i(\langle x,y\rangle)\\ &= 196560^2 + \sum_{i=1}^{10} c_i \left|\sum_{z\in\mathscr{C}_\Lambda} \mathrm{ev}_i(z)\right|^2,\end{aligned}$$

from which it follows that

$$\sum_{i=1}^{10} c_i \left| \sum_{z \in \mathscr{C}_\Lambda} \mathrm{ev}_i(z) \right|^2 \le 196560 f_\varepsilon(1) - 196560^2 < 7.9775 \cdot 10^{-15}.$$

Therefore,

$$\sum_{i=1}^{10} \left| \sum_{z \in \mathscr{C}_\Lambda} \mathrm{ev}_i(z) \right|^2 \le \left(7.9775 \cdot 10^{-15}\right) \max_i \frac{1}{c_i} < 6.25964 \cdot 10^{-10}.$$

We can now bound

$$\left| \sum_{z \in \mathscr{C}_\Lambda} g(z) - \frac{196560}{\mathrm{vol}(S^{23})} \int_{S^{23}} g(z)\, dz \right|.$$

Write $g = \sum_{i=0}^{10} g_i$, where g_i is homogeneous of degree i. The integral cancels with the g_0 term in the sum, so we simply need to bound

$$\left| \sum_{i=1}^{10} \sum_{z \in \mathscr{C}_\Lambda} g_i(z) \right|.$$

For that, we use the definition of the norm and the Cauchy-Schwarz inequality to deduce that

$$\begin{aligned} \left| \sum_{i=1}^{10} \sum_{z \in \mathscr{C}_\Lambda} g_i(z) \right| &\le \sum_{i=1}^{10} \left| \sum_{z \in \mathscr{C}_\Lambda} \mathrm{ev}_i(z) \right| |g_i|_2 \\ &\le \sqrt{\sum_{i=1}^{10} \left| \sum_{z \in \mathscr{C}_\Lambda} \mathrm{ev}_i(z) \right|^2} \sqrt{\sum_{i=1}^{10} |g_i|_2^2} \\ &\le 2.50193 \cdot 10^{-5} |g|_2, \end{aligned}$$

as desired. □

In fact, it follows immediately that $\mathscr{C}_\Lambda$ is nearly a spherical 11-design in the same sense, because it is antipodal (if $x \in \mathscr{C}_\Lambda$ then $-x \in \mathscr{C}_\Lambda$) and thus every homogeneous polynomial of odd degree averages to 0 over $\mathscr{C}_\Lambda$. However, we will not need that fact.

It is worth pointing out for completeness that the minimal vectors in Λ_{24} do not form a spherical 12-design: if y is a minimal vector then the polynomial

$$\left(16 - \langle x, y\rangle^2\right) \left(4 - \langle x, y\rangle^2\right)^2 \left(1 - \langle x, y\rangle^2\right)^2 \langle x, y\rangle^2$$

in x vanishes at each minimal vector but does not average to 0 over the sphere of radius 2, because it is nonnegative on that sphere.

The constant $2.50193 \cdot 10^{-5}$ in Lemma 6.2 can be made somewhat smaller for polynomials of total degree at most 8 (using the same proof), and that is the only case we need later. However, the present bound suffices.

6.2. *Intersection numbers.* We will now use the fact that $\mathscr{C}_\Lambda$ is nearly a spherical 10-design to determine the intersection numbers (still following the techniques of [DGS77]). As a computational aid, it is useful to know the following formula for averaging homogeneous polynomials over the sphere:

$$\frac{1}{\mathrm{vol}(S^{23})} \int_{S^{23}} g(z)\, dz = \frac{\int_{\mathbb{R}^{24}} g(z) e^{-|z|^2}\, dz}{\int_0^\infty r^{\deg g} e^{-r^2} \mathrm{vol}(S^{23}) r^{23}\, dr}.$$

In the exact case of Λ_{24}, we can compute the intersection numbers as follows. For each $x, y \in \mathscr{C}_{24}$ (the spherical code derived from the minimal vectors) with a specified inner product, we need to determine the number of $z \in \mathscr{C}_{24}$ with specified inner products with x and y. Let $P_\gamma(\alpha, \beta)$ denote this number when $\langle x, y\rangle = \gamma$, $\langle x, z\rangle = \alpha$, and $\langle y, z\rangle = \beta$. The cases $\gamma = \pm 1$ simply amount to the valencies, which are determined automatically once the other intersection numbers are determined. For instance $P_1(\alpha, \beta) = 0$ unless $\alpha = \beta$, and $P_1(\alpha, \alpha) = \sum_\beta P_0(\alpha, \beta)$ once we demonstrate that every vector in $\mathscr{C}_{24}$ has a vector in $\mathscr{C}_{24}$ orthogonal to it (which follows from, say, showing that $P_\alpha(0, 0) \neq 0$ for each $\alpha \neq \pm 1$). Hence we will focus on the remaining cases, i.e., $\gamma \neq \pm 1$.

For such a pair (x, y) with $\langle x, y\rangle = \gamma$, *a priori* there are 49 unknowns $P_\gamma(\alpha, \beta)$ for $\alpha, \beta \in \{-1, -1/2, -1/4, 0, 1/4, 1/2, 1\}$. We first note that $P_\gamma(1, \alpha) = P_\gamma(\alpha, 1) = \delta_{\alpha,\gamma}$, where δ is the Kronecker delta. Similarly $P_\gamma(-1, \alpha) = P_\gamma(\alpha, -1) = \delta_{\gamma,-\alpha}$. Thus we can eliminate ± 1 from consideration, which reduces the problem to finding only 25 unknowns. We will find 25 linear equations that determine these values.

Consider the polynomials $g_{i,j}(z) = \langle z, x\rangle^i \langle z, y\rangle^j$ for $i, j \in \{0, 1, \dots, 4\}$. Let S be the set $\{-1, -1/2, -1/4, 0, 1/4, 1/2, 1\}$. We then know that

$$\sum_{\alpha,\beta \in S} \alpha^i \beta^j P_\gamma(\alpha, \beta) = \frac{196560}{\mathrm{vol}(S^{23})} \int_{S^{23}} g_{i,j}(z)\, dz,$$

because $\mathscr{C}_{24}$ is a spherical 11-design (although even an 8-design would suffice). These equations can be solved to yield the unknown values of $P_\gamma(\alpha, \beta)$. Note that the right-hand side does not depend on the choice of x and y, only on $\gamma = \langle x, y\rangle$. Therefore we see that the solutions of these equations, which are the intersection numbers, are independent of x, y and only depend on γ. We solve one such system of equations for each value of γ, and the values of the intersection numbers are

$P_0(0,0) = 43164$	$P_0(0,1/2) = 2464$	$P_0(0,1/4) = 22528$
$P_0(1/2,1/2) = 44$	$P_0(1/2,1/4) = 1024$	$P_0(1/4,1/4) = 11264$
$P_{1/2}(0,0) = 49896$	$P_{1/2}(0,1/2) = 891$	$P_{1/2}(0,1/4) = 20736$
$P_{1/2}(1/2,1/2) = 891$	$P_{1/2}(1/2,-1/2) = 1$	$P_{1/2}(1/2,1/4) = 2816$
$P_{1/2}(1/2,-1/4) = 0$	$P_{1/2}(1/4,1/4) = 20736$	$P_{1/2}(1/4,-1/4) = 2816$
$P_{1/4}(0,0) = 44550$	$P_{1/4}(0,1/2) = 2025$	$P_{1/4}(0,1/4) = 22275$
$P_{1/4}(1/2,1/2) = 275$	$P_{1/4}(1/2,-1/2) = 0$	$P_{1/4}(1/2,1/4) = 2025$
$P_{1/4}(1/2,-1/4) = 275$	$P_{1/4}(1/4,1/4) = 15400$	$P_{1/4}(1/4,-1/4) = 7128$

Table 1. Intersection numbers for the Leech lattice minimal vectors.

tabulated in Table 1, which is a complete list modulo the symmetries

$$P_\gamma(\alpha,\beta) = P_\gamma(\beta,\alpha) = P_\gamma(-\alpha,-\beta) = P_{-\gamma}(\alpha,-\beta).$$

(These numbers are of course known, but they are not tabulated in standard references such as [CS99], so we record them here for convenience.)

What happens when we are not necessarily dealing with exactly Λ_{24}, but rather with Λ? Suppose we have $x, y \in \mathscr{C}_\Lambda$ and we want to determine the number of $z \in \mathscr{C}_\Lambda$ with specified approximate inner products with them. Let $\widetilde{P}_\gamma(\alpha,\beta)$ denote the intersection numbers for $\mathscr{C}_\Lambda$ (which may depend on x and y); here we use α, β, and γ to denote exact elements of $\{0, \pm 1/4, \pm 1/2, \pm 1\}$, and the inner products from $\mathscr{C}_\Lambda$ are required to be approximately equal to them. Then we have

$$\begin{aligned}\sum_{\alpha,\beta\in S} \alpha^i \beta^j\, \widetilde{P}_\gamma(\alpha,\beta) &= \sum_{w\in\mathscr{C}_\Lambda, \langle w,x\rangle\approx\alpha, \langle w,y\rangle\approx\beta} \alpha^i\beta^j\\ &\approx \sum_{w\in\mathscr{C}_\Lambda} \langle w,x\rangle^i \langle w,y\rangle^j\\ &= \sum_{w\in\mathscr{C}_\Lambda} g_{i,j}(w)\\ &\approx \frac{196560}{\mathrm{vol}(S^{23})}\int_{S^{23}} g_{i,j}(z)\,dz\\ &\approx \frac{196560}{\mathrm{vol}(S^{23})} G_{i,j}(\gamma),\end{aligned}$$

where

$$G_{i,j}(\gamma) = \int_{S^{23}} \langle z,u\rangle^i \langle z,v\rangle^j\,dz$$

with $\langle u,v\rangle = \gamma$ (recall that $\langle x,y\rangle \approx \gamma$).

If these approximations are close enough, we should get about the same values for $\widetilde{P}_\gamma(\alpha, \beta)$ as we did for $P_\gamma(\alpha, \beta)$, and this will show that the intersection numbers must be the same.

LEMMA 6.3. *Let* $\alpha, \beta \in \{0, \pm 1/4, \pm 1/2, \pm 1\}$ *and* $a, b \in [-(1/2+\sigma), 1/2+\sigma] \cup \{\pm 1\}$ *with* $\max\{|a-\alpha|, |b-\beta|\} \le \sigma < 0.1$. *Then for* $i, j \ge 0$,

$$|a^i b^j - \alpha^i \beta^j| \le (1+2\sigma)\sigma.$$

Proof. We begin by bounding $|\alpha^i - a^i|$. For $i = 0$ or $\alpha \in \{\pm 1\}$, $\alpha^i = a^i$, so we can assume that $i > 0$ and $\alpha \in \{0, \pm 1/4, \pm 1/2\}$. Then

$$\alpha^i - a^i = (\alpha - a) \sum_{k=0}^{i-1} \alpha^k a^{i-1-k}.$$

If we apply the triangle inequality (together with $|\alpha - a| \le \sigma$ and $|\alpha|, |a| \le 1/2+\sigma$), we find that

$$|\alpha^i - a^i| \le i(1/2+\sigma)^{i-1}\sigma. \tag{6.1}$$

The function $n(1/2+\sigma)^{n-1}$ on nonnegative integers attains its maximum value when $n = 2$, from which it follows that $|\alpha^i - a^i| \le (1+2\sigma)\sigma$. Note that this is the special case of the lemma in which $\beta = b = \pm 1$. Thus, we can henceforth assume that neither β nor b is ± 1, and by symmetry we can assume the same for α and a.

For the general case, we notice that

$$\alpha^i \beta^j - a^i b^j = (\alpha^i - a^i)\beta^j + a^i(\beta^j - b^j),$$

so

$$|\alpha^i \beta^j - a^i b^j| \le |\alpha^i - a^i| \cdot |\beta^j| + |a^i| \cdot |\beta^j - b^j|.$$

It now follows from (6.1) that

$$|\alpha^i \beta^j - a^i b^j| \le (i+j)(1/2+\sigma)^{i+j-1}\sigma.$$

The right-hand side is at most $(1+2\sigma)\sigma$, as before. $\square$

Now we need to make precise the errors in all three approximations in

$$\begin{aligned}\sum_{\alpha,\beta \in S} \alpha^i \beta^j \widetilde{P}_\gamma(\alpha, \beta) &\approx \sum_{w \in \mathscr{C}_\Lambda} g_{i,j}(w) \\ &\approx \frac{196560}{\mathrm{vol}(S^{23})} \int_{S^{23}} g_{i,j}(z)\, dz \\ &\approx \frac{196560}{\mathrm{vol}(S^{23})} G_{i,j}(\gamma).\end{aligned}$$

The first follows from Lemma 6.3:

$$\left|\sum_{\alpha,\beta\in S}\alpha^i\beta^j\widetilde{P}_\gamma(\alpha,\beta)-\sum_{w\in\mathscr{C}_\Lambda}g_{i,j}(w)\right|\le\sum_{w\in\mathscr{C}_\Lambda}(1+2\sigma)\sigma=196560(1+2\sigma)\sigma,$$

because $|\alpha^i\beta^j-a^ib^j|\le(1+2\sigma)\sigma$ for $\langle w,x\rangle=a\approx\alpha$ and $\langle w,y\rangle=b\approx\beta$.

The second we have already estimated sufficiently well in Lemma 6.2, in terms of $|g_{i,j}|_2$. Because $|g_{i,j}(z)|\le 1$ for all z, we have

$$|g_{i,j}|_2\le\sqrt{\operatorname{vol}(S^{23})}=\sqrt{24\cdot\frac{\pi^{12}}{12!}}=\frac{\pi^6}{\sqrt{19958400}}.$$

It follows that

$$\left|\sum_{w\in\mathscr{C}_\Lambda}g_{i,j}(w)-\frac{196560}{\operatorname{vol}(S^{23})}\int_{S^{23}}g_{i,j}(z)\,dz\right|$$
$$\le\frac{\pi^6}{\sqrt{19958400}}\cdot 2.50193\cdot 10^{-5}<5.3841\cdot 10^{-6}.$$

Finally, one can check by straightforward computation of each case that if $\langle x,y\rangle$ differs from one of $-1/2,-1/4,0,1/4,1/2$ by at most σ (where $0\le\sigma\le 1$), and $0\le i,j\le 4$, then

$$\frac{196560}{\operatorname{vol}(S^{23})}\int_{S^{23}}g_{i,j}(z)\,dz$$

differs by at most 8190σ from what it would be if σ were zero. (In fact, if one expands this quantity as a power series in σ, then the sum of the absolute values of the coefficients is at most 8190.) Therefore the error in the last approximation is at most 8190σ.

Thus

$$\sum_{\alpha,\beta\in S}\alpha^i\beta^j\widetilde{P}_\gamma(\alpha,\beta)=\frac{196560}{\operatorname{vol}(S^{23})}G_{i,j}(\gamma)+D_{i,j},$$

where

$$|D_{i,j}|<196560(1+2\sigma)\sigma+8190\sigma+5.3841\cdot 10^{-6}<6.7023\cdot 10^{-6}.$$

As before the values of $\tilde{P}_\gamma(\pm1,\alpha)$ and $\tilde{P}_\gamma(\alpha,\pm1)$ are known and are the same as the corresponding $P_\gamma(\pm1,\alpha)$ and $P_\gamma(\alpha,\pm1)$. Thus they serve as constants in the equation and do not contribute to the error.

Let A be the matrix of coefficients for these equations. One can check that $|A^{-1}|_\infty=7225$. (Here, $|\cdot|_\infty$ denotes the ∞-norm on matrices, which is induced by the ℓ_∞ norm on vectors. It is the maximum over all rows of the sum of the absolute values of the elements in that row.) It follows that the intersection numbers in $\mathscr{C}_\Lambda$ differ by at most

$$7225 \cdot 6.7023 \cdot 10^{-6} < 0.05$$

from those in $\mathscr{C}_{24}$. Because they must be integers, this proves that they are the same as in $\mathscr{C}_{24}$ (in particular, they do not depend on the choice of x and y, although what we have proved is far stronger).

The computer file `verifyrest.txt` carries out all these calculations (as well as those from several other points in this paper). In it, we assume without loss of generality that $\gamma > 0$ because $\widetilde{P}_\gamma(\alpha, \beta) = \widetilde{P}_{-\gamma}(\alpha, -\beta)$.

6.3. *Uniqueness of association scheme.* The spherical code $\mathscr{C}_{24}$ determines a 6-class association scheme $\mathscr{A}_{24}$ if we partition elements (x, y) of $\mathscr{C}_{24} \times \mathscr{C}_{24}$ with $x \neq y$ according to their inner products $\langle x, y \rangle$. We can similarly form the association scheme $\mathscr{A}_\Lambda$ of the spherical code $\mathscr{C}_\Lambda$ coming from Λ, where this time we group elements according to their approximate inner products. We wish to show that these two association schemes are isomorphic. We will need to know that this 6-class association scheme $\mathscr{A}_{24}$ is uniquely determined by its size, valencies, and intersection numbers. That can be proved as follows.

Let $N = 196560$, let $C = 6/N = 1/32760$, and let $u_1, \dots, u_N$ be the minimal vectors of the Leech lattice. The following lemma restates the (known) fact that Λ_{24} is strongly eutactic. We provide a proof here to make this article more self-contained.

LEMMA 6.4. *For every $x \in \mathbb{R}^{24}$,*

$$\langle x, x \rangle = C \sum_{i=1}^{N} \langle x, u_i \rangle^2.$$

Proof. Because the minimal vectors of Λ_{24} form a spherical 2-design, the polynomial $y \mapsto \langle x, y \rangle^2$ has the same average over $\{u_1, \dots, u_N\}$ and the sphere of radius 2 in $\mathbb{R}^{24}$, which is 4 times the average over the unit sphere. To average over the unit sphere, it will be convenient to work with orthonormal bases of $\mathbb{R}^{24}$. For each orthonormal basis $e_1, \dots, e_{24}$, we have $|x|^2 = \sum_i \langle x, e_i \rangle^2$. If we average over all orthonormal bases, then each of $e_1, \dots, e_{24}$ is uniformly distributed over the unit sphere, and therefore the average of $y \mapsto \langle x, y \rangle^2$ over the unit sphere is $|x|^2/24$. It follows that the average over the sphere of radius 2 is $|x|^2/6$, so

$$\frac{1}{N} \sum_{i=1}^{N} \langle x, u_i \rangle^2 = |x|^2/6,$$

as desired. $\square$

THEOREM 6.5. *There is only one* 6*-class association scheme with the same size*, *valencies and intersection numbers as the association scheme of minimal vectors of the Leech lattice.*

Proof. Let $\mathscr{A} = \{a_i : 1 \le i \le 196560\}$ be such an association scheme, with $\mathscr{A}^2$ partitioned into classes as

$$\mathscr{A}^2 = \mathscr{A}_1 \cup \mathscr{A}_{1/2} \cup \mathscr{A}_{1/4} \cup \mathscr{A}_0 \cup \mathscr{A}_{-1/4} \cup \mathscr{A}_{-1/2} \cup \mathscr{A}_{-1}$$

(labeled according to the corresponding inner products in the Leech case, when the minimal vectors are rescaled to lie on the unit sphere).

Let $A_1, A_{1/2}, \dots, A_{-1}$ denote the adjacency matrices of the identity relation and the six classes; in other words,

$$(A_\alpha)_{i,j} = \begin{cases} 1 & \text{if } (a_i, a_j) \in \mathscr{A}_\alpha, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

These matrices are symmetric and commute with each other. Their span forms an algebra, called the Bose-Mesner algebra, whose product is determined by the valencies and intersection numbers. (See [BH95, p. 755].) Namely,

$$A_\alpha A_\beta = \sum_\gamma P_\gamma(\alpha, \beta) A_\gamma.$$

Furthermore, note that because the A_α's have only 0 or 1 as entries, are not identically zero, and sum to the all 1's matrix, they must be linearly independent. Thus, the Bose-Mesner algebra is completely determined by the valencies and intersection numbers, with no additional relations possible.

Let

$$P = 4C\left(A_1 + \frac{1}{2}A_{1/2} + \frac{1}{4}A_{1/4} - \frac{1}{4}A_{-1/4} - \frac{1}{2}A_{-1/2} - A_{-1}\right).$$

If the association scheme $\mathscr{A}$ comes from the Leech lattice, then P is C times the Gram matrix of the 196560 minimal vectors (not rescaled to the unit sphere). We claim that P is a projection matrix, i.e., $P^2 = P$. One way to check that is to use the valencies and intersection numbers to compute P^2 and verify that it equals P. That is somewhat cumbersome to check by hand, so we will instead give a longer but conceptually simpler proof.

First, we check it in the case of the actual Leech lattice association scheme, using Lemma 6.4. From

$$\langle x, x \rangle = C \sum_{i=1}^{N} \langle x, u_i \rangle^2$$

it follows that

$$\begin{aligned}\langle x, y\rangle &= \frac{1}{2}(\langle x+y, x+y\rangle - \langle x, x\rangle - \langle y, y\rangle)\\ &= \frac{C}{2}\sum_{i=1}^{N}\bigl(\langle x+y, u_i\rangle^2 - \langle x, u_i\rangle^2 - \langle y, u_i\rangle^2\bigr)\\ &= C\sum_{i=1}^{N}\langle x, u_i\rangle\langle y, u_i\rangle.\end{aligned}$$

Therefore the (i, j) entry of P^2 is

$$(P^2)_{i,j} = C^2\sum_{k=1}^{N}\langle u_i, u_k\rangle\langle u_j, u_k\rangle = C\langle u_i, u_j\rangle = P_{i,j},$$

so for the Leech lattice, P is a projection matrix. Because the structure of the Bose-Mesner algebra is completely determined by the valencies and intersection numbers, the same must always be true.

Thus, P is always a projection matrix (in fact, an orthogonal projection because P is symmetric). The trace of P is $4C$ times the trace of A_1, because no other A_α's have entries on the diagonal. The trace is therefore $4NC = 24$, so P projects onto a 24-dimensional subspace.

Consider the images of the $N = 196560$ unit vectors (namely $e_1, \dots, e_{196560}$) under P. Their inner products are simply the entries of P, since $\langle Pe_i, Pe_j\rangle = \langle e_i, P^2e_j\rangle = \langle e_i, Pe_j\rangle = P_{i,j}$, and if one rescales the vectors by $1/\sqrt{4C}$ so that they lie on the unit sphere, then the result is a 196560-point kissing configuration in $\mathbb{R}^{24}$. (Appendix B reviews the kissing problem.) The only such configuration is the kissing configuration of the Leech lattice (see [BS81], which was reprinted as Chapter 14 of [CS99]), up to orthogonal transformations of $\mathbb{R}^{24}$. Thus, P/C must be the Gram matrix of the minimal vectors in the Leech lattice.

It follows that $\mathcal{A}$ is isomorphic to $\mathcal{A}_{24}$ (in particular, $a_i \mapsto P(e_i)/\sqrt{4C}$ yields an isomorphism). Thus, $\mathcal{A}_{24}$ is determined by its size and intersection numbers, as desired. □

7. Inner product bounds

We will first use the intersection numbers and isomorphism of association schemes to prove better bounds on σ. We already know that for all nearly minimal vectors u,

$$4 \le \langle u, u\rangle \le 4(1+\varepsilon)^2 < 4 + 9\varepsilon.$$

LEMMA 7.1. *For nearly minimal vectors* u, v *with* $\langle u, v\rangle \approx 2$,

$$2-5\varepsilon \le \langle u, v\rangle \le 2+9\varepsilon.$$

Proof. We know that $u-v$ is nearly minimal, so

$$\langle u-v, u-v\rangle \le 4(1+\varepsilon)^2.$$

It follows that

$$\begin{aligned} 2\langle u, v\rangle &\ge -4(1+2\varepsilon+\varepsilon^2) + \langle u, u\rangle + \langle v, v\rangle \\ &\ge 8-4(1+2\varepsilon+\varepsilon^2) \\ &\ge 4-10\varepsilon, \end{aligned}$$

which gives us one of the inequalities. Similarly,

$$\langle u-v, u-v\rangle \ge 4$$

gives us

$$\begin{aligned} 2\langle u, v\rangle &\le -4 + \langle u, u\rangle + \langle v, v\rangle \\ &\le -4+8(1+2\varepsilon+\varepsilon^2) \\ &\le 4+18\varepsilon, \end{aligned}$$

which is the other inequality. □

Note that these inequalities could be made slightly sharper, but we prefer simpler numbers.

LEMMA 7.2. *For nearly minimal vectors* u, v *with* $\langle u, v\rangle \approx 0$,

$$-14\varepsilon \le \langle u, v\rangle \le 14\varepsilon.$$

Proof. Since $P_0(1/2, 1/2) = 44 \neq 0$, we can find w with $\langle u, w\rangle \approx 2$ and $\langle v, w\rangle \approx 2$. Then $v-w$ is nearly minimal and we know from the previous lemma that

$$2-5\varepsilon \le \langle u, w\rangle \le 2+9\varepsilon$$

and

$$-2-9\varepsilon \le \langle u, v-w\rangle \le -2+5\varepsilon.$$

Adding these inequalities gives us the result. □

LEMMA 7.3. *If* $u, v \in \Lambda_{24}$ *are minimal vectors with* $\langle u, v\rangle = 1$, *then there are minimal vectors* w_1, w_2, *and* w_3 *satisfying* $\langle u, w_i\rangle = 2$, $\langle v, w_i\rangle = 0$, *and* $\langle w_i, w_j\rangle = 0$ *for* $i \neq j$.

Proof. We will use the fact that the automorphism group Co_0 of the Leech lattice acts transitively on pairs of minimal vectors with a fixed inner product between them (see Theorem 3.13 in [Tho83] for a proof). Thus it suffices to consider the case of a particular pair (u, v) of minimal vectors with inner product 1. Let

$$\begin{aligned}
u &= \frac{1}{\sqrt{8}}(1, 1, \dots, 1, 1, -3),\\
v &= \frac{1}{\sqrt{8}}(0, 0, \dots, 0, -4, -4),\\
w_1 &= \frac{1}{\sqrt{8}}(2, 2, 2, 2, 2, 2, 2, 2, 0, 0, \dots, 0),\\
w_2 &= \frac{1}{\sqrt{8}}(0, 0, \dots, 0, 4, -4), \text{ and}\\
w_3 &= \frac{1}{\sqrt{8}}(0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 0, 0, 2, 2, 0, 0, 2, 2, 0, 0, 2, 2, 0, 0).
\end{aligned}$$

(see [CS99, p. 131] for a description of the minimal vectors). It is easily checked that the inner products are as desired. □

LEMMA 7.4. *For nearly minimal vectors u, v with $\langle u, v\rangle \approx 1$,*

$$1 - 72\varepsilon \le \langle u, v\rangle \le 1 + 75\varepsilon.$$

Proof. We know that the association schemes of the Leech lattice Λ_{24} and our given lattice Λ are the same. Let u', v' be the corresponding vectors in the Leech lattice (corresponding via some fixed isomorphism of association schemes). Since $\langle u', v'\rangle = 1$, we know that we can find w_1', w_2', and w_3' in the Leech lattice satisfying $\langle u', w_i'\rangle = 2$, $\langle v', w_i'\rangle = 0$, and $\langle w_i', w_j'\rangle = 0$ by Lemma 7.3. Let w_1, w_2, w_3 be the corresponding vectors in Λ. Then the relations $\langle u, w_i\rangle \approx 2$, $\langle v, w_i\rangle \approx 0$, and $\langle w_i, w_j\rangle \approx 0$ must hold in Λ. It follows by a short computation that $2u - v - w_1 - w_2 - w_3$ is a nearly minimal vector. Therefore

$$\begin{aligned}
4 &\le \langle 2u - v - w_1 - w_2 - w_3, 2u - v - w_1 - w_2 - w_3\rangle\\
&= 4\langle u, u\rangle + \langle v, v\rangle + \sum_i \langle w_i, w_i\rangle - 4\langle u, v\rangle\\
&\qquad - 4\sum_i \langle u, w_i\rangle + 2\sum_i \langle v, w_i\rangle + 2\sum_{i<j}\langle w_i, w_j\rangle.
\end{aligned}$$

It follows that

$$\begin{aligned}
4\langle u, v\rangle &\le -4 + 4\langle u, u\rangle + \langle v, v\rangle + \sum_i \langle w_i, w_i\rangle\\
&\qquad - 4\sum_i \langle u, w_i\rangle + 2\sum_i \langle v, w_i\rangle + 2\sum_{i<j}\langle w_i, w_j\rangle\\
&\le -4 + 8(4 + 9\varepsilon) - 12(2 - 5\varepsilon) + 12(14\varepsilon).
\end{aligned}$$

Thus, $\langle u, v\rangle \le 1 + 75\varepsilon$. Similarly,

$$\begin{aligned}4 + 9\varepsilon &\ge \langle 2u - v - w_1 - w_2 - w_3, 2u - v - w_1 - w_2 - w_3\rangle \\ &= 4\langle u, u\rangle + \langle v, v\rangle + \sum_i \langle w_i, w_i\rangle - 4\langle u, v\rangle \\ &\quad - 4\sum_i \langle u, w_i\rangle + 2\sum_i \langle v, w_i\rangle + 2\sum_{i<j} \langle w_i, w_j\rangle.\end{aligned}$$

It follows that

$$\begin{aligned}4\langle u, v\rangle &\ge -4 - 9\varepsilon + 4\langle u, u\rangle + \langle v, v\rangle + \sum_i \langle w_i, w_i\rangle \\ &\quad - 4\sum_i \langle u, w_i\rangle + 2\sum_i \langle v, w_i\rangle + 2\sum_{i<j} \langle w_i, w_j\rangle \\ &\ge -4 - 9\varepsilon + 8(4) - 12(2 + 9\varepsilon) + 12(-14\varepsilon).\end{aligned}$$

Thus, $\langle u, v\rangle \ge 1 - (285/4)\varepsilon \ge 1 - 72\varepsilon$. □

We have proved the following proposition.

PROPOSITION 7.5. *If $u, v \in \Lambda$ are nearly minimal vectors, then $\langle u, v\rangle$ differs from an element of $\{0, \pm 1, \pm 2, \pm 4\}$ by at most 75ε.*

8. A basis of nearly minimal vectors

We wish to prove that Λ must have a basis of nearly minimal vectors. We first prove that the nearly minimal vectors span Λ. Let $x \in \Lambda$ be as small a vector as possible without being in the span of the nearly minimal vectors. Then there does not exist a nearly minimal vector u such that $|u - x| < |x|$. We know that $|x| > \sqrt{6}(1 - \mu)$ and $2 \le |u| \le 2(1 + \varepsilon)$ for each nearly minimal u. Because $|u - x| \ge |x|$, we have

$$\langle u, x\rangle \le |u|^2/2 \le 2(1 + \varepsilon)^2.$$

Consider the unit vectors $x/|x|$ and $u/|u|$. We have

$$\left\langle \frac{u}{|u|}, \frac{x}{|x|}\right\rangle \le \frac{2(1 + \varepsilon)^2}{\sqrt{6}(1 - \mu) \cdot 2} < \frac{1}{2}.$$

If we extend the spherical code $\mathscr{C}_\Lambda$ of vectors of the form $u/|u|$ to $\mathscr{C}_\Lambda \cup \{x/|x|\}$, then it will contain 196561 vectors without changing the minimal angle, and we have seen that that is impossible. Thus, the nearly minimal vectors do span the lattice.

The same argument (with $\varepsilon = \mu = 0$) also proves the following fact: if the kissing configuration of a lattice is an optimal kissing configuration for its dimension, then the lattice is spanned by its minimal vectors.

Now let B be $1/\sqrt{8}$ times the matrix

$$\begin{pmatrix}
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 & 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 \\
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 \\
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 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 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{pmatrix}.$$

The rows of B form a basis of Λ_{24} consisting of minimal vectors (see Figure 4.12 in [CS99]). One can compute the inverse matrix and check that its entries are integers divided by $\sqrt{8}$. The largest entry of B^{-1}, in absolute value, is $-13/\sqrt{8}$, so $\left|B^{-1}\right|_\infty \leq 24 \cdot 13/\sqrt{8}$.

Let $u'_1, \dots, u'_{24}$ be the rows of B. Every minimal vector u' is a linear combination $\sum_i c_i u'_i$ of this basis, and the coefficients are bounded by

$$|c_i| \leq \left|B^{-1}\right|_\infty |u'|_\infty \leq \left(24 \cdot 13/\sqrt{8}\right) \cdot \left(4/\sqrt{8}\right) = 156.$$

Consider the corresponding nearly minimal vectors $u_1, \dots, u_{24}$ of Λ (under an isomorphism of association schemes). We next prove that they form a basis.

We need only check that $u_1, \dots, u_{24}$ span the nearly minimal vectors of Λ. If u is any nearly minimal vector, the isomorphism of association schemes gives us numbers $c_1, \dots, c_{24}$ such that u should be $\sum_i c_i u_i$ (i.e., the corresponding equality is true for the Leech lattice). We first check that $\sum_i c_i u_i$ is a nearly minimal vector, and then that it equals u. To check that it is nearly minimal, we just need to know that all inner products of nearly minimal vectors are within 75ε of what they are in the Leech lattice (Proposition 7.5). When we compute the norm of $\sum_i c_i u_i$, each inner product $\langle u_i, u_j \rangle$ could be off by as much as 75ε, and multiplied by up to 156^2. There are 24^2 such pairs, for a total error of at most $156^2 \cdot 24^2 \cdot 75\varepsilon = 1051315200\varepsilon$, which is minuscule (less than 10^{-17}). Because the next smallest vectors beyond the nearly minimal vectors have norms at least $\sqrt{6}(1-\mu)$, we conclude that $\sum_i c_i u_i$ must be nearly minimal.

To check that $u = \sum_i c_i u_i$, we need only compute their inner product and verify that it is approximately 4. This time, the maximum error is $24 \cdot 156 \cdot 75\varepsilon$, which is again small enough by a huge margin.

Thus, $u_1, \dots, u_{24}$ form a basis of Λ, and their inner products are all within 75ε of what they would be in the Leech lattice.

9. **Local optimality of** Λ_{24}

In this section, we will prove in detail that the Leech lattice is locally optimal, and provide quantitative bounds. We will follow the notation and techniques from [GL87] closely. The basic result is Voronoi's theorem, which says that a lattice is a local maximum for sphere packing density if and only if it is perfect and eutactic. In this section of the paper only, Λ will denote an arbitrary lattice in $\mathbb{R}^n$.

It is convenient to work in terms of the quadratic form Q associated to Λ. Choose a lattice basis $\{b_i\}$, and for a vector $x \in \mathbb{R}^n$ (with coordinates $x_1, \dots, x_n$) define

$$Q(x) = \left\langle \sum_{i=1}^{n} x_i b_i, \sum_{i=1}^{n} x_i b_i \right\rangle.$$

The matrix of Q is $S = (s_{i,j})_{i,j=1}^{n}$, where $s_{i,j} = \langle b_i, b_j \rangle$.

Let M denote the minimal nonzero norm of Λ, and let $u_1, \dots, u_N \in \mathbb{Z}^n$ be the coefficient vectors of the minimal vectors in terms of the basis $\{b_i\}$. Thus, for $1 \le i \le N$,

$$Q(u_i) = M.$$

Recall that Q is *perfect* if these equations completely determine the quadratic form Q. Equivalently, every quadratic form that vanishes at $u_1, \dots, u_N$ must vanish everywhere.

Let D denote the determinant of S, and let $\tilde{S} = (\tilde{s}_{i,j})_{i,j=1}^{n}$ denote the adjoint matrix, where

$$\tilde{s}_{i,j} = \frac{\partial D}{\partial s_{i,j}}.$$

Strictly speaking this is an abuse of notation, but of course it means we take the partial derivatives of D as if the entries of S were variables, and then substitute their actual values.

In other words, $S\tilde{S}$ is D times the identity matrix. (It might seem that a transpose is missing, but note that all our matrices are symmetric.) Let $\tilde{Q}$ be the quadratic form with matrix $\tilde{S}$. Then Λ is *eutactic* if there are positive numbers $d_1, \dots, d_N$ such that for all $x \in \mathbb{R}^n$,

$$\tilde{Q}(x) = \sum_{k=1}^{N} d_k \langle u_k, x \rangle^2.$$

It is known that Λ_{24} is perfect and eutactic, with $d_1 = \cdots = d_{196560} = 1/32760$. For completeness we sketch a proof. Lemma 6.4 proves that the Leech lattice is eutactic.

LEMMA 9.1. *The Leech lattice Λ_{24} is perfect.*

Proof. Suppose Q is a quadratic form that vanishes on the minimal vectors. Then the symmetric bilinear form B corresponding to Q satisfies $B(u_i, u_i) = 0$. We first show that $B(u, v) = 0$ for all minimal vectors u, v. If $\langle u, v\rangle = 2$ we use the fact that $u - v$ is minimal to see that

$$B(u, v) = \frac{1}{2}\left(B(u, u) + B(v, v) - B(u - v, u - v)\right) = 0.$$

If $\langle u, v\rangle = 0$, then since $P_0(1/2, -1/2) = 44 \neq 0$, we can find w with $\langle u, w\rangle = 2$ and $\langle v, w\rangle = -2$. Then $v + w$ is nearly minimal and we know

$$0 = B(u, w) = B(u, v + w);$$

subtracting these two gives us the result. If $\langle u, v\rangle = 1$, then by Lemma 7.3 there are minimal vectors w_1, w_2, and w_3 with $\langle u, w_i\rangle = 2$, $\langle v, w_i\rangle = 0$, and $\langle w_i, w_j\rangle = 0$ for $i \neq j$. It follows that $2u - v - w_1 - w_2 - w_3$ is a minimal vector. Therefore

$$\begin{aligned}
0 &= B(2u - v - w_1 - w_2 - w_3, 2u - v - w_1 - w_2 - w_3)\\
&= 4B(u, u) + B(v, v) + \sum_i B(w_i, w_i) - 4B(u, v)\\
&\quad - 4\sum_i B(u, w_i) + 2\sum_i B(v, w_i) + 2\sum_{i<j} B(w_i, w_j)\\
&= -4B(u, v) + 0.
\end{aligned}$$

This forces $B(u, v) = 0$. Finally, the result for $\langle u, v\rangle < 0$ follows from the above because $B(u, v) = -B(u, -v)$ and $\langle u, -v\rangle > 0$.

To conclude the proof, we use the above information on a basis of minimal vectors to see that B is identically zero, and hence Q is as well. □

We begin by proving one direction of Voronoi's theorem. This proof is the one given in [GL87, §39], where one can also find a proof of the converse. We give the details of this direction because we will need to examine it in detail to derive quantitative estimates, and because it is the only direction needed here.

THEOREM 9.2 (Voronoi [Vor08]). *If Λ is perfect and eutactic, then it is a strict local maximum for density.*

Proof. We wish to show that if Λ is perturbed slightly (other than simply by scaling and isometries), then $D^{-1/n}M$ must strictly decrease. We perturb $S = (s_{i,j})$ by changing it to $(s_{i,j} + \rho t_{i,j})$, where $t_{j,i} = t_{i,j}$ and $\rho > 0$ is small. We assume $(t_{i,j})$ is not identically zero. Let Q_ρ denote the corresponding quadratic form, and let D_ρ be the determinant of the matrix $(s_{i,j} + \rho t_{i,j})$. We will show that for any fixed matrix $(t_{i,j})$ not proportional to S, if ρ is sufficiently small, then there exists a k such that

$$D_\rho^{-1/n} Q_\rho(u_k) < D^{-1/n} M.$$

Because $Q_\rho(u_k)$ is no smaller than the minimal norm of Q_ρ (i.e., the minimum value of Q_ρ on $\mathbb{Z}^n \setminus \{0\}$), this inequality is what we want.

First, note that without loss of generality we can assume that

$$\sum_{i,j} \tilde{s}_{i,j} t_{i,j} = 0. \tag{9.1}$$

The reason is that

$$\sum_{i,j} \tilde{s}_{i,j} s_{i,j} = nD \neq 0.$$

Every perturbation can be broken up into the sum of a perturbation proportional to S and a perturbation satisfying (9.1). If we deal with the latter, then we can ignore the former (which rescales the lattice but does not change its packing density).

Thus, we assume (9.1) from now on. Then the determinant D_ρ is given by

$$\begin{aligned} D_\rho = \det(s_{i,j} + \rho t_{i,j}) &= \det(s_{i,j}) + \rho \sum_{i,j} t_{i,j} \tilde{s}_{i,j} + O(\rho^2) \\ &= D + O(\rho^2) \quad \text{as } \rho \to 0. \end{aligned}$$

Because Λ is eutactic,

$$\tilde{Q}(x) = \sum_{k=1}^{N} d_k \langle u_k, x \rangle^2$$

for all $x \in \mathbb{R}^n$. The associated symmetric bilinear form is

$$\sum_{k=1}^{N} d_k \langle u_k, x \rangle \langle u_k, y \rangle,$$

from which it follows that

$$\tilde{s}_{i,j} = \sum_{k=1}^{N} d_k (u_k)_i (u_k)_j,$$

where $(u_k)_i$ denotes the i-th coefficient of u_k. Therefore

$$\sum_{k=1}^{N} d_k \sum_{i,j} t_{i,j} (u_k)_i (u_k)_j = \sum_{i,j} \tilde{s}_{i,j} t_{i,j} = 0.$$

Because Λ is perfect, the inner sum on the left-hand side in the above equation cannot vanish for all k. Therefore, there exists a k for which it is negative, say

$$\sum_{i,j} t_{i,j}(u_k)_i(u_k)_j \le -\alpha$$

with $\alpha > 0$. Then

$$Q_\rho(u_k) = \sum (s_{i,j} + \rho t_{i,j})(u_k)_i(u_k)_j \le M - \rho\alpha,$$

and hence

$$D_\rho^{-1/n} Q_\rho(u_k) \le D^{-1/n} M(1-\rho\alpha/M)(1+O(\rho^2))^{-1/n} < D^{-1/n} M$$

if ρ is positive and small enough. This proves that Λ is a strict local optimum for density when $(s_{i,j})$ is perturbed in the direction of $(t_{i,j})$. In fact, the choices of α and the implicit constant in the big-O can be made uniformly in $(t_{i,j})$, given $\sum_{i,j} |t_{i,j}|^2 = 1$. Thus Λ is a strict local optimum for density. $\square$

We now compute numerical bounds on the perturbations. We use the same basis of Λ_{24} as before. The corresponding Gram matrix is

$$\begin{pmatrix}
4 & 0 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 0 & 2 & 0 & 1 & 1 & 2 & 1 & 1 & 0 & -1 & 0 & 0 & -2\\
0 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 0 & 0 & -1\\
2 & 2 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 2 & 1 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & -1\\
2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 2 & 2 & 1 & 2 & 1 & 1 & 0 & 0 & -1\\
2 & 2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 0 & 0 & -1\\
2 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 & 2 & 1 & 2 & 2 & 1 & 1 & 2 & 1 & 2 & 1 & 0 & 0 & 0 & -1\\
2 & 2 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 1 & 2 & 0 & 0 & 0 & -1\\
0 & 2 & 2 & 2 & 2 & 2 & 2 & 4 & 1 & 1 & 1 & 2 & 1 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 0 & 0 & 1\\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & -1\\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 2 & 4 & 2 & 2 & 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 & 0 & 1 & 0 & -1\\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 2 & 2 & 4 & 2 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 0 & 0 & 1 & -1\\
0 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 4 & 1 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 1 & 1 & 1\\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 1 & 4 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & -1\\
0 & 2 & 1 & 1 & 2 & 2 & 1 & 2 & 2 & 2 & 1 & 2 & 2 & 4 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 1 & 1\\
1 & 1 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 4 & 2 & 1 & 2 & 2 & 2 & 2 & 1 & 2 & 1\\
1 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 2 & 2 & 4 & 1 & 2 & 2 & 2 & 2 & 1 & 1 & 1\\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 1 & 2 & 1 & 1 & 1 & 4 & 2 & 2 & 2 & 1 & 1 & 1 & -1\\
1 & 1 & 2 & 1 & 2 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 & 1 & 1\\
1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 2 & 1 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 1 & 2 & 1\\
0 & 2 & 1 & 1 & 2 & 1 & 2 & 2 & 2 & 1 & 1 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 4 & 2 & 1 & 1 & 1\\
-1 & 1 & 1 & 1 & 1 & 0 & 0 & 2 & 1 & 0 & 0 & 2 & 1 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 4 & 2 & 2 & 2\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 4 & 2 & 2\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 2 & 2 & 4 & 2\\
-2 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 2 & 2 & 2 & 4
\end{pmatrix}.$$

Suppose we assume that the Gram matrix entries are perturbed by $\rho t_{i,j}$ where $\max\{|t_{i,j}|\} \le 1$ (and (9.1) holds—we will eventually deal with the case where it does not). Then, with the same notation as in the proof of Theorem 9.2,

$$D_\rho - D = \sum_T \rho^{\dim T} \det(T) \det(\tilde{T}),$$

where T ranges over all nonvacuous minors of $(t_{i,j})$ and $\det(\tilde{T})$ is the corresponding cofactor of the matrix S. (The D term corresponds to the case where T is vacuous, i.e., contains no rows or columns.) This expansion follows from combining the Laplace expansion (see [Mui60, §95]) with multilinearity, and is known as Albeggiani's theorem [Mui60, §96].

Now let $\dim T = k$. Then $|\det(T)| \le k^{k/2}$ by Hadamard's inequality, since the length of each row of T is at most $\sqrt{k}$ (see (7.8.2) in [HJ85]). It follows that the absolute value of the sum of $\rho^k \det(T)\det(\tilde{T})$ over k-dimensional T is bounded by $k^{k/2}\rho^k A_k$, where A_k is the sum of the absolute values of the $(24-k)$-dimensional minors of the Gram matrix. For $k \ge 3$ we use the simple bound

$$A_k \le \binom{24}{k}^2 \cdot \left(4^2 + (24-k-1)(2^2)\right)^{(24-k)/2}$$

(the first factor is the number of $(24-k)\times(24-k)$ minors, and the second is the above bound on the determinant of the cofactor, because the largest entry in each row of S is 4 and the other entries are at most 2 in absolute value). For $k = 2$ we explicitly compute the sum of absolute values of the 22×22 minors, and find that it is 818153. Putting all this together, we see that for $0 < \rho < 10^{-20}$,

$$D_\rho \ge 1 - \rho^2\left(2^{2/2} \cdot 818153 + 2 \cdot 10^8\right), \tag{9.2}$$

where the $2 \cdot 10^8$ term bounds the contribution from all higher powers of ρ. (Recall that $D = 1$ for the Leech lattice.) See the computer file `verifygram.txt` for the details of this calculation.

Next, we find an α that works for any choice of $t_{i,j}$ such that $\max\{|t_{i,j}|\} = 1$. This is done by linear programming as follows.

We find an $\alpha > 0$ such that for all (i_0, j_0), and for all $t_{i,j}$ subject to the constraints $-1 \le t_{i,j} \le 1$ for $(i,j) \ne (i_0, j_0)$, $t_{i,j} = t_{j,i}$, $t_{i_0,j_0} = 1$, and $\sum_{i,j} \tilde{s}_{i,j} t_{i,j} = 0$, the following inequality holds for some minimal vector u_k:

$$\sum_{i,j} t_{i,j}(u_k)_i(u_k)_j \le -\alpha.$$

We do the same for $t_{i_0,j_0} = -1$. All these linear programs can be solved by computer, and it appears that $\alpha = 1/23$ works and is the largest possible value of α. However, that is the result of floating point calculations that are not rigorous. We will be content with proving (without computer assistance) that $\alpha = 4/1055$ satisfies these properties. This weaker bound will suffice for our purposes and is proved in Section 10.

We conclude that for every perturbation by $t_{i,j}$ where $\max\{|t_{i,j}|\} = \rho$ and $\sum_{i,j} \tilde{s}_{i,j} t_{i,j} = 0$, there exists a k such that for $0 < \rho < 10^{-20}$,

$$\frac{D_\rho^{-1/24} Q_\rho(u_k)}{D^{-1/24} \cdot M} \leq (1 - \rho/1055)\big(1 - (2 \cdot 10^8 + 2 \cdot 818153)\rho^2\big)^{-1/24}. \tag{9.3}$$

We used here that $M = 4$ for Λ_{24}. The upper bound in (9.3) is strictly less than 1 when $0 < \rho < 10^{-20}$. (Note that for notational convenience we have absorbed the factor ρ into the perturbations $t_{i,j}$.)

The last remaining issue is that our perturbation may not satisfy $\sum_{i,j} \tilde{s}_{i,j} t_{i,j} = 0$. Suppose our perturbed matrix entries are $s_{i,j} + \eta_{i,j}$. Let

$$\Delta = \sum_{i,j} \tilde{s}_{i,j} \eta_{i,j}.$$

By Proposition 7.5, $|\eta_{i,j}| \leq 75\varepsilon$. It follows that $|\Delta| \leq 152100\varepsilon$, since the sum of the absolute values of the entries of $\tilde{S}$ is 2028.

If we divide the quadratic form by $1 + \Delta/24$, which is nonzero, then it is equivalent to Λ_{24} perturbed by

$$t_{i,j} = \frac{s_{i,j} + \eta_{i,j}}{1 + \Delta/24} - s_{i,j},$$

where now

$$\sum_{i,j} \tilde{s}_{i,j} t_{i,j} = 0,$$

because

$$\sum_{i,j} \tilde{s}_{i,j} s_{i,j} = 24D = 24.$$

To conclude our proof, we need only check that $|t_{i,j}| < 10^{-20}$. (Note that if $t_{i,j} = 0$ for all i, j, then the perturbed quadratic form is proportional to the original one and therefore equal to it because they have the same determinant.)

Using $|\Delta| \leq 152100\varepsilon$, $|\eta_{i,j}| \leq 75\varepsilon$, and $|s_{i,j}| \leq 4$, we have

$$|t_{i,j}| = \left| \frac{\eta_{i,j} - s_{i,j}\Delta/24}{1 + \Delta/24} \right| \leq \frac{75\varepsilon + 4 \cdot 152100\varepsilon/24}{1 - 152100\varepsilon/24} < 1.8 \cdot 10^{-22}. \tag{9.4}$$

Because $1.8 \cdot 10^{-22} < 10^{-20}$, we find that the dense lattice Λ is close enough to Λ_{24} to conclude that Λ is either the same as Λ_{24} (up to isometries of $\mathbb{R}^{24}$) or strictly less dense than Λ_{24}.

This completes the proof of our main theorem, except for the postponed computation of α in Section 10:

THEOREM 9.3. *The Leech lattice is the unique densest lattice in* $\mathbb{R}^{24}$, *up to scaling and isometries of* $\mathbb{R}^{24}$.

Note that the reason why scaling ambiguity appears in the theorem statement but not in the above proof is that we fixed $|\Lambda| = 1$.

10. **Computation of** α

Suppose $i_0, j_0 \in \{1, 2, \dots, 24\}$ and $t = \pm 1$. We wish to find a number $\alpha > 0$ such that whenever $-1 \le t_{i,j} \le 1$ for $(i, j) \neq (i_0, j_0)$, $t_{i,j} = t_{j,i}$, $t_{i_0,j_0} = t$, and $\sum_{i,j} \tilde{s}_{i,j} t_{i,j} = 0$, there is a k such that

$$\sum_{i,j} t_{i,j} (u_k)_i (u_k)_j \le -\alpha.$$

We will see that we can take $\alpha = 4/1055$, whatever i_0, j_0, and t are.

LEMMA 10.1. *Each minimal vector of the Leech lattice is contained in a set of twenty-four orthogonal minimal vectors.*

In fact, more is true: the minimal vectors can be partitioned into 4095 sets $\{\pm v_1, \dots, \pm v_{24}\}$ with v_i and v_j orthogonal for $i \neq j$. See footnote 3 of [Elk97, p. 6] for an elegant proof.

Proof. Because the automorphism group of the Leech lattice acts transitively on the minimal vectors, we need only verify that there exists a set of twenty-four orthogonal minimal vectors. Let w_i be the vector

$$\frac{1}{\sqrt{8}}(0, \dots, 0, 4, 4, 0, \dots, 0),$$

where only coordinates i and $i + 1$ are nonzero, and let v_i be the vector

$$\frac{1}{\sqrt{8}}(0, \dots, 0, 4, -4, 0, \dots, 0).$$

These are all minimal vectors in the Leech lattice, and $w_1, v_1, w_3, v_3, \dots, w_{23}, v_{23}$ is an orthogonal basis of $\mathbb{R}^{24}$. $\square$

Let T denote the matrix $(t_{i,j})$. We will also write $T(v) = \langle v, Tv \rangle$ and $T(u, v) = \langle u, Tv \rangle$. In these terms, our goal is to show that given the assumptions on T, there is some k such that $T(u_k) \le -\alpha$.

We will make use of the following lemma, which depends only on the hypotheses listed in its statement:

LEMMA 10.2. *Let $v_1, \dots, v_{24}$ be orthogonal minimal vectors in the Leech lattice. If $\sum_{i,j} \tilde{s}_{i,j} t_{i,j} = 0$, then*

$$\sum_{i=1}^{24} T(v_i) = 0.$$

Proof. Let B be the matrix whose rows are the coordinates of $v_1, \dots, v_{24}$ relative to the basis we have chosen for the Leech lattice. Then we see by orthogonality that $BSB^t = 4I$. Thus, $S = 4B^{-1}(B^t)^{-1}$. It follows that

$$\mathrm{Tr}(BTB^t) = \mathrm{Tr}(B^tBT) = 4\,\mathrm{Tr}(S^{-1}T) = 4\sum_{i,j} \tilde{s}_{i,j}t_{i,j} = 0,$$

which implies

$$\sum_{i=1}^{24} T(v_i) = 0. \qquad \square$$

Let us rephrase our basic problem, and slightly weaken the hypotheses, as follows. Suppose $\sum_{i,j} \tilde{s}_{i,j}t_{i,j} = 0$, and we are given minimal vectors x, y such that

$$\langle x, y\rangle = \beta \in \{\pm 4, \pm 2, \pm 1, \pm 0\}$$

and $T(x, y) = t \neq 0$. We wish to find $\alpha > 0$ such that there must always exist a minimal vector w with $T(w, w) \le -\alpha|t|$ under these hypotheses. We will apply it with $t = \pm 1$. (Note that we are no longer assuming $|t_{i,j}| \le 1$.)

If we prove a bound for a certain (β, t) we automatically get the same bound of α for the case of $(-\beta, -t)$ (just consider the pair $(x, -y)$ instead of (x, y)). Thus it suffices to prove bounds of α for the cases when β is nonnegative.

LEMMA 10.3. *If $\beta = 4$ and $t < 0$ then we can take $\alpha = 1$.*

Proof. The hypothesis says that $x = y$ and $T(x, x) = t < 0$ so we just take $w = x$. $\square$

LEMMA 10.4. *If $\beta = 4$ and $t > 0$, then we can take $\alpha = 1/23$.*

Proof. The hypothesis says that $x = y$ and $T(x, x) = t > 0$. By Lemma 10.1, the Leech lattice contains orthogonal minimal vectors $v_1, \dots, v_{24}$ with $v_1 = x$. Then Lemma 10.2, together with $T(v_1) = t$, implies that $T(v_i) \le -t/23$ for some $i \in \{2, \dots, 24\}$. $\square$

LEMMA 10.5. *If $\beta = 2$ and $t < 0$, then we can take $\alpha = 2/25$.*

Proof. Let x, y be minimal vectors such that $\langle x, y\rangle = 2$ and $T(x, y) = t < 0$. We know that $x - y$ is a minimal vector. Also

$$T(x - y) = T(x, x) + T(y, y) - 2T(x, y) = T(x, x) + T(y, y) - 2t.$$

Thus either $T(x, x) \le 2t/25 = -2|t|/25$ or $T(y, y) \le 2t/25$ or $T(x - y, x - y) \ge 4t/25 - 2t = -46t/25 = 46|t|/25$. However, in the last case we see by Lemma 10.4 that $T(v, v) \le -(1/23)(46|t|/25) = -2|t|/25$ for some minimal vector v. $\square$

LEMMA 10.6. *If $\beta = 2$ and $t > 0$, then we can take $\alpha = 2/47$.*

Proof. Let x, y be minimal vectors such that $\langle x, y\rangle = 2$ and $T(x, y) = t > 0$. Again we have

$$T(x-y, x-y) = T(x, x) + T(y, y) - 2t.$$

Thus either $T(x-y, x-y) \leq -2t/47$ or one of $T(x, x)$ and $T(y, y)$ is at least $(2t - 2t/47)/2 = 46t/47$. Then by Lemma 10.4, we see that there exists a minimal vector v with $T(v, v) \leq (-1/23)(46t/47) = -2|t|/47$. □

LEMMA 10.7. *If $\beta = 0$, then we can take $\alpha = 1/60$.*

Proof. By possibly exchanging $(\beta, t) = (0, t)$ with $(0, -t)$ we can assume $t > 0$. Let x, y be minimal vectors such that $\langle x, y\rangle = 0$ and $T(x, y) = t > 0$. We have computed the intersection numbers for the Leech lattice. The intersection number $P_0(1/2, 1/2)$ is 44, so there exists a minimal vector w with $\langle x, w\rangle = 2$ and $\langle y, w\rangle = 2$. We compute that

$$\begin{aligned}\langle x+y-w, x+y-w\rangle &= \langle x, x\rangle + \langle y, y\rangle + \langle w, w\rangle + 2\langle x, y\rangle - 2\langle x, w\rangle - 2\langle y, w\rangle\\ &= 4+4+4+0-4-4\\ &= 4,\end{aligned}$$

so $x + y - w$ is a minimal vector. Then we compute

$$\begin{aligned}T(x+y-w) &= T(x, x) + T(y, y) + T(w, w) + 2T(x, y) - 2T(x, w) - 2T(y, w)\\ &= T(x, x) + T(y, y) + T(w, w) + 2t - 2T(x, w) - 2T(y, w).\end{aligned}$$

If $T(x, x)$ or $T(y, y)$ or $T(w, w)$ is at most $-t/60$ we are done. Similarly if $T(x+y-w, x+y-w) \geq 23t/60$ we are done, by Lemma 10.4, so we may assume none of these is true. Then we see that $T(x, w) + T(y, w) \geq 1/2(2t - 3t/60 - 23t/60) = 47t/60$. It follows that one of the summands is at least $47t/120$, say $T(x, w)$ without loss of generality. But since $\langle x, w\rangle = 2$, an application of Lemma 10.6 finishes the proof. □

LEMMA 10.8. *If $\beta = 1$ and $t > 0$, then we can take $\alpha = 4/1055$.*

Proof. Let x and y be minimal vectors with $\langle x, y\rangle = 1$. By Lemma 7.3, there are minimal vectors w_1, w_2, and w_3 satisfying $\langle x, w_i\rangle = 0$, $\langle y, w_i\rangle = 2$, and $\langle w_i, w_j\rangle = 0$ for $i \neq j$. It follows that $z = 2y - x - w_1 - w_2 - w_3$ has norm 4, so it is a minimal vector. Now,

$$\begin{aligned}T(z, z) = 4T(y, y) + T(x, x) + \sum_i T(w_i, w_i) - 4T(x, y)\\ - 4\sum_i T(y, w_i) + 2\sum_i T(x, w_i) + 2\sum_{i<j} T(w_i, w_j).\end{aligned}$$

Since we know $T(x, y) = t$, we get

$$4t = 4T(y, y) + T(x, x) + \sum_i T(w_i, w_i) - T(z, z) \\ - 4\sum_i T(y, w_i) + 2\sum_i T(x, w_i) + 2\sum_{i<j} T(w_i, w_j).$$

Next, we assume that $T(v, v) \geq -\alpha t$ for all minimal vectors v, and prove that α cannot be less than $4/1055$. It follows from this assumption and Lemma 10.4 that $T(y, y) \leq 23\alpha t$. Similarly $T(x, x)$ and $T(w_i, w_i)$ are at most $23\alpha t$, and $-T(z, z) \leq \alpha t$ by hypothesis. The inner products $\langle y, w_i\rangle$ are 2 so by Lemma 10.5, $-T(y, w_i) \leq 25\alpha t/2$. Finally, $T(x, w_i)$ and $T(w_i, w_j)$ are at most $60\alpha t$ by Lemma 10.7. Therefore

$$4t \leq 8 \cdot (23\alpha t) + \alpha t + 3 \cdot 4 \cdot (25\alpha t/2) + 2 \cdot 6 \cdot (60\alpha t) = 1055\alpha t,$$

and hence $\alpha \geq 4/1055$. Thus, $T(v, v) \leq -4t/1055$ for some minimal vector v, since otherwise α could be decreased. □

LEMMA 10.9. *If $\beta = 1$ and $t < 0$, then we can take $\alpha = 4/1033$.*

Proof. With the same notation as in the proof of Lemma 10.8 we have

$$T(z, z) = 4T(y, y) + T(x, x) + \sum_i T(w_i, w_i) - 4T(x, y) \\ - 4\sum_i T(y, w_i) + 2\sum_i T(x, w_i) + 2\sum_{i<j} T(w_i, w_j).$$

Since we know $T(x, y) = t < 0$, we get as before

$$-4t = -4T(y, y) - T(x, x) - \sum_i T(w_i, w_i) + T(z, z) \\ + 4\sum_i T(y, w_i) - 2\sum_i T(x, w_i) - 2\sum_{i<j} T(w_i, w_j).$$

We now use the same strategy as in Lemma 10.8. Namely, we assume that for all minimal vectors v, $T(v, v) \geq -\alpha|t| = \alpha t$. It follows that $-T(y, y) \leq \alpha|t| = -\alpha t$, and the same holds for $T(x, x)$ and $T(w_i, w_i)$. By Lemma 10.4, $T(z, z) \leq -23\alpha t$. This time by Lemma 10.6, $T(y, w_i)$ is at most $-47\alpha t/2$, whereas by Lemma 10.7, $T(x, w_i)$ and $T(w_i, w_j)$ are at least $60\alpha t$, so their negatives are at most $-60\alpha t$. Therefore

$$-4t \leq -(23\alpha t) - 8\alpha t + 3 \cdot 4 \cdot (-47\alpha t/2) + 2 \cdot 6 \cdot (-60\alpha t) = -1033\alpha t,$$

and hence $\alpha \geq 4/1033$ after canceling $-t$ which is positive. □

We conclude that $\alpha = 4/1055$ satisfies the properties we stated at the beginning of the section.

11. The case of E_8

A very similar proof shows that the E_8 lattice is the unique densest lattice packing in $\mathbb{R}^8$. Since the details of the proofs are analogous, and the result was already known, we merely sketch them in this section.

In E_8 there are 240 minimal vectors of length $\sqrt{2}$, if we normalize the length as usual so that the lattice is unimodular. Let Λ be a lattice of covolume 1 that is at least as dense as E_8. As in the case of the Leech lattice, we find a suitable radial function f with $r \le \sqrt{2}(1+1.2\cdot 10^{-15})$, which proves that no sphere packing in $\mathbb{R}^8$ can exceed the density of E_8 by a factor of more than $1+10^{-14}$.

This function allows us to show that for $0 \neq |x| \le \sqrt{7}$, the length of x is restricted to the set

$$\big[\sqrt{2},\sqrt{2}(1+\varepsilon)\big) \cup \big(2(1-\mu),2(1+\mu)\big) \cup \big(\sqrt{6}(1-\nu),\sqrt{6}(1+\nu)\big),$$

where

$$\begin{aligned}\varepsilon &= 1.45\cdot 10^{-13},\\ \mu &= 1.03\cdot 10^{-6}, \text{ and}\\ \nu &= 4.44\cdot 10^{-6}.\end{aligned}$$

The details of this calculation are in the accompanying PARI file `E8verifyf.txt`. All the remaining calculations from this point on for the E_8 case are verified in the Maple file `E8rest.txt`.

Define a nearly minimal vector to be a vector with length in $[\sqrt{2},\sqrt{2}(1+\varepsilon)]$. We form a spherical code by rescaling the nearly minimal vectors to lie on the unit sphere S^7.

We use the polynomial

$$f_\varepsilon(x) = (x+1)\left(x+\frac{1}{2}\right)^2 x^2\left(x-\left(1-\frac{1}{2(1+\varepsilon)^2}\right)\right)$$

to show as before that there are at most 240 nearly minimal vectors. Similarly, the analogue of Lemma 4.4 goes through with a different function defined on $\mathbb{R}^8$, and proves that there are exactly 240 nearly minimal vectors.

11.1. *Spherical code.* The analogue of Section 5 is that all the inner products between the normalized nearly minimal vectors $u/|u|$ must be either ± 1 or at most $6\cdot 10^{-5}$ from some element of the set $\{-1/2,0,1/2\}$. Then further analysis gives us the following better bounds.

For $\langle u,v\rangle \approx 1$ we have

$$\frac{2-(1+\varepsilon)^2}{2(1+\varepsilon)^2} \le \left\langle \frac{u}{|u|},\frac{v}{|v|}\right\rangle \le (1+\varepsilon)^2-\frac{1}{2},$$

whereas for $\langle u, v\rangle \approx 0$ we have

$$\frac{1-(1+\mu)^2}{(1+\varepsilon)^2} \leq \left\langle \frac{u}{|u|}, \frac{v}{|v|} \right\rangle \leq (1+\varepsilon)^2 - (1-\mu)^2.$$

We conclude that $\sigma \leq 8.89\cdot 10^{-6}$, where σ is the maximal error in the inner products from the spherical code.

11.2. *Intersection numbers.* The analogue of Lemma 6.2 is easily shown using the polynomial f_ε.

LEMMA 11.1. *If $g\colon S^7 \to \mathbb{R}$ is a polynomial of total degree at most* 6, *then*

$$\left| \sum_{z\in\mathscr{C}_\Lambda} g(z) - \frac{240}{\mathrm{vol}(S^7)} \int_{S^7} g(z)\,dz \right| \leq 3.48\cdot 10^{-4} |g|_2,$$

where $|g|_2$ denotes the norm on $L^2(S^7)$.

Now, since the kissing configuration of E_8 is a 7-spherical design, we find that the intersection numbers of E_8 can be obtained by solving the linear system of equations

$$\sum_{\alpha,\beta\in S} \alpha^i \beta^j P_\gamma(\alpha,\beta) = \frac{240}{\mathrm{vol}(S^7)} \int_{S^7} g_{i,j}(z)\,dz.$$

for $i, j \in \{0,1,2\}$, where $S = \{0, \pm 1/2, \pm 1\}$ is the set of possible inner products. As before, we know the values of $P_\gamma(\pm 1, \alpha)$ and $P_\gamma(\alpha, \pm 1)$. When we perform the same calculation for Λ, the value of

$$\frac{240}{\mathrm{vol}(S^7)} \int_{S^7} g_{i,j}(z)\,dz$$

differs by at most 30σ from the corresponding value for E_8. If we apply Lemma 6.3 and compute the error introduced into the system of equations by going from E_8 to Λ, we get a bound of

$$\left(3.48\cdot 10^{-4}\right) \frac{\pi^2}{\sqrt{3}} + 30\sigma + 240(1+2\sigma)\sigma < 4.4\cdot 10^{-3}.$$

The ∞-norm of the inverse matrix is 100, from which it follows that the intersection numbers in Λ differ from those in E_8 by at most 0.44. Because that number is less than 1, they must be the same.

11.3. *Association scheme.* The proof of uniqueness for the Leech lattice association scheme depended only on the eutaxy of the Leech lattice and the uniqueness of its kissing arrangement. The same holds for the E_8 lattice. With $N = 240$ and $C = 4/N = 1/60$ we have the following lemma.

LEMMA 11.2. *For every $x \in \mathbb{R}^8$,*

$$\langle x, x\rangle = C\sum_{i=1}^{N}\langle x, u_i\rangle^2.$$

The proof of the lemma is essentially the same. We then use the lemma to prove the uniqueness of the association scheme.

THEOREM 11.3. *There is only one 4-class association scheme with the same size, valencies and intersection numbers as the association scheme of minimal vectors of the E_8 lattice.*

The proof of the theorem involves, as before, the operator

$$P = 2C\left(A_1 + \frac{1}{2}A_{1/2} - \frac{1}{2}A_{-1/2} - A_{-1}\right),$$

which turns out to be a projection to an 8-dimensional space. Again, the proof is essentially the same as for the Leech lattice.

11.4. *Inner product bounds.* The inner product bounds use only the intersection numbers (Lemma 7.4, for which we needed the isomorphism of association schemes, deals with a case that does not occur in E_8). We get almost the same bounds as in Section 7. The proofs have to be slightly modified due to the fact that the minimal norm of the E_8 lattice is 2 instead of 4 for the Leech lattice. We get the following result:

LEMMA 11.4. *Let u, v be nearly minimal vectors.*

(1) *For $\langle u, v\rangle \approx 2$ we have $2 \le \langle u, v\rangle \le 2 + (5/2)\varepsilon$.*

(2) *For $\langle u, v\rangle \approx 1$ we have $1 - (5/2)\varepsilon \le \langle u, v\rangle \le 1 + (9/2)\varepsilon$.*

(3) *For $\langle u, v\rangle \approx 0$ we have $-7\varepsilon \le \langle u, v\rangle \le 7\varepsilon$.*

11.5. *A basis of nearly minimal vectors.* The proof that there is a basis of nearly minimal vectors is completely analogous. Consider the basis of minimal vectors

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 \end{pmatrix}$$

of E_8, where the row vectors are the basis elements. Then the corresponding vectors in Λ (via an isomorphism of association schemes) can be shown to be a basis for Λ.

11.6. *Computing* α. One first proves an analogue of Lemma 10.1 by considering the vectors $w_i = (0, \dots, 1, 1, \dots, 0)$ and $v_i = (0, \dots, 1, -1, \dots, 0)$ where the i and $i+1$ coordinates are nonzero, for $i \in \{1, 3, 5, 7\}$.

The analogue of Lemma 10.2 is immediate:

LEMMA 11.5. *Let* $v_1, \dots, v_8$ *be orthogonal minimal vectors in the* E_8 *lattice. If* $\sum_{i,j} \tilde{s}_{i,j} t_{i,j} = 0$, *then*

$$\sum_{i=1}^{8} T(v_i) = 0.$$

We then proceed to use these lemmas as before to prove bounds on α.

LEMMA 11.6. *With the same notation for* β *and* t *as before, we have the following bounds*:

(1) *If* $\beta = 2$ *and* $t < 0$ *then we can take* $\alpha = 1$.

(2) *If* $\beta = 2$ *and* $t > 0$ *then we can take* $\alpha = 1/7$.

(3) *If* $\beta = 1$ *and* $t < 0$ *then we can take* $\alpha = 2/9$.

(4) *If* $\beta = 1$ *and* $t > 0$ *then we can take* $\alpha = 2/15$.

(5) *If* $\beta = 0$ *then we can take* $\alpha = 1/20$.

In fact, the greatest possible value of α is $1/7$, and that can be rigorously proved by computer calculations. (The linear programs are small enough that one can solve them using exact rational arithmetic. The Maple file `E8seventh.txt` contains the calculations.) However, the weaker bound of $1/20$ will suffice.

11.7. *Local optimality of* E_8. The proofs of perfection and eutaxy of E_8 closely parallel those for the Leech lattice. The Gram matrix for the basis of E_8 that we chose above is small enough that we can compute all its minors quickly. We find that for $0 < \rho < 10^{-3}$,

$$\begin{aligned} D_\rho &\geq 1 - \rho^2(7936 + 21162\sqrt{3}\rho + 84256\rho^2 + 47300\sqrt{5}\rho^3 \\ &\qquad + 74088\rho^4 + 10290\sqrt{7}\rho^5 + 4096\rho^6) \\ &\geq 1 - 7973\rho^2. \end{aligned}$$

We conclude from the above calculations that for every perturbation by $\rho t_{i,j}$ where $\max\{|t_{i,j}|\} \leq 1$ and $\sum_{i,j} \tilde{s}_{i,j} t_{i,j} = 0$, we have some k such that

$$\frac{D_\rho^{-1/8} Q_\rho(u_k)}{D^{-1/8} \cdot 2} \leq (1 - \rho/40)(1 - 7973\rho^2)^{-1/8}.$$

This bound is strictly less than 1 when $0 < \rho \leq 2.5 \cdot 10^{-5}$.

As before, we have one final issue to deal with: our perturbation may not satisfy $\sum_{i,j} \tilde{s}_{i,j} t_{i,j} = 0$. We normalize as before by setting

$$t_{i,j} = \frac{s_{i,j} + \eta_{i,j}}{1 + \Delta/8} - s_{i,j}$$

(the notation is as in the Leech lattice case), and need to check that $|t_{i,j}| \le 2.5 \cdot 10^{-5}$. From Lemma 11.4, we have $|\eta_{i,j}| \le 7\varepsilon$. Now the sum of the absolute values of the entries of $\tilde{S}$ is 620, so $|\Delta| \le 4340\varepsilon$. The maximum value of $|s_{i,j}|$ is 2, so putting everything together we have

$$|t_{i,j}| = \left| \frac{\eta_{i,j} + s_{i,j}\Delta/8}{1 + \Delta/8} \right| \le \frac{7\varepsilon + 2 \cdot 4340\varepsilon/8}{1 - 4340\varepsilon/8} < 1.6 \cdot 10^{-10}.$$

This proves that Λ must be the same as E_8 since it lies within the range of local optimality of E_8.

This completes our new proof of the optimality of E_8:

THEOREM 11.7 (Blichfeldt, Vetčinkin). *The E_8 root lattice is the unique densest lattice in $\mathbb{R}^8$, up to scaling and isometries of $\mathbb{R}^8$.*

Acknowledgements

We thank Noam Elkies, László Lovász, and Stephen D. Miller for helpful discussions, Richard Pollack, Fabrice Rouillier, and Marie-Françoise Roy for advice on computer algebra, John Dunagan for advice on linear programming software, William Stein for allowing us to use several of his computers, Dimitar Jetchev for translating our computer code into Magma, and Richard Borcherds, Noam Elkies, Simon Litsyn, and Eric Rains for comments on the manuscript.

Appendix A. Computer calculations

The computer files for checking our calculations are available from the arXiv. This paper is available as `math.MG/0403263`. To access the auxiliary files, download the source files for the paper. That will produce not only the LaTeX files for the paper but also the computer algebra code.

By far the most extensive use of computer calculations in this paper occurs in Subsection 4.1. The calculations are carried out in the file `verifyf.txt`, which consists of PARI code. PARI is a free computer algebra system designed for rapid number-theoretic calculations. See `http://pari.math.u-bordeaux.fr` for more information on PARI or to download a copy.

Our PARI files all contain comments that should help make them understandable to those unfamiliar with PARI.

First, we will explain how one proves the properties of the function f used in Subsection 4.1; then we will explain how it was constructed. Finally, we briefly discuss the verification of the other calculations in this paper.

There are two auxiliary files for dealing with f: `fcoeffs.txt` contains coefficients $c_0, \dots, c_{803}$ which we will use to construct f, and `roots.txt` contains values $r_0, \dots, r_{200}$ that are nearly roots (meaning the polynomial is very near 0 at those locations, although in fact no real roots are nearby, except near r_0).

The file `verifyf.txt` carries out the following verifications. Let

$$f_0(z) = \sum_{i=0}^{803} c_i i! L_i^{11}(z). \tag{A.5}$$

Define $f\colon \mathbb{R}^{24} \to \mathbb{R}$ by $f(x) = f_0(2\pi|x|^2)e^{-\pi|x|^2}/10^{3000}$. (The denominator of 10^{3000} makes the coefficients c_i integers, which is convenient.) The value of r used in Subsection 4.1 satisfies $2\pi r^2 = r_0$.

We first need to check that $f(x) \le 0$ for $|x| \ge r$, which is equivalent to $f_0(z) \le 0$ for $z \ge r_0$. In principle one could check this straightforwardly using Sturm's theorem, but that takes a tremendous amount of time for such a huge polynomial. Instead, we will use Descartes' rule of signs in a somewhat complicated way that may not appear *a priori* superior, but works overwhelmingly better in practice: the number of roots of a polynomial p in the interval (a,b) is at most the number of sign changes in the coefficients of

$$p\left(\frac{a+bz}{1+z}\right)(1+z)^{\deg(p)},$$

and is congruent to it modulo 2. For (a,∞) one can simply use $p(a+z)$. This result is sometimes known as Jacobi's rule of signs (see Corollary 10.1.13 in [RS02, p. 320]).

We check using Jacobi's rule of signs that f_0 has no roots in $(\lceil r_{200} \rceil, \infty)$ or $(\lceil r_i \rceil, \lfloor r_{i+1} \rfloor)$ for $1 \le i \le 199$ (and also check that it does not vanish at the endpoints), and that it has exactly one root in $(0, \lfloor r_1 \rfloor)$. Then we must check that it does not vanish on $[\lfloor r_i \rfloor, \lceil r_i \rceil]$ with $1 \le i \le 200$, and that its one root is less than r_0 (for that we simply compute the sign of $f_0(r_0)$).

Dealing with the intervals $[\lfloor r_i \rfloor, \lceil r_i \rceil]$ is a little more difficult. We use Jacobi's rule of signs to check that f_0'' has no roots on these intervals, so f_0' is monotonic and has at most one root in each. We then check that $f_0'(r_i - 10^{-350}) > 0$ and $f_0'(r_i + 10^{-350}) < 0$, so the maximum of f_0 must occur within 10^{-350} of r_i. However,

$$|f_0'(r_i \pm 10^{-350})| \le 10^{3285},$$

from which it follows (by the mean value theorem and the monotonicity of f_0') that

$$\left| f_0(r_i) - \max_{x \in [\lfloor r_i \rfloor, \lceil r_i \rceil]} f_0(x) \right| \le 10^{-350} \cdot 10^{3285} = 10^{2935}.$$

Because $|f_0(r_i)| \le -10^{2945}$, f_0 has no roots in $[\lfloor r_i \rfloor, \lceil r_i \rceil]$.

To make the proof more efficient, we arrange the calculations to ensure that only integer arithmetic is used, so that PARI does not spend time reducing fractions to lowest terms. (That explains why the coefficients in (A.5) are multiplied by $i!$.)

Dealing with $\widehat{f}$ is similar, but of course it uses the polynomial

$$h_0(z) = \sum_{i=0}^{803} (-1)^i c_i i! L_i^{11}(z)$$

instead of f_0, and in this case r_0 plays the same role as $r_1, \dots, r_{200}$ do (rather than being treated differently, as above).

All that remains is to check $f(0) = \widehat{f}(0) = 1$, which is true because $f_0(0) = h_0(0) = 10^{3000}$. These calculations suffice for the proof that no sphere packing can be more than a factor of $1 + 1.65 \cdot 10^{-30}$ times denser than Λ_{24}. However, Proposition 4.3 requires more detailed information on the values of f. In `verifyf.txt` we check these inequalities using

$$\sum_{i=0}^{351} \frac{(-z)^i}{i!} \le e^{-z} \le \sum_{i=0}^{350} \frac{(-z)^i}{i!}$$

for $0 \le z \le 60$, as well as rational upper and lower bounds for π, to avoid having to deal with irrational numbers.

Unfortunately the file `verifyf.txt` cannot address where f comes from (it takes far longer to locate f than to verify its properties). The construction is based on the numerical technique described in Section 7 of [CE03], which describes functions via forced double root locations that are then repeatedly perturbed until they reach a local optimum. Instead of this straightforward optimization algorithm we implemented a high-dimensional version of Newton's method (which locates a root of the derivative of $f(2)$ as an implicit function of the forced double roots—this is valuable because $f(2)$ is roughly proportional to $|r - 2|$). We arrived at 200 forced double roots, whose locations are specified in `roots.txt`. The next step of the method from [CE03] also caused trouble: solving for the polynomial with those forced roots. Exact rational arithmetic was immensely time-consuming and produced huge denominators. Instead, we carried out high-precision floating point arithmetic and rounded the result to within 10^{-3000}. That could ruin the sign conditions on f and $\widehat{f}$, by turning a double root into a pair of nearby single roots, so instead of solving for actual double roots we required that f and $\widehat{f}$ should stay slightly on the correct side of 0. That does not greatly change the resulting bounds, and leads to the function f used in this paper.

Lemma 4.4 requires the second largest amount of computation to check, although far less than Subsection 4.1. The file `verifyg.txt` and the auxiliary file `gcoeffs.txt` deal with it in a fairly straightforward way. The calculations required for (9.2) and (9.3) are dealt with in `verifygram.txt`.

Finally, the file `verifyrest.txt` verifies all remaining calculations in the paper for the Leech lattice case. Many of the calculations in this file could be checked by hand, but that would be unpleasant and error-prone. Instead of PARI code, this file contains Maple code. Maple is less efficient but more flexible, and it seemed easiest to use in these calculations.

Our computer calculations are completely rigorous, in the sense that they are carried out using exact arithmetic, and thus avoid traps such as round-off error. Nevertheless, we cannot eliminate the possibility of a hardware error or a bug in software beyond our control, such as the operating system or computer algebra program. Under these circumstances, even assuming our programs are correctly written they may return incorrect results. This possibility appears quite unlikely, and we do not consider it a serious worry. However, we have addressed it by asking Dimitar Jetchev to translate our programs into the Magma computer algebra system. His translation is contained in the file `magmacode.txt`. Using it, we have independently checked our calculations on a different type of processor, a different computer algebra system, and a different operating system.

We have also documented our calculations for the E_8 proof. The details can be found in the files `E8verifyf.txt` and `E8rest.txt`. We include fewer comments in these files than in the others, because their structure is parallel to the Leech lattice case. The file `E8seventh.txt` contains a proof that $\alpha = 1/7$ works in the E_8 case, although we do not require that for the proof of Theorem 11.7.

Appendix B. Background

In this appendix we collect brief definitions and descriptions of a few of the principal objects and techniques used in this paper.

An *even unimodular lattice* $\Lambda \subset \mathbb{R}^n$ is a lattice such that $|\Lambda| = 1$, $\langle x, y\rangle \in \mathbb{Z}$ for all $x, y \in \Lambda$, and $\langle x, x\rangle \in 2\mathbb{Z}$ for all $x \in \Lambda$. Such lattices exist only when n is a multiple of 8. Up to isometries of $\mathbb{R}^n$, the unique example when $n = 8$ is E_8, and there are 24 examples in $\mathbb{R}^{24}$, among which the Leech lattice is the unique one containing no vectors of length $\sqrt{2}$. See [CS99, p. 48] for more information.

A *spherical code* of minimal angle φ in the unit sphere S^{n-1} is a collection $\mathscr{C} \subset S^{n-1}$ of points such that $\langle x, y\rangle \le \cos\varphi$ for all $x, y \in \mathscr{C}$ with $x \ne y$. In other words, no two distinct points of $\mathscr{C}$ form an angle smaller than φ centered at the origin. Spherical codes are to S^{n-1} as binary error-correcting codes are to $\{0,1\}^n$, or as sphere packings are to $\mathbb{R}^n$.

The most important approach to bounding the size of spherical codes is *linear programming bounds* (due to Delsarte [Del72]; see Chapter 9 of [CS99] for an exposition). These bounds rely on the following property of the ultraspherical polynomials, which follows from Lemma 6.1: if $\lambda = n/2-1$, then for each finite subset $\mathscr{C} \subset S^{n-1}$,

$$\sum_{x,y\in\mathscr{C}} C_i^{\lambda}(\langle x,y\rangle) \geq 0.$$

Suppose $f_0,\dots,f_d \geq 0$, and that $f(z) = \sum_{i=0}^{d} f_i C_i^{\lambda}(z)$ satisfies $f(z) \leq 0$ for $z \in [-1,\cos\varphi]$. Then every spherical code $\mathscr{C}$ in S^{n-1} with minimal angle φ has size bounded by $|\mathscr{C}| \leq f(1)/f_0$ (assuming $f_0 \neq 0$). The proof is simple:

$$\begin{aligned}
|\mathscr{C}|f(1) &= \sum_{x\in\mathscr{C}} f(\langle x,x\rangle)\\
&\geq \sum_{x,y\in\mathscr{C}} f(\langle x,y\rangle)\\
&= \sum_{x,y\in\mathscr{C}} f_0 + \sum_{i=1}^{d} f_i \sum_{x,y\in\mathscr{C}} C_i^{\lambda}(\langle x,y\rangle)\\
&\geq \sum_{x,y\in\mathscr{C}} f_0\\
&= |\mathscr{C}|^2 f_0.
\end{aligned}$$

The most dramatic application of the linear programming bounds for spherical codes is the solution of the *kissing problem* in $\mathbb{R}^8$ and $\mathbb{R}^{24}$: how many unit balls can be placed tangent to a central unit ball so that their interiors do not overlap? This condition amounts to saying that the points of tangency form a spherical code with minimal angle $\pi/3$. In $\mathbb{R}^8$ the answer is 240, and in $\mathbb{R}^{24}$ the answer is 196560. The codes are formed from the minimal vectors in E_8 and the Leech lattice, respectively (of course the radius of the sphere involved differs in the two examples). Optimality follows from the linear programming bounds by taking

$$f(z) = (z+1)\left(z+\frac{1}{2}\right)^2 z^2 \left(z-\frac{1}{2}\right)$$

in $\mathbb{R}^8$ and

$$f(z) = (z+1)\left(z+\frac{1}{2}\right)^2\left(z+\frac{1}{4}\right)^2 z^2 \left(z-\frac{1}{4}\right)^2\left(z-\frac{1}{2}\right)$$

in $\mathbb{R}^{24}$. This most remarkable fact was discovered independently by Levenshtein [Lev79] and by Odlyzko and Sloane [OS79].

A *spherical t-design* in S^{n-1} is a nonempty finite subset $\mathcal{D}$ of S^{n-1} such that for every polynomial $f\colon \mathbb{R}^n \to \mathbb{R}$ of total degree at most t,

$$\frac{1}{|\mathcal{D}|}\sum_{x\in\mathcal{D}} f(x) = \frac{1}{\mathrm{vol}(S^{n-1})}\int_{S^{n-1}} f(x)\,dx.$$

In other words, the average of f over $\mathcal{D}$ equals its average over the entire sphere. The minimal vectors of the Leech lattice form a spherical 11-design, and those of E_8 form a spherical 7-design.

A *k-class association scheme* is a set $\mathcal{A}$ together with a partition

$$\mathcal{A}^2 = \mathcal{A}_0 \cup \cdots \cup \mathcal{A}_k$$

such that $\mathcal{A}_0 = \{(x,x) : x \in \mathcal{A}\}$, $(x,y)\in\mathcal{A}_i$ if and only if $(y,x)\in\mathcal{A}_i$, and the following property holds. Fix ℓ, m, and n in $\mathbb{Z}\cap[0,k]$; then for all $x,y\in\mathcal{A}$ with $(x,y)\in\mathcal{A}_\ell$, there are the same number $P_\ell(m,n)$ of $z\in\mathcal{A}$ such that $(x,z)\in\mathcal{A}_m$ and $(y,z)\in\mathcal{A}_n$. (That is, $P_\ell(m,n)$ depends only on ℓ, m, and n, and not on x and y.) These numbers are called the *intersection numbers* of the association scheme. When $\ell = 0$ and $m = n$ they are also called *valencies*. In the body of the paper we modify this notation slightly for the association scheme $\mathcal{C}_\Lambda$ (in a trivial way): we label the classes with the corresponding inner products in $\mathcal{C}_{24}$, and use these labels in the notation for the intersection numbers.

References

[AAR99] G. E. ANDREWS, R. ASKEY, and R. ROY, *Special Functions*, *Encyclopedia Math. Appl.* **71**, Cambridge Univ. Press, Cambridge, 1999. MR 2000g:33001 Zbl 0920.33001

[BS81] E. BANNAI and N. J. A. SLOANE, Uniqueness of certain spherical codes, *Canad. J. Math.* **33** (1981), 437–449. MR 83a:94020 Zbl 0457.05017

[Bar57] E. S. BARNES, The complete enumeration of extreme senary forms, *Philos. Trans. Roy. Soc. London. Ser. A.* **249** (1957), 461–506. MR 19,251d Zbl 0077.26601

[Bli35] H. F. BLICHFELDT, The minimum values of positive quadratic forms in six, seven and eight variables, *Math. Z.* **39** (1935), 1–15. MR 1545485 Zbl 0009.24403

[BH95] A. E. BROUWER and W. H. HAEMERS, Association schemes, in *Handbook of Combinatorics*, *Vol.* 1, Elsevier, Amsterdam, 1995, pp. 747–771. MR 97a:05217 Zbl 0849.05072

[Cha46] T. W. CHAUNDY, The arithmetic minima of positive quadratic forms, I, *Quart. J. Math.*, *Oxford Ser.* **17** (1946), 166–192. MR 8,137g Zbl 0060.11102

[Coh02] H. COHN, New upper bounds on sphere packings, II, *Geom. Topol.* **6** (2002), 329–353. MR 2004b:52032 Zbl 1028.52011

[CE03] H. COHN and N. ELKIES, New upper bounds on sphere packings, I, *Ann. of Math.* **157** (2003), 689–714. MR 2004b:11096 Zbl 1041.52011

[CS82] J. H. CONWAY and N. J. A. SLOANE, Laminated lattices, *Ann. of Math.* **116** (1982), 593–620. MR 84c:52015 Zbl 0502.52016

[CS99] ———, *Sphere Packings*, *Lattices and Groups*, third ed., *Grundl. Math. Wissen.* **290**, Springer-Verlag, New York, 1999. MR 2000b:11077 Zbl 0915.52003

[Del72] P. DELSARTE, Bounds for unrestricted codes, by linear programming, *Philips Res. Rep.* **27** (1972), 272–289. MR 47 #3096 Zbl 0348.94016

[DGS77] P. DELSARTE, J. M. GOETHALS, and J. J. SEIDEL, Spherical codes and designs, *Geometriae Dedicata* **6** (1977), 363–388. MR 58 #5302 Zbl 0376.05015

[Elk97] N. D. ELKIES, Mordell-Weil lattices in characteristic 2, II: The Leech lattice as a Mordell-Weil lattice, *Invent. Math.* **128** (1997), 1–8. MR 98c:11063 Zbl 0897.11023

[Elk00a] ———, Lattices, linear codes, and invariants, I, *Notices Amer. Math. Soc.* **47** (2000), 1238–1245. MR 2001g:11110 Zbl 0992.11041

[Elk00b] ———, Lattices, linear codes, and invariants, II, *Notices Amer. Math. Soc.* **47** (2000), 1382–1391. MR 2001k:11128 Zbl 1047.11065

[Gau31] C. F. GAUSS, Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen von Ludwig August Seeber, Göttingische gelehrte Anzeigen, July 9, 1831, Reprinted in *Werke*, Vol. 2, Königliche Gesellschaft der Wissenschaften, Göttingen, 1863, 188–196; Available at `http://gdz.sub.uni-goettingen.de`.

[GL87] P. M. GRUBER and C. G. LEKKERKERKER, *Geometry of Numbers*, second ed., *North-Holland Math. Library* **37**, North-Holland Publ. Co., Amsterdam, 1987. MR 88j:11034 Zbl 0611.10017

[Hel00] S. HELGASON, *Groups and Geometric Analysis*: *Integral Geometry*, *Invariant Differential Operators*, *and Spherical Functions*, *Math. Surveys and Monogr.* **83**, Amer. Math. Soc., Providence, RI, 2000. MR 2001h:22001 Zbl 0965.43007

[HJ85] R. A. HORN and C. R. JOHNSON, *Matrix Analysis*, Cambridge Univ. Press, Cambridge, 1985. MR 87e:15001 Zbl 0576.15001

[Kha91] V. P. KHAVIN, Methods and structure of commutative harmonic analysis, in *Commutative Harmonic Analysis*, I (V. P. KHAVIN and N. K. NIKOL'SKIJ, eds.), *Encycl. Math. Sci.* **15**, Springer-Verlag, New York, 1991, pp. 1–111. MR 1134136 Zbl 0727.43001

[KZ73] A. KORKINE and G. ZOLOTAREFF, Sur les formes quadratiques, *Math. Annalen* **6** (1873), 366–389. MR 1509828

[KZ77] ———, Sur les formes quadratiques positives, *Math. Annalen* **11** (1877), 242–292. MR 1509914 JFM 09.0139.01

[Leb72] N. N. LEBEDEV, *Special Functions and their Applications*, Dover Publ., New York, 1972. MR 50 #2568 Zbl 0271.33001

[Lev79] V. I. LEVENŠTEĬN, On bounds for packings in n-dimensional Euclidean space, *Soviet Math. Dokl.* **20** (1979), 417–421. MR 80d:52017 Zbl 0436.52011

[Mar03] J. MARTINET, *Perfect Lattices in Euclidean Spaces*, *Grundl. Math. Wissen.* **327**, Springer-Verlag, New York, 2003. MR 2003m:11099 Zbl 1017.11031

[Mui60] T. MUIR, *A Treatise on the Theory of Determinants*, *Revised and enlarged by William H. Metzler*, Dover Publ., New York, 1960. MR 22 #5644

[OS79] A. M. ODLYZKO and N. J. A. SLOANE, New bounds on the number of unit spheres that can touch a unit sphere in n dimensions, *J. Combin. Theory Ser.* A **26** (1979), 210–214. MR 81d:52010 Zbl 0408.52007

[RS02] Q. I. RAHMAN and G. SCHMEISSER, *Analytic Theory of Polynomials*, *London Math. Soc. Monogr.* **26**, The Clarendon Press, Oxford Univ. Press, Oxford, 2002. MR 2004b:30015 Zbl 1072.30006

[Tho83] T. M. THOMPSON, *From Error-Correcting Codes Through Sphere Packings to Simple Groups*, *Carus Math. Monogr.* **21**, Mathematical Association of America, Washington, DC, 1983. MR 86j:94002 Zbl 0545.94016

[Vet80] N. M. VETČINKIN, Uniqueness of classes of positive quadratic forms on which values of the Hermite constant are attained for $6 \leq n \leq 8$, *Trudy Mat. Inst. Steklov.* **152** (1980), 34–86, English translation in *Proc. Steklov Inst. Math.* **152** (1982), 37–95. MR 82f:10040 Zbl 0457.10013

[Vor08] G. VORONOI, Propriétés des formes quadratiques positives parfaites, *J. Reine Angew. Math.* **133** (1908), 97–178.

(Received March 17, 2004)

E-mail address: cohn@microsoft.com
MICROSOFT RESEARCH, ONE MICROSOFT WAY, REDMOND, WA 98052-6399, UNITED STATES
Current address: MICROSOFT RESEARCH NEW ENGLAND, ONE MEMORIAL DRIVE, CAMBRIDGE, MA 02142, UNITED STATES

E-mail address: abhinav@math.mit.edu
DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MA 02138, UNITED STATES
Current address: DEPARTMENT OF MATHEMATICS, ROOM 2-169, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139, UNITED STATES