hexagon:2611.01075v1

EXPLICIT LATTICE PACKINGS

Abstract. We give explicit lattices in large dimension n with packing density at least $2^{-1.2463n}$. The best previous explicit lattices reached $2^{-1.3889n}$. A simpler version of the construction reaches $2^{-1.3n}$, and a basis can be computed in time polynomial in n. We build the lattices from the Leech lattice, a Ramanujan graph and algebraic-geometry codes. We also explain what would be needed to push the same construction past the Minkowski–Hlawka bound 2^{-n}.

1. Introduction

1.1. **Dense lattices in high dimensions.** Let $\Lambda \subset \mathbb{R}^n$ be a lattice of rank n. Its Hermite invariant $\gamma(\Lambda) = \lambda_1(\Lambda)^2/\operatorname{covol}(\Lambda)^{2/n}$ is the squared length of a shortest nonzero vector after rescaling Λ to covolume one, and the density of the associated packing of equal balls is $\Delta(\Lambda) = V_n\gamma(\Lambda)^{n/2}2^{-n}$, where V_n is the volume of the unit ball. A sequence with $\gamma(\Lambda_n) \geq (c - o(1))n$ has density at least $2^{-(E(c)+o(1))n}$, where $E(c) = 1 - \frac{1}{2}\log_2(2\pi ec)$; see Section 2.

The Minkowski–Hlawka theorem [13] asserts that lattices with $\Delta(\Lambda) \geq \zeta(n)2^{1-n}$ exist in every dimension. In the normalization above this corresponds to $c = 1/(2\pi e) = 0.05855\ldots$ and $E = 1$. The existential bound has been improved by polynomial factors, by Rogers [26], Ball [1], Vance [32], Venkatesh [33] and Klartag [17], who obtains lattices of density at least $cn^2 2^{-n}$. Abuya, Gargava and Zhao [18] combined Klartag's method with Venkatesh's cyclotomic symmetries and gained a further factor $\log\log n$ along a sparse sequence of dimensions. Gargava, Gröbner and Simkin [19] then obtained lattices of density $\gg n^2 \log\log n\, 2^{-n}$ in every sufficiently large dimension. For general packings Campos, Jenssen, Michelen and Sahasrabudhe [3] obtained density $(1 - o(1))\frac{1}{2}n\log n\, 2^{-n}$. On the other side, the Kabatiansky–Levenshtein bound [15] gives $\Delta \leq 2^{-(0.599\ldots+o(1))n}$ for every packing. All of the lower bounds above are existential: they show that a random lattice, or a random element of a structured family, is good with positive probability.

1.2. **Explicit constructions.** Finding an explicit sequence of lattices with $E(c)$ bounded, let alone $E(c) \leq 1$, is a much harder problem.

What we mean by explicit. The word is used in different ways in the literature, so we state our meaning plainly. A sequence of lattices Λ_n is *explicit* if there is a deterministic algorithm that, given n, outputs a basis of Λ_n in time polynomial in n. The bound on the minimum must then be proved for the lattice that the algorithm outputs. The algorithm does not have to check the bound itself.

This is the analogue of the notion used for error-correcting codes, where one asks for codes that can be written down in polynomial time. There, random codes meet the Gilbert–Varshamov bound, but no polynomial-time construction of binary codes on that bound is known. Dense lattices are in the same position.

The definition rules out several familiar ways of producing good lattices.

- *Random lattices.* The Minkowski–Hlawka theorem and all its improvements show that a random lattice from a suitable distribution is good with positive probability. This does not give a specific lattice.

Date: November 2026.

- *Randomized algorithms.* An algorithm that flips coins and succeeds with high probability is not allowed, even if it runs fast. Its output is a distribution, not a sequence.
- *Exhaustive search.* One can list exponentially many candidates and keep a good one. The effective versions of the Minkowski–Hlawka theorem do this, in time $\exp(O(n \log n))$. This is deterministic, but it is not polynomial time.
- *Testing candidates by their minimum.* Computing the minimum of a lattice is the shortest vector problem, which is NP-hard under randomized reductions. So even a short list of candidates cannot be tested in polynomial time by computing minima.
- *Existence without construction.* A construction that uses an object known only to exist, such as a code on the Gilbert–Varshamov bound, is not explicit unless that object can itself be produced in polynomial time.

The definition also allows some things that deserve to be said openly. Any fixed finite object may be used, however it was found, because it costs constant time. Our constructions use the Leech lattice and several large fixed integers in this way. Constants may be enormous: in our constructions the graph degree is $2^{36} + 1$ or $2^{120} + 1$, and the smallest lattices are far too large to write down in practice. The definition is a statement about growth rates, not about practical computation. Finally, a search over polynomially many candidates would be allowed, but our constructions do not use any search.

Lattices given by a canonical algebraic definition, such as the lattices built from class field towers below, are explicit in a weaker sense. They are described exactly, but a polynomial-time algorithm for a basis may not be known. We point this out where it matters.

Construction complexity. The systematic study of how hard it is to construct dense packings goes back to Litsyn and Tsfasman [20]. They proposed to measure a family of packings by the complexity of a deterministic procedure that describes it, and they showed that packings of Minkowski–Hlawka quality, with density $2^{-(1+o(1))n}$, can be described with complexity $\exp(O(n \log n))$; a graph-theoretic proof of this, together with a gain of a linear factor, was later given by Krivelevich, Litsyn and Vardy [14]. Litsyn and Tsfasman also gave constructive families of packings with density exponent 1.31 and of lattices with exponent 2.30. The known constructive bounds, separated according to whether the construction complexity is polynomial or exponential in the dimension, are collected in the book of Tsfasman and Vlăduţ [30, p. 628]. The effective versions of the Minkowski–Hlawka theorem due to Rush [28], Gaborit and Zémor [9], Moustrou [25] and Gargava and Serban [11] search a structured family of lattices in time $\exp(O(n \log n))$. As Gargava and Serban put it, "currently known polynomial time algorithms produce lattices whose densities are exponentially worse than these bounds" [11].

Classical explicit lattices. The Barnes–Wall, Craig and Mordell–Weil lattices [6, Chapters 1 and 8] are records in many fixed dimensions, but their densities have the form $2^{-n \cdot \omega(1)}$, that is, $E(c) \to \infty$. Root lattices are also asymptotically bad. Multilevel constructions from polynomial-time codes, such as those of Mook and Peikert [23], achieve λ_1^2 of order $n/\log n$, which again gives $c \to 0$.

Global fields. Asymptotically good lattices with explicit algebraic descriptions come from global fields, and most of what is known is due to Tsfasman and his coauthors. Tsfasman's survey [29] describes eight constructions of codes and lattices from number fields and function fields, using either their additive or their multiplicative structure. He stresses that "it is in fact very difficult to construct asymptotically good lattices explicitly [...], and each construction leading to good lattices is of interest". In the additive construction, the ring of integers of a number field in an infinite unramified class field tower is embedded in Euclidean space. Martinet's tower [21] gives exponent $2.2218\ldots$, and the Odlyzko–Serre discriminant bounds

show that this construction can never do better than $1.193\ldots$ (or $1.694\ldots$ under the generalized Riemann hypothesis). Rosenbloom and Tsfasman [27] introduced multiplicative lattices: the lattice of logarithmic embeddings of units, or of divisors of S-units, in a global field. Their function field version was found independently by Quebbemann (see [29]). The best of these are the congruence sublattices of the function field lattices. On a Garcia–Stichtenoth tower over $\mathbb{F}_{47^2}$ they give

$$\gamma(\Lambda_n) \geq (0.0341511\ldots - o(1))\, n, \qquad \Delta(\Lambda_n) \geq 2^{-(1.3888\ldots + o(1))n} \tag{1.1}$$

[29, Theorem 6.2]. To our knowledge (1.1) has been the best bound for a sequence of lattices with an explicit algebraic description. These lattices are canonical: for each curve in the tower the lattice is the group of divisors of the functions that are congruent to 1 modulo a fixed power of one place and whose divisors are supported on a fixed set of rational points. Their minimum is easy to bound, and their covolume is controlled by class numbers. Computing a basis, however, amounts to computing all relations among the classes of the chosen points in the divisor class group of a curve of genus proportional to n, and we do not know a polynomial-time algorithm for that.

Class field towers and unit distances. Class field towers recently played a central role in another problem of discrete geometry. Erdős conjectured that n points in the plane determine at most $n^{1+o(1)}$ pairs at distance one. This conjecture was disproved in 2026. The first construction was found by an internal model at OpenAI, and Sawin [5] then gave sets with more than $n^{1.014}$ unit distances; see Alon, Bloom, Gowers, Litt, Sawin, Shankar, Tsimerman, Wang and Wood [31] for an account. The construction uses CM fields in an infinite Golod–Shafarevich class field tower. In such a tower the degree grows while the root discriminant stays bounded. Through the Minkowski embedding, the ring of integers then stays a well-shaped lattice, much as in the lattice constructions above. Many of its elements have absolute value 1 in every complex embedding, and looking at one complex coordinate turns pairs of lattice points into pairs of points at distance one. Alon et al. point out that these are the same towers that Litsyn and Tsfasman used for lattice packings. In both problems, a bounded root discriminant is what makes the geometry work.

Packings that are not lattices. Concatenating the Rosenbloom–Tsfasman lattices with codes, Xing [34] and Cheng [4] obtained density exponent 1.2653. Their packings are not shown to be lattices, and they use codes on the Gilbert–Varshamov bound, for which only exponential time or randomized constructions are known.

In this language, Theorem A below is a polynomial-time construction of lattices with density exponent $1.30\ldots$, below the exponents of Litsyn–Tsfasman and Rosenbloom–Tsfasman. Theorem B is given by the same kind of explicit algebraic data. Its exponent, $1.2462\ldots$, is smaller than every exponent quoted above, whether for lattices or not. Both remain well above the exponent 1 of the Minkowski–Hlawka bound.

1.3. **Results.**

Theorem A. *There is an explicit sequence of lattices Λ_u, $u \geq 2$, of ranks $n_u \to \infty$, such that*

$$\frac{\gamma(\Lambda_u)}{n_u} \;>\; \frac{1}{26} \quad \textit{for every } u \geq 2, \qquad \textit{and} \qquad \liminf_{u\to\infty} \frac{\gamma(\Lambda_u)}{n_u} \;\geq\; 0.038635588\ldots.$$

A basis of Λ_u can be computed by a deterministic algorithm in time polynomial in n_u.

Theorem B. *There is a sequence of lattices Λ_t, $t \geq 2^{20}$, given by explicit algebraic data, of ranks $n_t \to \infty$, such that*

$$\liminf_{t\to\infty} \frac{\gamma(\Lambda_t)}{n_t} \;\geq\; 0.0416175026437\ldots, \qquad \Delta(\Lambda_t) \;\geq\; 2^{-(1.246238 + o(1))\, n_t}.$$

Theorem A improves (1.1) by 13% in the coefficient and Theorem B by 22%; the density exponents are $E = 1.30\ldots$ and $E = 1.2462\ldots$. In terms of the Minkowski–Hlawka coefficient, the two theorems reach 66% and 71% of $1/(2\pi e)$.

Theorem A is explicit in the sense defined above, and we prove this in Section 4.6. The lattices of Theorem B are built from fixed data by the same kinds of steps, and we explain at the end of Section 5 why the same basis algorithm applies. We have not written out that argument in full detail, so we state Theorem B without the word "explicit".

The first theorem is included because its proof is short and contains all the ideas: one prime of $\mathbb{Z}[i]$, two nested families of codes, and one graph. The second theorem refines the same argument and is the main quantitative result. Both are completely uniform: the parameters are fixed numbers, and the dimension grows through the size of a Ramanujan graph and the height in a tower of function fields. The ranks are astronomically large, since the graph degree is $2^{36} + 1$ in Theorem A and $2^{120} + 1$ in Theorem B; the results are asymptotic.

1.4. **The construction.** The lattices are sublattices of B^M, where B is the Leech lattice and M is the number of edges of a Ramanujan graph. We use two kinds of conditions on $x = (x_e) \in B^M$.

Graph equations. At each vertex of a d-regular bipartite Ramanujan graph [24] we impose a fixed number h of integer linear equations on the vectors attached to the incident edges, with Vandermonde coefficients. A nonzero solution must then be nonzero on at least $h + 1$ edges at every vertex it touches, and the expander mixing lemma shows that it is nonzero on a fixed positive proportion σ of all edges (Lemma 3.1). Since h/d is tiny, these equations cost almost nothing in covolume. The resulting lattice L has minimum of order σM, which is far too small by itself, but which grows linearly in M.

Multilevel congruences. The Leech lattice is a module over the Lipschitz quaternions, so it carries similarities α of squared scale q for $q = 2, 3, 5, 7, 11, 13, 23$, and the residue groups $B/\alpha B$ are vector spaces of dimension 12 over $\mathbb{F}_q$. We identify $(B/\alpha B)^M$ with $\mathbb{F}_{q^{12}}^M$ and impose, digit by digit in the α-adic expansion, that the residues lie in nested algebraic-geometry codes from the Garcia–Stichtenoth tower. This is a multilevel version of Construction D [6, Chapter 8] over a quadratic order. If the first nonzero digit of a vector occurs at level j, the code at that level forces many nonzero components, each of squared length at least 4; the designed distances decrease like q^{-j}, matching the growth of the squared scale, so every level gives the same lower bound $4\delta M$. Riemann–Roch bounds the index, and the near-optimal genus of the tower keeps the cost small.

A vector divisible by all the similarities is handled by the graph: after dividing out a fixed similarity of squared scale D, it lies in L, and $D\sigma M$ exceeds δM once D is a large enough constant. The graph therefore replaces an unbounded number of code levels by a bounded number, and its cost vanishes in the limit.

For Theorem B we use congruences at several primes. Their similarities do not commute, and a code imposed at one prime is not preserved by the similarities used at another. We resolve this by transporting each code through the product of the preceding similarities, which is invertible modulo the relevant prime power (Lemma 5.2). The order of the primes and the number of levels at each are chosen by optimizing an explicit formula, (5.5); no lattice is examined in the process.

1.5. **Limits of the method and a route to the Minkowski–Hlawka bound.** The proofs charge exactly 4, the minimum of the Leech lattice, to each nonzero component at the first nonzero digit. In Section 6 we show that no choice of primes, levels and distances lets an

argument of this kind certify more than $1/(12e\log 2) = 0.0442\ldots$ (Proposition 6.1); Theorem B reaches 94% of this ceiling.

The ceiling is a property of the proof, not of the lattices. Counting the short vectors of B^M suggests that the lattices of Theorem B have a considerably larger minimum than we can prove. More importantly, the architecture separates the problem into a question about codes. If a minimum argument could charge each nonzero component an average of $4\varkappa$ instead of 4, the ceiling would become $\varkappa/(12e\log 2)$, which exceeds the Minkowski–Hlawka coefficient $1/(2\pi e)$ as soon as

$$\varkappa > \frac{6\log 2}{\pi} = 1.3238\ldots.$$

The Leech lattice leaves room for this. Over each nonzero residue modulo a similarity of squared scale 2, only 24 of the 4096 possible next digits give a vector of squared length 4; all others give 6 or 8 (Proposition 6.2). A second digit that avoids these 24 classes gives $\varkappa = 3/2$. What is missing is a weighted distance bound for explicit nested pairs of algebraic-geometry codes coupled by a fixed linear map. Such a bound would give an explicit sequence of lattices exceeding the Minkowski–Hlawka bound by an exponential factor in density. We formulate this precisely in Section 6.3, and we point out why it cannot hold for a typical choice of coupling: the required property must come from algebraic structure, not from averaging. We regard this as a concrete route toward explicit lattices beyond the Minkowski–Hlawka bound, but we do not claim to have carried it out.

1.6. **Organization.** Section 2 collects facts about lattices, the Leech lattice and its quaternionic structure, the Garcia–Stichtenoth tower and Ramanujan graphs. Section 3 constructs the graph lattice. Section 4 proves Theorem A and describes the basis algorithm. Section 5 proves Theorem B. Section 6 proves the ceiling, computes the two-digit weights of the Leech lattice, and discusses the route described above. The finite identities used in the proofs (the action of J and K on the Leech lattice, the similarity relations, and the rational inequalities) are checked by short scripts described in Section 7.

2. Preliminaries

2.1. **Lattices and density.** A lattice $\Lambda \subset \mathbb{R}^N$ of rank n is a discrete subgroup isomorphic to $\mathbb{Z}^n$. Its covolume $\operatorname{covol}(\Lambda)$ is the n-dimensional volume of a fundamental domain in the real span of Λ, so that $\operatorname{covol}(\Lambda)^2$ is the Gram determinant of any basis. We write

$$\lambda_1(\Lambda)^2 = \min_{0\neq x\in\Lambda} \|x\|^2, \qquad \gamma(\Lambda) = \frac{\lambda_1(\Lambda)^2}{\operatorname{covol}(\Lambda)^{2/n}}$$

for the squared minimum and the Hermite invariant. The packing density of the balls of radius $\lambda_1(\Lambda)/2$ centred at the points of Λ is

$$\Delta(\Lambda) = \frac{V_n}{2^n}\,\gamma(\Lambda)^{n/2}, \qquad V_n = \frac{\pi^{n/2}}{\Gamma(n/2+1)}. \tag{2.1}$$

If $\gamma(\Lambda_n) \geq (c - o(1))n$ along a sequence of ranks $n \to \infty$, Stirling's formula turns (2.1) into

$$\Delta(\Lambda_n) \geq 2^{-(E(c)+o(1))n}, \qquad E(c) = 1 - \tfrac{1}{2}\log_2(2\pi e\, c). \tag{2.2}$$

In particular $E(c) = 1$ exactly when $c = 1/(2\pi e)$, the coefficient of the Minkowski–Hlawka theorem.

We use three elementary facts repeatedly.

(1) If $\Lambda' \subseteq \Lambda$ has finite index, then $\operatorname{covol}(\Lambda') = [\Lambda : \Lambda']\operatorname{covol}(\Lambda)$.

(2) If $\Lambda' \subseteq \Lambda$ and $\Lambda'' \subseteq \Lambda$ have finite index, then $[\Lambda : \Lambda' \cap \Lambda''] \le [\Lambda : \Lambda'][\Lambda : \Lambda'']$, and $[L : L \cap \Lambda'] \le [\Lambda : \Lambda']$ for every sublattice $L \subseteq \Lambda$ of full rank.
(3) If $K \subseteq \mathbb{Z}^M$ is the integer kernel of an integer matrix of rank $M-r$, then K is primitive, and $\mathrm{covol}(K)$ equals the covolume of the saturation of the row lattice. Hence, by Hadamard's inequality, $\mathrm{covol}(K)$ is at most the product of the Euclidean lengths of any $M-r$ linearly independent rows.

The third fact is the classical duality between a primitive lattice and its orthogonal complement in $\mathbb{Z}^M$; see for instance [22, Section 1.2].

2.2. **The Leech lattice and its quaternionic structure.** Index coordinates of $\mathbb{R}^{24}$ by the projective line $\Omega = \mathbb{F}_{23} \cup \{\infty\}$. Let $\mathcal{G} \subset \mathbb{F}_2^{\Omega}$ be the extended quadratic residue code of length 24, that is, the binary span of the sets $\{\infty\} \cup (a + R)$, $a \in \mathbb{F}_{23}$, where R is the set of nonzero squares in $\mathbb{F}_{23}$. It is the extended binary Golay code, a self-dual doubly even $[24, 12, 8]$ code [6, Chapter 11]. We use the standard model

$$B = \frac{1}{\sqrt{8}} \left\{ a \in \mathbb{Z}^{\Omega} : \begin{array}{l} a_t \equiv m \pmod 2 \text{ for all } t, \text{ for some } m \in \{0,1\}, \\ ((a_t - m)/2 \bmod 2)_{t \in \Omega} \in \mathcal{G}, \quad \sum_t a_t \equiv 4m \pmod 8 \end{array} \right\} \tag{2.3}$$

of the Leech lattice [6, Chapter 4, Section 11]. It is the even unimodular lattice of rank 24 with no vectors of squared length 2; it has covolume 1 and squared minimum 4, and its theta series is

$$\Theta_B(q) = \sum_{x \in B} q^{\|x\|^2/2} = 1 + 196560\, q^2 + 16773120\, q^3 + 398034000\, q^4 + \cdots . \tag{2.4}$$

Two anticommuting complex structures. The group $\mathrm{SL}_2(\mathbb{F}_{23})$ acts on Ω by fractional linear transformations, and this action lifts to signed permutations of the coordinates. Put $v_t = (t, 1)$ for $t \in \mathbb{F}_{23}$ and $v_\infty = (1, 0)$. For $g \in \mathrm{SL}_2(\mathbb{F}_{23})$ write $g v_t = s_t\, v_{g(t)}$ with $s_t \in \mathbb{F}_{23}^{\times}$, and let χ be the quadratic character of $\mathbb{F}_{23}^{\times}$. The signed permutation matrix

$$\rho(g) e_t = \chi(s_t)\, e_{g(t)}$$

preserves B; this is the classical monomial action of $\mathrm{SL}_2(\mathbb{F}_{23})$ on the Leech lattice [6, Chapter 10]. Fix

$$J = \rho \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad K = \rho \begin{pmatrix} 2 & 8 \\ 8 & -2 \end{pmatrix}. \tag{2.5}$$

Both matrices are orthogonal and map B onto B, and

$$J^2 = K^2 = -I, \qquad JK = -KJ. \tag{2.6}$$

These are identities between explicit 24×24 signed permutation matrices; they follow from multiplication in $\mathrm{SL}_2(\mathbb{F}_{23})$, using that both matrices in (2.5) have order four and anticommute modulo ± 1. The accompanying script checks them, together with $J(B) = K(B) = B$, on a basis of B.

Thus B is a module over the Lipschitz quaternions $\mathbb{Z}\langle J, K\rangle$. For integers a, b, c, d put

$$\alpha = aI + bJ + cK + dJK, \qquad \alpha^* = aI - bJ - cK - dJK.$$

Because J, K and JK are orthogonal, skew-symmetric, square to $-I$ and anticommute in pairs, α^* is the transpose of α and

$$\alpha^* \alpha = \alpha \alpha^* = q\, I, \qquad q = a^2 + b^2 + c^2 + d^2. \tag{2.7}$$

So α is a similarity of squared scale q: $\|\alpha x\|^2 = q \|x\|^2$. It maps B into B, and $[B : \alpha B] = |\det \alpha| = q^{12}$. When $q = p$ is a prime, the relation $p = \alpha \alpha^*$ gives $pB \subseteq \alpha B$, so $B/\alpha B$ is an

$\mathbb{F}_p$-vector space of dimension 12. In this case α satisfies $\alpha^2 - 2a\alpha + p = 0$, the ring $\mathcal{O} = \mathbb{Z}[\alpha]$ is an order in an imaginary quadratic field, and $\mathcal{O}/\alpha\mathcal{O} \cong \mathbb{F}_p$.

We also use the scalar similarity $\alpha = pI$, for which B/pB has dimension 24 over $\mathbb{F}_p$. In every case we identify the residue group $B/\alpha B$ additively with a finite field $\mathbb{F}_{p^l}$ ($l = 12$ or 24) by a fixed choice of basis. Only the additive structure of this identification matters.

2.3. **Algebraic-geometry codes from the Garcia–Stichtenoth tower.** Let s be a prime power. The Garcia–Stichtenoth tower over $\mathbb{F}_{s^2}$ [10] is the sequence of function fields

$$F_1 = \mathbb{F}_{s^2}(x_1), \qquad F_{k+1} = F_k(z_{k+1}), \qquad z_{k+1}^s + z_{k+1} = x_k^{s+1}, \quad x_{k+1} = z_{k+1}/x_k.$$

At height k, every place of F_1 corresponding to $x_1 = a$ with $a \in \mathbb{F}_{s^2}^\times$ splits completely in F_k, and the pole of x_1 is totally ramified. This gives a set of

$$N_s(k) = (s^2 - 1)s^{k-1} \tag{2.8}$$

rational places, together with one further rational place P_∞, and the genus satisfies

$$g_s(k) - 1 \le (s+1)s^{k-1} = \frac{N_s(k)}{s-1} \tag{2.9}$$

[10]; see also [2, Section 3.1] for these two statements in exactly this form.

Let $P_1, \dots, P_M$ be distinct rational places different from P_∞, with $M \le N_s(k)$, and let $0 \le D < M$. The one-point code

$$C = \operatorname{ev} \mathcal{L}(DP_\infty) = \{(f(P_1), \dots, f(P_M)) : \ f \in \mathcal{L}(DP_\infty)\} \subseteq \mathbb{F}_{s^2}^M$$

has minimum Hamming distance at least $M - D$, because a nonzero function with at most D poles has at most D zeros. By Riemann's inequality, $\dim \mathcal{L}(DP_\infty) \ge D + 1 - g$, so C has codimension at most $M - D + g - 1$ in $\mathbb{F}_{s^2}^M$. For $D \le D'$ these codes are nested. We always list the split places in a fixed order (for instance lexicographically in their coordinates), so that each code is determined by (s, k, M, D).

2.4. **Ramanujan graphs.** Let Q be a power of 2 and $k \ge 2$ even. Morgenstern [24, Theorems 5.11–5.13] gives an explicit set of $Q + 1$ generators of $\mathrm{PSL}_2(\mathbb{F}_{Q^k})$ whose Cayley graph is $(Q+1)$-regular, connected and non-bipartite, with all eigenvalues other than $Q + 1$ of absolute value at most $2\sqrt{Q}$. Its bipartite double cover is $(Q+1)$-regular with $N = |\mathrm{PSL}_2(\mathbb{F}_{Q^k})| = Q^{3k} - Q^k$ vertices on each side, and its eigenvalues are $\pm$ those of the Cayley graph. We call a bipartite d-regular graph with N vertices on each side λ-*expanding* if all its eigenvalues other than $\pm d$ have absolute value at most λ. The double cover above is $2\sqrt{Q}$-expanding.

3. Lattices from graph kernels

Both constructions start from the same lattice. Its purpose is to handle vectors that are divisible by a very large similarity, so that only a bounded number of congruence levels is needed. It costs almost nothing in covolume.

3.1. **Moment equations at the vertices.** Let G be a bipartite d-regular graph with N vertices on each side and $m_G = dN$ edges. Let $1 \le h < d$ and let $P \ge d$ be a prime. At each vertex v label the d incident edges by distinct integers $a_v(e) \in \{0, 1, \dots, d-1\}$. For an integer k let $[k]_P$ denote its representative in $(-P/2, P/2]$. The *moment equations* of G are

$$\sum_{e \ni v} [a_v(e)^j]_P \, x_e = 0 \qquad (v \in V(G),\ 0 \le j < h), \tag{3.1}$$

with the convention $a^0 = 1$, so that the equation with $j = 0$ says that the values on the edges at v sum to zero. Let $E' \subseteq E(G)$ be a set of M edges, and let $K \subseteq \mathbb{Z}^{E'}$ be the group of integer vectors on E' which, extended by zero to $E(G)$, satisfy (3.1). Put $r = \operatorname{rank} K$ and $\rho = r/M$.

Lemma 3.1. *Suppose G is λ-expanding with $\lambda < h + 1$. Then*

(1) $\rho \geq 1 - 2hN/M$;

(2) $\operatorname{covol}(K)^{2/r} \leq d^{3(1-\rho)/\rho}$;

(3) every nonzero $x \in K$ has at least σm_G nonzero coordinates, where

$$\sigma = \frac{(h+1)(h+1-\lambda)}{d(d-\lambda)}. \tag{3.2}$$

Proof. (1) There are $2Nh$ equations.

(2) The rows of (3.1), restricted to E', have rank $M - r$. Each row has at most d nonzero entries, each of absolute value less than $P/2$. We may take $P < 2d$ by Bertrand's postulate, so each row has squared length at most d^3. Fact (3) of Section 2 gives $\operatorname{covol}(K)^2 \leq d^{3(M-r)}$, which is the claim.

(3) Fix a vertex v and suppose that the values x_e on the edges at v are not all zero. Any h columns of the $h \times d$ matrix $([a_v(e)^j]_P)$ are linearly independent modulo P, since they form a Vandermonde matrix with distinct nodes in $\mathbb{F}_P$. A nonzero integer solution, divided by the greatest common divisor of its entries, is nonzero modulo P; hence it has at least $h + 1$ nonzero entries.

Call a vertex active if some edge at v carries a nonzero value. Let S_1, S_2 be the active vertices on the two sides, and put $a = |S_1|/N$, $b = |S_2|/N$, $t = \sqrt{ab}$. Since $x \neq 0$, both sets are nonempty. Every edge with a nonzero value joins S_1 to S_2, and each active vertex lies on at least $h + 1$ such edges. Hence the number Z of nonzero coordinates of x satisfies

$$(h+1)N \max(a, b) \leq Z \leq e(S_1, S_2), \tag{3.3}$$

where $e(S_1, S_2)$ is the number of edges between S_1 and S_2. Let A be the $N \times N$ biadjacency matrix. Its largest singular value is d, with both singular vectors equal to the all-ones vector $\mathbf{1}$, and its other singular values are at most λ. Write $\mathbf{1}_{S_1} = a\mathbf{1} + f$ and $\mathbf{1}_{S_2} = b\mathbf{1} + g$ with $f, g \perp \mathbf{1}$. Then

$$e(S_1, S_2) = \mathbf{1}_{S_1}^{\mathsf{T}} A\, \mathbf{1}_{S_2} = dabN + f^{\mathsf{T}} A g \leq dabN + \lambda \|f\| \|g\| = dabN + \lambda N \sqrt{a(1-a)b(1-b)}.$$

Since $\sqrt{(1-a)(1-b)} \leq 1 - t$, we get $e(S_1, S_2) \leq N(dt^2 + \lambda t(1-t))$. Combining with (3.3) and $\max(a, b) \geq t$ gives $h + 1 \leq dt + \lambda(1 - t)$, that is $t \geq (h + 1 - \lambda)/(d - \lambda)$. Then

$$Z \geq (h+1)Nt \geq \frac{(h+1)(h+1-\lambda)}{d-\lambda}\, N = \sigma m_G. \qquad \square$$

3.2. **Putting a Leech vector on every edge.** Let B be the Leech lattice of Section 2.2 and put $A = B^{E'} = B^M$, with the orthogonal sum metric. The lattice

$$L = K \otimes_{\mathbb{Z}} B \subseteq A$$

consists of the vectors $(x_e)_{e \in E'}$, $x_e \in B$, which satisfy the moment equations (3.1) with vector values. Its rank is $n = 24r$, and since $\operatorname{covol}(B) = 1$,

$$\operatorname{covol}(L)^{2/n} = \operatorname{covol}(K)^{2/r} \leq d^{3(1-\rho)/\rho}. \tag{3.4}$$

By (2.3), each component satisfies $\sqrt{8}\, x_e \in \mathbb{Z}^{24}$, and for each of the 24 coordinates the integer vector $(\sqrt{8}\, x_{e,i})_{e \in E'}$ lies in K. Applying Lemma 3.1(3) to a coordinate i in which a nonzero

$x \in L$ has a nonzero entry, we see that at least σm_G of the components x_e are nonzero. Each has squared length at least 4, so

$$\lambda_1(L)^2 \geq 4\sigma m_G. \tag{3.5}$$

Finally, the moment equations have integer coefficients, so they commute with any linear map applied to all components simultaneously. In particular, if β is an injective endomorphism of B applied componentwise, $y \in A$ and $\beta y \in L$, then $y \in L$.

If G is replaced by a disjoint union of C copies of the same graph, the moment equations decouple, K is the direct sum of the kernels of the copies, and Lemma 3.1 and (3.4) hold unchanged, with N and m_G referring to a single copy. Indeed a nonzero vector is nonzero on at least one copy.

The lattice L alone is a poor packing: its minimum is of order m_G/d^2 while its rank is of order m_G. The congruences of the next two sections raise the minimum by a large fixed factor, and the graph kernel is used only for vectors that are divisible by that factor.

4. A simple construction: one Gaussian prime and two code flags

This section proves Theorem A. The construction uses only the complex structure J of the Leech lattice, a single prime of the Gaussian integers, and two nested families of algebraic-geometry codes. It is a multilevel version of Construction D [6, Chapter 8] over $\mathbb{Z}[i]$, intersected with the graph lattice of Section 3.

4.1. **Parameters.** Fix

$$Q = 2^{36}, \qquad d = Q + 1, \qquad h = 2^{20}, \qquad \lambda = 2^{19}, \qquad \delta = \frac{5}{7}.$$

For $u \geq 2$ let G_u be the bipartite double cover of Morgenstern's Cayley graph on $\mathrm{PSL}_2(\mathbb{F}_{Q^{2u}})$ (Section 2.4). It is d-regular and λ-expanding, with $N = Q^{6u} - Q^{2u}$ vertices on each side and $m_G = dN$ edges. Let E' consist of the first

$$M = 4095 \cdot 2^{216u+24} = \tfrac{4095}{4096}\, Q^{6u+1} \tag{4.1}$$

edges in a fixed ordering, and let P be the least prime with $P \geq d$. Then $m_G/M = \frac{4096}{4095}(1 + Q^{-1})(1 - Q^{-4u}) > 1$, and Lemma 3.1(1) gives

$$\rho \;\geq\; 1 - \frac{2hN}{M} \;>\; 1 - \frac{2h}{Q} \cdot \frac{4096}{4095} = \rho_0 := \frac{32759}{32760}. \tag{4.2}$$

Let $L = K \otimes B \subseteq A = B^M$ be the lattice of Section 3, of rank $n = 24r$.

4.2. **The Gaussian structure and the code flags.** By (2.6), J makes B a module over the Gaussian integers $\mathcal{O} = \mathbb{Z}[i]$, with i acting as J. It is torsion free, hence free of rank 12. Put $\varpi = 1 + i$. Then ϖ acts as the similarity $I + J$ of squared scale 2, and $B/\varpi B \cong \mathbb{F}_2^{12}$. Fix an $\mathcal{O}$-basis of B and write $\zeta(x) \in \mathcal{O}^{12M}$ for the coordinates of $x \in A$. Reducing modulo ϖ identifies $A/\varpi A$ with $(\mathbb{F}_2^{12})^M$. We identify $\mathbb{F}_2^{12}$ with $\mathbb{F}_{2^{12}}$, and pairs of consecutive components, $(\mathbb{F}_2^{12})^2$, with $\mathbb{F}_{2^{24}}$.

For $0 \leq j < 36$ put $d_j = \lceil \delta M / 2^j \rceil$. We use two Garcia–Stichtenoth towers (Section 2.3):

- $s = 64$ at height $k_1 = 36u + 5$, so that $\mathbb{F}_{s^2} = \mathbb{F}_{2^{12}}$ and, by (2.8), exactly $N_{64}(k_1) = M$ split places;
- $s = 4096$ at height $k_2 = 18u + 2$, so that $\mathbb{F}_{s^2} = \mathbb{F}_{2^{24}}$ and $N_{4096}(k_2) = \frac{4097}{2048} \cdot \frac{M}{2} \geq \frac{M}{2}$.

Write g_1, g_2 for their genera. By (2.9),

$$g_1 - 1 \le \frac{M}{63}, \qquad g_2 - 1 \le \frac{4097\,M}{4096 \cdot 4095}. \tag{4.3}$$

For $0 \le j < 10$ let $C_j \subseteq \mathbb{F}_{2^{12}}^{M}$ be the one-point code ev $\mathcal{L}((M - d_j)P_\infty)$ on the M split places of the first tower. For $10 \le j < 36$ let $C_j \subseteq \mathbb{F}_{2^{24}}^{M/2}$ be the code ev $\mathcal{L}((M/2 - d_j)P_\infty)$ on the first $M/2$ split places of the second tower, read on pairs of consecutive components. Each C_j is an $\mathbb{F}_2$-subspace of $A/\varpi A$. A nonzero word of C_j has at least d_j nonzero symbols, and every nonzero symbol contains at least one nonzero component of $B/\varpi B$. The codes increase with j within each range, and Section 2.3 bounds their $\mathbb{F}_2$-codimensions r_j by

$$r_j \le 12(d_j + g_1 - 1) \ \ (j < 10), \qquad r_j \le 24(d_j + g_2 - 1) \ \ (10 \le j < 36). \tag{4.4}$$

Choose parity checks compatibly with the nesting. For $j < 10$ choose $\mathbb{F}_2$-linear forms on $A/\varpi A$ whose common kernel is C_j, such that the forms chosen for C_{j+1} are a subset of those chosen for C_j; do the same for $10 \le j < 36$. Lift every form, once and for all, to a $\mathcal{O}$-linear form on $\mathcal{O}^{12M}$ with coefficients in $\{0, 1\}$, and let H_j be the matrix of lifted forms at level j.

4.3. **The lattice and its minimum.** Define

$$\Lambda_u = \{x \in L : \ H_j\,\zeta(x) \equiv 0 \pmod{\varpi^{j+1}} \text{ for } 0 \le j < 36\}. \tag{4.5}$$

It is a subgroup of L containing $\varpi^{36}L$, so it has rank n.

Proposition 4.1. $\lambda_1(\Lambda_u)^2 \ge 4\delta M$.

Proof. Let $0 \ne x \in \Lambda_u$ and let j be the largest integer with $x \in \varpi^j A$, capped at 36.

Suppose $j < 36$, and write $x = \varpi^j y$ with $y \in A \setminus \varpi A$. Then $y \in L$ by the remark at the end of Section 3. The condition at level j reads $\varpi^j H_j\zeta(y) \equiv 0 \pmod{\varpi^{j+1}}$, so $H_j\zeta(y) \equiv 0 \pmod{\varpi}$, which says that the residue of y modulo ϖA lies in C_j. This residue is nonzero, so y has at least d_j nonzero components, each of squared length at least 4. Since ϖ has squared scale 2,

$$\|x\|^2 = 2^j\|y\|^2 \ge 2^j \cdot 4d_j \ge 4\delta M.$$

Suppose $j = 36$, and write $x = \varpi^{36}y$ with $0 \ne y \in L$. Then (3.5) gives $\|x\|^2 = 2^{36}\|y\|^2 \ge 4Q\sigma m_G$. With the parameters above one checks directly that $Q\sigma > 1$, and $m_G > M$, so $\|x\|^2 > 4M > 4\delta M$. □

4.4. **The index.**

Lemma 4.2. $\log_2[L : \Lambda_u] \le \sum_{j=0}^{9} r_j + 11\,r_{10} + \sum_{j=11}^{35} r_j$.

Proof. Consider one lifted form ℓ, and let b be the last level at which it is used. Since the forms are nested, ℓ is used at every level of its range up to b, and the strongest condition it imposes is $\ell(\zeta(x)) \equiv 0 \pmod{\varpi^{b+1}}$. The other conditions on ℓ follow from this one. A single $\mathcal{O}$-linear congruence modulo ϖ^{b+1} has index at most $|\mathcal{O}/\varpi^{b+1}\mathcal{O}| = 2^{b+1}$ in any lattice. Multiplying over the forms, and using fact (2) of Section 2, the exponent of 2 is $\sum_\ell (b_\ell + 1)$. If a range of levels $a_0 \le j \le b_0$ uses $r_{a_0} \ge r_{a_0+1} \ge \cdots$ forms, this sum equals $(a_0 + 1)r_{a_0} + \sum_{a_0 < j \le b_0} r_j$. Applying this with $a_0 = 0$ and $a_0 = 10$ gives the lemma. □

4.5. **The coefficient.** Insert (4.4), (4.3) and $d_j \le \delta M 2^{-j} + 1$ into Lemma 4.2. The result is

$$\log_2[L : \Lambda_u] \le 12M\Big(\delta S + T + \frac{82}{M}\Big), \tag{4.6}$$

where

$$S = \sum_{j=0}^{9} 2^{-j} + \frac{22}{2^{10}} + 2\sum_{j=11}^{35} 2^{-j} = \frac{1035}{512} - 2^{-34}, \qquad T = \frac{10}{63} + \frac{36\cdot 4097}{2048\cdot 4095}.$$

The factor 2 in S and the coefficient 24 in (4.4) come from the pairs of components, and the term $22/2^{10}$ comes from the factor 11 at level 10. The constant $82 = 10 + 2\cdot 36$ accounts for the rounding of the d_j.

Proof of Theorem A. By fact (1) of Section 2, (3.4) and (4.6),

$$\log_2 \operatorname{covol}(\Lambda_u)^{2/n} \le \frac{3(1-\rho)\log_2 d + \delta S + T + 82/M}{\rho}.$$

Exact rational arithmetic gives $\frac{5}{7}S + T + 82/2^{16} < \frac{13}{8}$. Since $M > 2^{16}$, $d < 2^{37}$ and $(1-\rho)/\rho < 1/32759$,

$$\log_2 \operatorname{covol}(\Lambda_u)^{2/n} < \frac{111}{32759} + \frac{13}{8}\cdot\frac{32760}{32759} = \frac{53346}{32759} < \frac{163}{100}.$$

On the other hand Proposition 4.1 gives $\lambda_1(\Lambda_u)^2/n \ge 4\delta M/(24\rho M) \ge 5/42$. Hence

$$\frac{\gamma(\Lambda_u)}{n} \;\ge\; \frac{5}{42}\,2^{-163/100} \;>\; \frac{1}{26},$$

the last inequality being equivalent to $65^{100} > 21^{100}\,2^{163}$.

For the limit, keep the exact budget. With $X = 3\log d + (\delta S + T)\log 2$,

$$\frac{\gamma(\Lambda_u)}{n} \;\ge\; \frac{\delta d^3}{6}\cdot\frac{e^{-X/\rho}}{\rho}\cdot 2^{-82/(\rho M)}.$$

The function $\rho \mapsto \rho^{-1}e^{-X/\rho}$ is increasing on $(0,1]$ because $X > 1$, so we may replace ρ by ρ_0. Letting $u \to \infty$,

$$\liminf_{u\to\infty} \frac{\gamma(\Lambda_u)}{n} \;\ge\; \frac{\delta}{6\rho_0}\,d^{-3(1-\rho_0)/\rho_0}\,2^{-(\delta S+T)/\rho_0} = 0.03863558809\ldots.$$

Finally $n = 24r \ge 24\rho_0 M \to \infty$. □

4.6. **Computing a basis.** The lattice Λ_u is defined by integer linear equations and congruences, so a basis can be computed by integer linear algebra. Write $z \in \mathbb{Z}^{24M}$ for the real and imaginary parts of $\zeta(x)$. Since $\varpi^{36} = -2^{18}$, the condition at level j is equivalent to $\varpi^{35-j}H_j\zeta \equiv 0 \pmod{2^{18}}$, which is a system of integer congruences modulo 2^{18} in z. Together with the moment equations, Λ_u corresponds to

$$\mathcal{Z} = \{z \in \mathbb{Z}^{24M} :\; Rz = 0,\; Cz \equiv 0 \pmod{2^{18}}\}$$

for explicit integer matrices R and C. Let K_0 be a basis of the integer kernel of R, and let $U(CK_0)V = \operatorname{diag}(s_1, \ldots)$ be a Smith normal form with U, V unimodular. Put $f_i = 2^{18}/\gcd(2^{18}, s_i)$, with $f_i = 1$ when $s_i = 0$. Then the columns of $K_0V\operatorname{diag}(f_i)$ form a basis of $\mathcal{Z}$. Indeed, every solution of $Rz = 0$ is $z = K_0Vw$ for a unique integer vector w, and the congruence becomes $s_iw_i \equiv 0$ modulo 2^{18} in each coordinate.

Theorem 4.3. *With the parameters above fixed, a basis of Λ_u can be computed by a deterministic algorithm in time polynomial in n.*

Sketch. The group $\mathrm{PSL}_2(\mathbb{F}_{Q^{2u}})$ has $O(n)$ elements, and $\log n = \Theta(u)$. A defining polynomial of $\mathbb{F}_{Q^{2u}}$ over $\mathbb{F}_Q$ can be found deterministically by testing the $O(Q^{2u}) = O(n^{1/3})$ monic polynomials of degree $2u$ in a fixed order, so the graph and the moment equations are computed in polynomial time. The two towers have $O(n)$ rational places of interest and genus $O(n)$, and the function fields at height k have presentations of size polynomial in $s^k = O(n)$. Bases of the Riemann–Roch spaces can then be computed in polynomial time [12], [8, Appendix B]; factoring over the fixed field $\mathbb{F}_{s^2}$ of characteristic two is deterministic polynomial time by Berlekamp's algorithm. The Hermite and Smith normal forms are computed in polynomial time by [16]. A Euclidean basis is obtained by multiplying by the fixed 24×24 matrix of the Leech basis. □

The parameter u is logarithmic in n, and every constant above is fixed. The ranks are astronomically large; the theorem is asymptotic.

5. The stronger construction: several primes and multilevel flags

This section proves Theorem B. Compared with Section 4 there are three changes. First, congruences are imposed at several primes, using similarities of the Leech lattice of squared scale $2, 3, 5, 7, 11, 13, 23$ and 289; a prime of larger norm buys more squared length per level. Second, each prime carries its own multilevel code flag. Third, the codes at different primes are made compatible by transporting each of them through the similarities of the preceding stages (Lemma 5.2). The minimum is again read off from the first nonzero digit of a vector, now in a mixed radix expansion.

5.1. **Two lemmas on congruence modules.** Let α be one of the similarities of Section 2.2, either $\alpha = aI + bJ + cK + dJK$ of prime squared scale p, or $\alpha = pI$. Put $\mathcal{O} = \mathbb{Z}[\alpha]$; in both cases $\mathcal{O}$ is a domain with $\mathcal{O}/\alpha\mathcal{O} \cong \mathbb{F}_p$. Let $A = B^M$, on which α acts componentwise, and let $m = \dim_{\mathbb{F}_p} A/\alpha A$, which is $12M$ or $24M$.

Lemma 5.1 (Multilevel construction over $\mathcal{O}$)**.** *Let $R \geq 1$ and let $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_{R-1}$ be $\mathbb{F}_p$-subspaces of $A/\alpha A$. There is an $\mathcal{O}$-submodule $\Gamma \subseteq A$ with $\alpha^R A \subseteq \Gamma$ such that*

$$[A : \Gamma] = p^{\sum_{j<R}(m - \dim C_j)} \quad \text{and} \quad \{\, y \bmod \alpha A : \ y \in A,\ \alpha^j y \in \Gamma \,\} = C_j \quad (0 \leq j < R). \tag{5.1}$$

Proof. Choose an $\mathbb{F}_p$-basis $\bar{e}_1, \ldots, \bar{e}_m$ of $A/\alpha A$ adapted to the flag, and let a_i be the least j with $\bar{e}_i \in C_j$, or $a_i = R$ if there is none. Choose lifts $e_i \in A$ and put

$$\Gamma = \alpha^R A + \sum_{i=1}^{m} \mathcal{O}\, \alpha^{a_i} e_i.$$

The map $\phi : (\mathcal{O}/\alpha^R\mathcal{O})^m \to A/\alpha^R A$, $(c_i) \mapsto \sum c_i e_i$, is surjective: reduce an element modulo α, subtract the corresponding combination of the e_i, divide by α, and repeat. Both sides have p^{Rm} elements, since $|\mathcal{O}/\alpha\mathcal{O}| = p$ and $[A : \alpha A] = p^m$, so ϕ is an isomorphism. It maps $\bigoplus_i \alpha^{a_i}\mathcal{O}/\alpha^R\mathcal{O}$ onto $\Gamma/\alpha^R A$, so $[A : \Gamma] = p^{\sum_i a_i}$. Since $\#\{i : a_i > j\} = m - \dim C_j$, this is the first claim. For the second, write $y \equiv \sum c_i e_i$ modulo $\alpha^R A$. Then $\alpha^j y \in \Gamma$ if and only if $\alpha^j c_i \in \alpha^{a_i}\mathcal{O} + \alpha^R\mathcal{O}$ for all i. For $a_i \leq j$ this always holds. For $a_i > j$ it holds if and only if $c_i \in \alpha^{a_i - j}\mathcal{O} + \alpha^{R-j}\mathcal{O}$, because $\mathcal{O}$ is a domain, and in particular it forces $c_i \in \alpha\mathcal{O}$. Hence the residue of y lies in the span of the $\bar{e}_i$ with $a_i \leq j$, which is C_j. Conversely every element of C_j is the residue of some $y = \sum_{a_i \leq j} c_i e_i$, and for such y we have $\alpha^j y \in \Gamma$. □

The module Γ is the multilevel Construction D of the flag over the ring $\mathcal{O}$; compare [6, Chapter 8, Section 8] for the case $\mathcal{O} = \mathbb{Z}$.

Lemma 5.2 (Transport)**.** *Let $\Gamma \subseteq A$ be a subgroup with $p^e A \subseteq \Gamma$, and let β be an endomorphism of A whose determinant is prime to p. Put $\widehat{\Gamma} = \beta\Gamma + p^e A$. Then $[A : \widehat{\Gamma}] = [A : \Gamma]$, and for $y \in A$ we have $\beta y \in \widehat{\Gamma}$ if and only if $y \in \Gamma$.*

Proof. The map β induces an automorphism of A/p^eA, and $\widehat{\Gamma}/p^eA$ is the image of Γ/p^eA. This gives the index. If $\beta y = \beta\gamma + p^e z$ with $\gamma \in \Gamma$, then $\beta(y-\gamma) \in p^eA$, so $y - \gamma \in p^eA \subseteq \Gamma$. The converse is clear. □

5.2. **The stages.** The construction uses the following eight similarities, in this order. In the table, q_s is the squared scale of α_s, p_s the prime with q_s a power of p_s, R_s the number of levels at that stage, $l_s = \dim_{\mathbb{F}_{p_s}} B/\alpha_s B$, and $D_s = \prod_{i<s} q_i^{R_i}$.

s	α_s	p_s	q_s	R_s	l_s	D_s
1	$J + K$	2	2	4	12	1
2	$I + J + K$	3	3	2	12	16
3	$2I + J$	5	5	2	12	144
4	$2I + J + K + JK$	7	7	1	12	3600
5	$3I + J + K$	11	11	1	12	25200
6	$3I + 2J$	13	13	1	12	277200
7	$3I + 3J + 2K + JK$	23	23	1	12	3603600
8	$17I$	17	289	85	24	82882800

By (2.7) each α_s is a similarity of squared scale q_s mapping B into B. The eight primes p_s are distinct. In every row $p_s^{l_s} = q_s^{12}$, and we identify $B/\alpha_s B$ additively with $\mathbb{F}_{q_s^{12}}$. Put

$$\beta_s = \alpha_1^{R_1}\alpha_2^{R_2}\cdots\alpha_{s-1}^{R_{s-1}}, \qquad \beta_{\mathrm{end}} = \beta_9, \qquad D = \prod_{s=1}^{8} q_s^{R_s} = 82882800 \cdot 289^{85}.$$

So β_s is a similarity of squared scale D_s, and $\det \beta_s$ is a power of D_s, hence prime to p_s. The similarities do not commute in general, which is why the order matters and why transport is needed.

5.3. **Graph and code lengths.** Fix

$$Q = 2^{120}, \quad d = Q + 1, \quad h = 2^{62}, \quad \lambda = 2^{61},$$
$$\kappa = \frac{4095}{4096}, \quad C = \Big\lfloor \frac{\kappa Q^6}{d} \Big\rfloor, \quad \tau = \frac{Cd}{Q^6}, \quad \delta = \frac{711612}{10^6}.$$

For each odd squared scale $q \in \{3, 5, 7, 11, 13, 23, 289\}$ put $\theta_q = \log Q / \log q$, which is irrational. For an integer $t \geq 2^{20}$ let $v = v(t)$ be the least integer $v \geq t$ such that $\|v\theta_q\|_{\mathbb{R}/\mathbb{Z}} < 1/t$ for all seven values of q. It exists by Dirichlet's simultaneous approximation theorem, and it can be found by integer comparisons: for m_q the integer nearest to $v\theta_q$, the condition reads $q^{tm_q - 1} < Q^{vt} < q^{tm_q + 1}$. Put $m_2 = 120v$, so that $2^{m_2} = Q^v$.

Let G be the disjoint union of C copies of the bipartite double cover of Morgenstern's Cayley graph on $\mathrm{PSL}_2(\mathbb{F}_{Q^{2(v-1)}})$ (Section 2.4). A single copy is d-regular and λ-expanding, with $N = Q^{6(v-1)} - Q^{2(v-1)}$ vertices on each side and $m_G = dN$ edges. Use all $M = Cm_G$ edges. With $X = Q^{6v}$ this gives

$$M = \tau X\big(1 - Q^{-4(v-1)}\big) < \kappa X, \tag{5.2}$$

and Lemma 3.1(1) gives $\rho \geq \rho_0 := 1 - 2h/d$. Let P be the least prime $\geq d$ and let $L \subseteq A = B^M$ be the lattice of Section 3, of rank $n = 24r$.

For each squared scale q in the table use the Garcia–Stichtenoth tower over $\mathbb{F}_{s^2}$ with $s = q^6$, at height $m_q - 1$. By (2.8) it has

$$N_q = (1 - q^{-12})\, q^{6m_q}$$

split places. For $q = 2$ this is κX. For odd q, the choice of v gives $q^{6m_q} \geq X q^{-6/t}$, and since $6 \log q < 42$, $N_q/X \geq (1 - 3^{-12})(1 - 42/t) > \kappa$. So in all cases $N_q > M$ by (5.2). By (2.9) and (5.2), the genus g_q satisfies

$$\limsup_{t \to \infty} \frac{g_q - 1}{M} \leq \eta_q := \frac{1 - q^{-12}}{\tau\,(q^6 - 1)}. \tag{5.3}$$

5.4. **The lattice.** At stage s and level $0 \leq j < R_s$ put

$$d_{s,j} = \Big\lceil \frac{\delta M}{D_s q_s^j} \Big\rceil, \qquad C_{s,j} = \mathrm{ev}\ \mathcal{L}\big((M - d_{s,j})P_\infty\big) \subseteq \mathbb{F}_{q_s^{12}}^M,$$

evaluated at the first M split places of the tower for q_s. These codes increase with j, have minimum distance at least $d_{s,j}$, and have $\mathbb{F}_{p_s}$-codimension at most $l_s(d_{s,j} + g_{q_s} - 1)$ in $A/\alpha_s A$. Let Γ_s be the module given by Lemma 5.1 for $\alpha = \alpha_s$, $R = R_s$ and the flag $(C_{s,j})_{j<R_s}$, and put

$$\widehat{\Gamma}_s = \beta_s \Gamma_s + p_s^{R_s} A, \qquad \Lambda_t = L \cap \bigcap_{s=1}^{8} \widehat{\Gamma}_s.$$

Lemma 5.2 applies with $e = R_s$, since $p_s^{R_s} A = \alpha_s^{R_s} (\alpha_s^*)^{R_s} A \subseteq \alpha_s^{R_s} A \subseteq \Gamma_s$ (for the last stage $\alpha_s^* = 1$ in this formula).

The lattice Λ_t has rank n. Indeed β_{end} maps L into L, and for each s it maps A into $\beta_s \alpha_s^{R_s} A \subseteq \beta_s \Gamma_s$.

5.5. **The minimum.**

Proposition 5.3. *$\lambda_1(\Lambda_t)^2 \geq 4\delta M$.*

Proof. Let $0 \neq x \in \Lambda_t$. Let s be the least index such that $x \notin \beta_{s+1} A$, or $s = 9$ if $x \in \beta_9 A = \beta_{\mathrm{end}} A$.

Suppose $s \leq 8$. Then $x = \beta_s w$ with $w \in A \setminus \alpha_s^{R_s} A$. Let $j < R_s$ be maximal with $w \in \alpha_s^j A$ and write $w = \alpha_s^j y$, so that $y \notin \alpha_s A$. Since $x \in \widehat{\Gamma}_s$, Lemma 5.2 gives $\alpha_s^j y \in \Gamma_s$, and Lemma 5.1 puts the nonzero residue of y modulo $\alpha_s A$ in $C_{s,j}$. So at least $d_{s,j}$ components of y are nonzero, and

$$\|x\|^2 = D_s q_s^j \|y\|^2 \geq 4 D_s q_s^j d_{s,j} \geq 4\delta M.$$

Suppose $s = 9$, so $x = \beta_{\mathrm{end}} y$ with $0 \neq y \in A$. Since β_{end} acts componentwise and is injective, $y \in L$. By (3.5), $\|x\|^2 = D\|y\|^2 \geq 4D\sigma m_G$. The fixed integers satisfy $D\sigma > \delta C$ (in fact $D\sigma/(\delta C) > 25$), so $\|x\|^2 > 4\delta C m_G = 4\delta M$. □

The last case is the only place where the graph enters. With 84 levels at the last stage instead of 85, the inequality $D\sigma > \delta C$ fails.

5.6. **The index and the coefficient.** By fact (2) of Section 2, Lemma 5.2 and Lemma 5.1,

$$[L : \Lambda_t] \le \prod_{s=1}^{8} [A : \Gamma_s] \le \prod_{s=1}^{8} q_s^{\,12\sum_{j<R_s}(d_{s,j}+g_{q_s}-1)}. \tag{5.4}$$

Define

$$A_0 = \sum_{s=1}^{8} \frac{\log q_s}{D_s} \sum_{j=0}^{R_s-1} q_s^{-j}, \qquad B_0 = \sum_{s=1}^{8} R_s\, \eta_{q_s} \log q_s.$$

Proof of Theorem B. Since $n = 24\rho M$, Proposition 5.3 gives $\lambda_1(\Lambda_t)^2/n \ge \delta/(6\rho)$. By (3.4), (5.4) and (5.3), and since the rounding in $d_{s,j}$ costs a bounded number of symbols,

$$\log \operatorname{covol}(\Lambda_t)^{2/n} \le \frac{3(1-\rho)\log d + \delta A_0 + B_0 + o(1)}{\rho} \qquad (t \to \infty).$$

As in the proof of Theorem A, the function $\rho \mapsto \rho^{-1}e^{-X/\rho}$ with $X = 3\log d + \delta A_0 + B_0 > 1$ is increasing, so we may replace ρ by ρ_0. Hence

$$\liminf_{t\to\infty} \frac{\gamma(\Lambda_t)}{n} \;\ge\; c_B := \frac{\delta}{6} \exp\Big(-\frac{\delta A_0 + B_0 + 3(1-\rho_0)\log d}{\rho_0}\Big). \tag{5.5}$$

Here $A_0 = 1.40525984714916\ldots$ and $B_0 = 0.04725276406630\ldots$, and interval arithmetic with rational endpoints gives $0.041617502643793227 \le c_B \le 0.041617502643793228$. The density bound follows from (2.2): $E(c_B) = 1.2462373\ldots$. □

5.7. **Remarks on the choices.** The coefficient (5.5) is explicit in the stage table, and the table was chosen by comparing this formula across tables; no lattice was examined. A level of squared scale q placed after squared scale U adds $\log q\,(\delta/U + \eta_q)$ to the exponent in (5.5). The first term pays for the designed distance and the second for the genus of the tower. Early levels need a large distance, so cheap squared scales 2 and 3 are used there; after the squared scale has grown, the distance term is small and the genus term dominates, which favours primes with small η_q, that is, large residue fields. The final stage at 17 has negligible cost and exists only to make the graph case of Proposition 5.3 work.

The basis algorithm of Section 4.6 applies with the obvious changes: the congruences at stage s become integer congruences modulo $p_s^{R_s}$ after writing β_s and the lifts in integer coordinates, and the eight moduli are combined by the Chinese remainder theorem. The choice of $v(t)$ costs time polynomial in $t = O(\log n)$.

6. Limits of the method and a route beyond them

6.1. **A ceiling for counting nonzero components.** The minimum bounds of Propositions 4.1 and 5.3 use one piece of information about a vector: at its first nonzero digit, the code forces many nonzero components, and each is charged the minimum 4 of the Leech lattice. The next proposition shows that no choice of primes, depths and distances can push this argument far beyond Theorem B.

Consider the construction of Section 5 with an arbitrary finite sequence of levels, the i-th level having integer squared scale $q_i \ge 2$, and write $U_i = q_1 \cdots q_{i-1}$ and $D = q_1 \cdots q_k$. The certified coefficient then has the form (5.5), with $A_0 = \sum_i \log q_i/U_i$ and some $B_0 \ge 0$.

Proposition 6.1. *For every such sequence, $A_0 \ge 2\log 2\,(1-1/D)$. Consequently the right-hand side of* (5.5) *is at most*

$$\frac{1}{12e\log 2\,(1-1/D)} \qquad \textit{and} \qquad \frac{1}{12e\log 2} = 0.0442281\ldots$$

is an upper bound for every certificate of this kind in which D is large.

Proof. The function $f(q) = \log q - 2\log 2\,(1 - 1/q)$ vanishes at $q = 2$ and has derivative $(q - 2\log 2)/q^2 > 0$ for $q \geq 2$, so $\log q_i \geq 2\log 2\,(1 - 1/q_i)$. Hence

$$A_0 = \sum_i \frac{\log q_i}{U_i} \geq 2\log 2 \sum_i \Big(\frac{1}{U_i} - \frac{1}{U_{i+1}}\Big) = 2\log 2\Big(1 - \frac{1}{D}\Big).$$

Since $B_0 \geq 0$ and $\rho_0 \leq 1$, the right-hand side of (5.5) is at most $(\delta/6)e^{-\delta A_0} \leq 1/(6eA_0)$. □

In the graph construction, D must exceed $\delta C/\sigma$, which is enormous, so the ceiling applies. Theorem B reaches 94.1% of it. The remaining gap consists of the genus term B_0, which the Drinfeld–Vlăduţ bound [7] prevents from being much smaller at squared scale 2, and the steps of squared scale larger than 2.

6.2. **Two-digit weights in the Leech lattice.** To go further, a proof must charge some nonzero components more than 4. The Leech lattice offers room for this, as the following exact count shows. Let $H = J + K$, so that $H^2 = -2I$ and $HB \supseteq 2B$.

Proposition 6.2. *(1) Every nonzero class of B/HB contains exactly* 48 *vectors of squared length* 4*, and no shorter vectors.*

(2) The minimal squared lengths of the classes of $B/2B$ are distributed as follows: 0 *once,* 4 *for* 98280 *classes,* 6 *for* 8386560 *classes and* 8 *for* 8292375 *classes.*

(3) Fix a nonzero class $a \in B/HB$. Of the 4096 *classes of $B/2B$ lying over a, exactly* 24 *have minimal squared length* 4*, exactly* 2048 *have* 6*, and exactly* 2024 *have* 8*.*

Proof. (1) Since $\lambda_1(HB)^2 = 8$, two distinct vectors of squared length 4 in the same class of B/HB differ by a vector of squared length at least 8, so their inner product is at most 0. A family of nonzero vectors with pairwise nonpositive inner products in $\mathbb{R}^{24}$ has at most 48 members. No such vector lies in HB, and $196560 = 48(2^{12} - 1)$ by (2.4), so each of the 4095 nonzero classes contains exactly 48 of them.

(2) If $x \equiv y \pmod{2B}$ and $x \neq \pm y$, then $(x \pm y)/2$ are nonzero vectors of B, and $\|(x + y)/2\|^2 + \|(x - y)/2\|^2 = (\|x\|^2 + \|y\|^2)/2 \geq 8$. Hence a class containing a vector of squared length 4 or 6 contains exactly one opposite pair of vectors of squared length at most 7, and no vector of squared length 8 shares a class with one of length 4 or 6. By (2.4) this gives 98280 and 8386560 classes of minimal length 4 and 6. Two vectors of squared length 8 in one class differ by an element of $2B$, of squared length at least 16, so their inner product is at most 0, and a class contains at most 48 of them. There are $2^{24} - 1 - 98280 - 8386560 = 8292375$ remaining nonzero classes and $398034000 = 48 \cdot 8292375$ vectors of squared length 8, so each remaining class contains exactly 48, and none shorter.

(3) Because B is even and unimodular, $\mathsf{q}(x) = \|x\|^2/2 \bmod 2$ is a nondegenerate quadratic form on $B/2B$ with polar form $\langle x, y\rangle \bmod 2$. The subspace $HB/2B$ has dimension 12, and $\mathsf{q}(Hy) = \|y\|^2 \equiv 0$, so it is a maximal totally singular subspace and equals its own orthogonal. On the coset $a + HB/2B$ with $a \notin HB$, $\mathsf{q}(a + w) = \mathsf{q}(a) + \langle a, w\rangle$, and $w \mapsto \langle a, w\rangle$ is a nonzero linear form; so q takes the value 1 exactly 2048 times. Classes of minimal length 6 have $\mathsf{q} = 1$, and classes of minimal length 4 or 8 have $\mathsf{q} = 0$. By (1) and (2), the 48 vectors of length 4 over a give exactly 24 classes modulo $2B$. The remaining 2024 classes have minimal length 8. □

Thus a single digit at squared scale 2 always costs exactly 4 per nonzero component, but two consecutive digits cost at least 6 per nonzero component unless the second digit falls in one of 24 out of 4096 prescribed classes.

6.3. **A route beyond the Minkowski–Hlawka bound.** Suppose that a minimum argument for the same kind of lattice could charge every nonzero component at the first nonzero digit an average of $4\varkappa$ instead of 4. The designed distances could then be divided by $\varkappa$, the distance term δA_0 in (5.5) would become $\delta A_0/\varkappa$, and the proof of Proposition 6.1 would give the ceiling $\varkappa/(12e\log 2)$. This exceeds $1/(2\pi e)$ exactly when

$$\varkappa > \varkappa^* = \frac{6\log 2}{\pi} = 1.3238\ldots.$$

Proposition 6.2 shows that the local room exists: at the binary stage, a second digit that avoids the 24 cheap classes over every nonzero first digit gives $\varkappa = 3/2$. What is missing is a global statement, a weighted distance bound for explicit pairs of nested codes in which the second code is coupled to the first by a fixed linear map. Such a statement would yield an explicit sequence of lattices with $\gamma(\Lambda_n) \geq (c - o(1))n$ for some $c > 1/(2\pi e)$, that is, with density exponentially larger than 2^{-n} by (2.2).

We stress two points. First, nothing in this section is proved beyond Propositions 6.1 and 6.2; the coefficients proved in this paper are 66% and 71% of $1/(2\pi e)$. Second, the required property cannot come from averaging. A first-moment count of the vectors of B^M shows that a sublattice of B^M of given index whose short vectors are distributed like those of a random coset has coefficient at most $1/(2\pi e)$; this is the Minkowski–Hlawka bound in another guise. Exceeding it requires codes and couplings whose algebraic structure prevents short vectors more efficiently than chance does, in the way that the Leech lattice itself does in dimension 24. The constructions of this paper isolate that requirement as a problem about weighted distances of explicit algebraic-geometry codes.

7. Verification of the finite computations

The proofs use a small number of finite identities, which can be checked by hand with some patience and which we have checked by computer with exact arithmetic.

(1) The matrices J and K of (2.5) map a basis of the Leech lattice (2.3) into the lattice and satisfy (2.6); each of the eight similarities of Section 5 satisfies (2.7) with the stated q and has determinant q^{12}.
(2) The inequality $Q\sigma > 1$ of Section 4, the bound $\frac{5}{7}S + T + 82/2^{16} < \frac{13}{8}$, and $65^{100} > 21^{100}2^{163}$.
(3) The inequality $D\sigma > \delta C$ of Section 5 and its failure with 84 levels at the last stage, and rational enclosures of A_0, B_0 and c_B.
(4) The arithmetic in the proof of Proposition 6.2.

No step of the construction or of the proofs involves computing a lattice minimum or selecting a lattice by its minimum.

References

[1] K. Ball, *A lower bound for the optimal density of lattice packings*, Int. Math. Res. Not. **1992**, no. 10, 217–221.
[2] S. Ballet and R. Rolland, *Families of curves over any finite field with a class number greater than the Lachaud–Martin-Deschamps bounds*, arXiv:0906.5432.
[3] M. Campos, M. Jenssen, M. Michelen and J. Sahasrabudhe, *A new lower bound for sphere packing*, arXiv:2312.10026.
[4] S. Cheng, *Improvement on asymptotic density of packing families derived from multiplicative lattices*, Finite Fields Appl. **36** (2015), 133–150.
[5] W. Sawin, *An explicit lower bound for the unit distance problem*, arXiv:2605.20579.

[6] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 3rd ed., Springer, New York, 1999.
[7] V. G. Drinfeld and S. G. Vlăduţ, *Number of points of an algebraic curve*, Funct. Anal. Appl. **17** (1983), 53–54.
[8] K. Eisenträger and S. Hallgren, *Computing the unit group, class group, and compact representations in algebraic function fields*, in: ANTS X, Open Book Series **1** (2013), 335–358.
[9] P. Gaborit and G. Zémor, *On the construction of dense lattices with a given automorphisms group*, Ann. Inst. Fourier **57** (2007), 1051–1062.
[10] A. Garcia and H. Stichtenoth, *A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound*, Invent. Math. **121** (1995), 211–222.
[11] N. Gargava and V. Serban, *Dense packings via lifts of codes to division rings*, arXiv:2111.03684.
[12] F. Hess, *Computing Riemann–Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), 425–445.
[13] E. Hlawka, *Zur Geometrie der Zahlen*, Math. Z. **49** (1943), 285–312.
[14] M. Krivelevich, S. Litsyn and A. Vardy, *A lower bound on the density of sphere packings via graph theory*, arXiv:math/0402132.
[15] G. A. Kabatiansky and V. I. Levenshtein, *Bounds for packings on a sphere and in space*, Probl. Inf. Transm. **14** (1978), 1–17.
[16] R. Kannan and A. Bachem, *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*, SIAM J. Comput. **8** (1979), 499–507.
[17] B. Klartag, *Lattice packing of spheres in high dimensions using a stochastically evolving ellipsoid*, Invent. Math. (2026); arXiv:2504.05042.
[18] E. B. Abuya, N. Gargava and Y. Zhao, *Stochastically evolving ellipsoids with symmetries*, arXiv:2606.05105.
[19] N. Gargava, M. Gröbner and M. Simkin, *A cyclotomic gluing construction for lattice sphere packings*, arXiv:2610.12619.
[20] S. N. Litsyn and M. A. Tsfasman, *Constructive high-dimensional sphere packings*, Duke Math. J. **54** (1987), 147–161.
[21] J. Martinet, *Tours de corps de classes et estimations de discriminants*, Invent. Math. **44** (1978), 65–73.
[22] J. Martinet, *Perfect lattices in Euclidean spaces*, Springer, Berlin, 2003.
[23] E. Mook and C. Peikert, *Lattice (list) decoding near Minkowski's inequality*, IEEE Trans. Inform. Theory **68** (2022); arXiv:2010.04809.
[24] M. Morgenstern, *Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q*, J. Combin. Theory Ser. B **62** (1994), 44–62.
[25] P. Moustrou, *On the density of cyclotomic lattices constructed from codes*, Int. J. Number Theory **13** (2017); arXiv:1603.00743.
[26] C. A. Rogers, *Existence theorems in the geometry of numbers*, Ann. of Math. **48** (1947), 994–1002.
[27] M. Yu. Rosenbloom and M. A. Tsfasman, *Multiplicative lattices in global fields*, Invent. Math. **101** (1990), 687–696.
[28] J. A. Rush, *A lower bound on packing density*, Invent. Math. **98** (1989), 499–509.
[29] M. A. Tsfasman, *Global fields, codes and sphere packings*, Astérisque **198–200** (1991), 373–396.
[30] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*, Kluwer, Dordrecht, 1991.
[31] N. Alon, T. F. Bloom, W. T. Gowers, D. Litt, W. Sawin, A. Shankar, J. Tsimerman, V. Wang and M. M. Wood, *Remarks on the disproof of the unit distance conjecture*, arXiv:2605.20695.
[32] S. Vance, *Improved sphere packing lower bounds from Hurwitz lattices*, Adv. Math. **227** (2011), 2144–2156.
[33] A. Venkatesh, *A note on sphere packings in high dimension*, Int. Math. Res. Not. **2013**, no. 7, 1628–1642.
[34] C. Xing, *Dense packings from quadratic fields and codes*, J. Combin. Theory Ser. A **115** (2008), 1021–1035.