On the Extremality of an 80-Dimensional Lattice

Damien Stehlé[1,2] and Mark Watkins[2]

[1] CNRS and Macquarie University.
[2] Magma Computer Algebra Group, School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia.
damien.stehle@gmail.com, watkins@maths.usyd.edu.au

Abstract. We show that a specific even unimodular lattice of dimension 80, first investigated by Schulze-Pillot and others, is extremal (i.e., the minimal nonzero norm is 8). This is the third known extremal lattice in this dimension. The known part of its automorphism group is isomorphic to $\mathbf{SL}_2(\mathbf{F}_{79})$, which is smaller (in cardinality) than the two previous examples. The technique to show extremality involves using the positivity of the Θ-series, along with fast vector enumeration techniques including pruning, while also using the automorphisms of the lattice.

1 Introduction

We show that a specific 80-dimensional even unimodular lattice is extremal, that is, that it has no (nonzero) vectors of norm less than 8. It follows that the kissing number of this lattice is 1 250 172 000.[1] Although two other even unimodular extremal lattices in dimension 80 are known [3], the one we describe has a construction related to coding theory, and has an automorphism group that contains $\mathbf{SL}_2(\mathbf{F}_{79})$.

In Section 2 we recall some facts and results about extremal lattices.

In Section 3 we follow the method of Schulze-Pillot [40] to construct our lattice $\mathbf{N}_{80}$ as a 2-neighbour of a lattice derived from a length 80 extended quadratic residue code over $\mathbf{F}_{19}$. The prime 19 here is not overly significant; the construction produces five unimodular lattices in correspondence with the class group of $\mathbf{Q}(\sqrt{-79})$, and the ideal class that yields $\mathbf{N}_{80}$ (the only extremal one among the five) has an ideal of norm 19 in it.[2] Alternatively, a variation (see [1]) on a method of Gross [18, §11] can be used to construct $\mathbf{N}_{80}$, and deals more directly with the ideals of this imaginary quadratic field. Via either method, it is fairly immediate that $\mathbf{N}_{80}$ has an automorphism group that contains $\mathbf{SL}_2(\mathbf{F}_{79})$.

In Section 4 we note that various choices of bases make the group action nice (doubly transitive as signed permutations on the coordinates), and then make a specific basis choice that relates directly to the construction in [1].

[1] We do not describe herein any features of these minimal vectors. In fact, the 2 555 orbits of these vectors under the known automorphisms were first found (without proof of completeness) by the authors of [1], with whom we started this project.

[2] We could also have chosen $l = 5$ (as indicated in [40, Example 3]), but for technical reasons (in lattice generation) wanted l not to be too small.

In Section 5 we first briefly outline our method of proof that the lattice $\mathbf{N}_{80}$ is extremal. We need to show that $\mathbf{N}_{80}$ has no nonzero vectors of norm 6 or smaller. We can almost immediately eliminate vectors of norm 2, while a slightly more involved argument is necessary to show there are no vectors of norm 4. We then use the nonnegativity of the coefficients of the Θ-series of the lattice to reduce the problem of showing that there is no vector of norm 6 to the problem of finding (almost) all the vectors of norm 10. The latter is feasible due to the fact that we need only find one representative in each orbit class under the known automorphisms, whereas the more direct method of an exhaustive search for norm 6 vectors would be significantly more time-consuming. After first cataloguing the norm 10 orbits that have a nontrivial stabiliser, all the other vectors will have a full orbit under the known automorphisms, and so we can reduce the problem by a factor of approximately $\#\mathbf{SL}_2(\mathbf{F}_{79}) = 492\,960$. This leaves us with only 15.3 million orbits of norm 10 to find.

In Section 6 we describe our method to find all the norm 10 orbits. One principal idea is to prune the tree corresponding to the Kannan-Fincke-Pohst enumeration algorithm that finds all short lattice vectors [21,12]. Our tree pruning strategy, which generalizes that of [38, §7] and improves the one from [39], considers a truncated search domain that is much smaller but still finds a significant proportion of the desired vectors. Note that the pruning strategy we describe and its analysis have been independently discovered by Gama, Nguyen, and Regev [15, §4]. In our case, we need only find one vector in each orbit class, so the fact we miss some vectors when searching is unimportant. Another idea to speed the search is to periodically apply a random perturbation to the basis and re-apply lattice reduction (namely LLL with deep insertions [38]), before again searching with tree pruning. As our lattices are of quite high dimension, the new basis is very likely to be different than the previous ones. This can help in two ways: firstly, searching with a given lattice basis for short vectors, even with pruning available, tends to become less cost-effective over time, in terms of the number of vectors found per second; and secondly, and rather surprisingly to us, a "good basis" for searching can sometimes have many orbit classes which will not show up until quite deep in the search. We still do not understand this latter phenomenon, but it is easily overcome via the random perturbations.

Section 7 gives our results and verification methods, plus related questions.

Computations. All timings are given for 2.3Ghz Opteron 8356 processors. If otherwise unspecified, only one processor is used.

2 Extremal lattices

The extremality of a lattice is typically defined using Θ-series, as for instance in [7, §7.4].[3] In particular, an extremal unimodular even lattice in dimension d with $8|d$ has a minimum nonzero vector norm of $2(1+\lfloor d/24 \rfloor)$, as this is twice the

[3] The precise notion of "extremal" seems to vary over time; for instance [6] is more demanding, asking that the minimum be at least $1 + \lfloor d/8 \rfloor$.

dimension of the associated space of modular forms. For odd lattices, shadow theory is typically used to obtain satisfactory bounds [8]. A relatively recent survey on extremality appears in [14].

In particular, there were already two extremal even unimodular lattices known in dimension 80, both due to Bachoc and Nebe [3] via a coding theory construction. The first lattice $\mathbf{L}_{80}$ has an automorphism group $2.A_7 \otimes_{\sqrt{-7}} 2.M_{22}.2$ of size $2^{12}\,3^4\,5^2\,7^2\,11 = 4\,470\,681\,600$, and this group is known to be a maximal finite subgroup of $\mathbf{GL}_{80}(\mathbf{Z})$ (see [3, Theorem 3.2]). The second extremal lattice $\mathbf{M}_{80}$ has known automorphisms [3, Lemma 4.11] of order $2^{12}3^45^2 = 8\,294\,400$. For comparison, the number of known automorphisms of our lattice is 492 960.

Our lattice $\mathbf{N}_{80}$ is isometric neither to $\mathbf{L}_{80}$ nor $\mathbf{M}_{80}$. The argument for $\mathbf{L}_{80}$ is immediate, as its automorphism group is known to be maximal but 79 does not divide the order. For $\mathbf{M}_{80}$ we can compute the minimal vectors in a few days, and perhaps argue via some property of them versus those for $\mathbf{N}_{80}$. We can also argue via Aschbacher's theorem on maximal subgroups of finite classical groups, and in an appendix, we sketch a proof along these lines, showing that $\mathrm{Aut}(\mathbf{N}_{80})$ is a maximal finite subgroup of $\mathrm{GL}_{80}(\mathbf{Z})$ up to a possible index of 4.

The idea of extremality can also be extended to include other lattices which are isomorphic to their dual(s). In this case, the full space of modular forms is typically replaced by the subspace that is fixed under the Atkin-Lehner involutions [36]. This then relates the question to a simultaneous maximisation of the minimum of a lattice and that of its shadow; see [13] and [32] for instance.

Finally, we note that [28] shows that there are only finitely many extremal lattices, though the most easily computed bound on maximal dimension still seems to be quite high.[4] In the other direction, King [22] classifies all (even) unimodular lattices in dimension 32 with no roots, and finds there to be at least 10^7 such; as the lack of roots implies that the lattices have no vectors of norm 2, it follows that each is extremal. Similarly, Peters [33] shows there are at least 10^{51} extremal lattices in dimension 40.

3 Construction of the lattice $\mathbf{N}_{80}$

We follow the paper [40] of Schulze-Pillot on quadratic residue codes and cyclotomic lattices, which builds on works from Thompson, Feit [9], and Quebbemann [35, §3] about unimodular lattices with an automorphism of prime order.

[4] The proof therein is similar in flavour to the idea we exploit, that is, for sufficiently large dimension, the first form in a triangular basis will have coefficients that are negative, and thus positivity precludes the existence of an extremal lattice. See the recent [42, p. 36] for a brief sketch. Our computations give that the q^{n+2} term in the expansion is negative for $n \geq 6\,775, 6\,789, 6\,803$ for the respective 0, 8, 16 mod 24 classes, which gives an upper bound of $163\,264 = (6802 \cdot 24) + 16$ for the dimension of an even unimodular extremal lattice. Finally, Rains [37] has followed upon the work of Krasikov and Litsyn [27] to obtain that the minimal norm of a unimodular lattice is (asymptotically with dimension $d \to \infty$) smaller than the Siegel bound $\sim d/12$ by at least a *constant factor* (see $N = 1$ in the Remark after Theorem 4.2 in [37]).

The construction gives a unimodular lattice as a sublattice of index p in a (rescaled) direct sum of two lattices of dimensions 2 and $(p-1)$. In this, the 2-dimensional lattice T_2 can be taken as any integral lattice of determinant p. The lattice U_{p-1} of dimension $(p-1)$ comes about from an (unpublished) construction of Thompson (see [9, §9]). We let $E = \mathbf{Q}(\zeta_p)$ be cyclotomic, and take an ideal $\mathfrak{A} \subseteq \mathcal{O}_E$ such that $\mathfrak{A}\bar{\mathfrak{A}} = (d)$ with $d \in E^+$ totally positive. This ideal induces a (positive definite) lattice of dimension $(p-1)$ via a basis for the ring of integers $\mathbf{Z}[\zeta_p]$, with the quadratic form given by $Q_1(u) = \mathrm{tr}_{\mathbf{Q}}^E(u\bar{u}d^{-1})$. Via a computation (with the different as in [9, Theorem 9.3], or with a Vandermonde determinant) one can show that the lattice U_{p-1} has determinant p^{p-2}.

To obtain a unimodular lattice of dimension $(p+1)$, we start with the direct sum $T_2 \oplus U_{p-1}$, and take the sublattice of this consisting of all vectors whose norm is a multiple of p. Upon dividing the whole lattice by p, the result will be integral and unimodular, the latter since $(p \cdot p^{p-2}) \cdot p^2/p^{p+1} = 1$. We need to show that this actually yields a sublattice, that is, the resulting subset of the original lattice satisfies the group law, and this is most easily done via homomorphic projection maps. We take the lattice

$$\mathbf{N}(T_2, U_{p-1}) = \{(\boldsymbol{m}, \boldsymbol{u}) \in T_2 \oplus U_{p-1} \mid \pi(\boldsymbol{m}) = \rho(\boldsymbol{u})\}$$

under the quadratic form $Q\big((\boldsymbol{m}, \boldsymbol{u})\big) = \big(Q_0(\boldsymbol{m}) + Q_1(\boldsymbol{u})\big)/p$, with the projection maps being $\pi : T_2 \to R/\mathrm{rad}_{Q_0}(R)$ where $R = T_2/pT_2$, and $\tilde{\rho} : \mathfrak{A} \to \mathfrak{A}/(1-\zeta_p)\mathfrak{A}$ (here $\tilde{\rho}$ is on $\mathfrak{A}$, with ρ on U_{p-1}). Since $(1-\zeta_p)$ has norm p, both images will be vector spaces over $\mathbf{F}_p$ of dimension 1, and we can identify them (arbitrarily) by taking $\boldsymbol{m}_0 \in T_2$ and $u_0 \in \mathfrak{A}$ with $Q_0(\boldsymbol{m}_0) \equiv 1 \pmod{p}$ and $u_0\bar{u}_0 d^{-1} \equiv 1 \pmod{(1-\zeta_p)\mathcal{O}_E}$. The lattice $\mathbf{N}(T_2, U_{p-1})$ will be even if and only if T_2 is even.

3.1 An odd lattice

Rather than derive our desired even unimodular lattice directly, we again follow Schulze-Pillot, who first constructs an odd lattice for which the automorphism group can be determined via a relation to coding theory, and then passes to an even lattice via Kneser's neighbouring construction.

We let K be the imaginary quadratic field $\mathbf{Q}(\sqrt{-79})$, and $d = l = 19$ an auxiliary prime that splits. Writing $(l)\mathcal{O}_K = \mathfrak{l}\bar{\mathfrak{l}}$, the location of $\mathfrak{l}$ in the class group of K will have a determining factor on the lattice we derive in the end, and so the choice of l is not completely arbitrary. We let $\mathfrak{a}$ be the ideal of K generated by l and the twisted Gauss sum $\frac{1}{2}\big[1 - 33\sum_a \chi_p(a)\zeta_p^a\big]$ where χ_p is the quadratic character modulo p. Using the notation of Schulze-Pillot, we have $p = -j^2 + 8ml$ with $p = 79$, $j = 15$, $m = 2$, and $l = 19$, so that $yj \equiv 1 \pmod{l}$ together with $y \equiv 1 \pmod{4}$ yields $y = 33$.[5] Noting that $\mathfrak{a}\bar{\mathfrak{a}} = (l)$ and taking $E = \mathbf{Q}(\zeta_{79})$, we write $\mathfrak{A} = \mathfrak{a}\mathcal{O}_E$ so that $\mathfrak{A}\bar{\mathfrak{A}} = (19)$ in $\mathcal{O}_E$. Letting T_2 be the 2-dimensional lattice (in a basis $\{\boldsymbol{w}_1, \boldsymbol{w}_2\}$) of determinant 79 given by the

[5] The import of this numerology only becomes clear when proofs are included, as this choice of y for the scaling factor of the Gauss sum allows one to show that the cyclotomic and coding theory constructions agree.

Gram matrix $Q_0 = \begin{pmatrix} l & j \\ j & 8m \end{pmatrix} = \begin{pmatrix} 19 & 15 \\ 15 & 16 \end{pmatrix}$, we fix the gluing via $\pi(\boldsymbol{w}_1) = \rho(\big[l\zeta_p\big])$, where here $\big[\cdot\big]$ gives the map from $\mathfrak{A}$ to U_{p-1}. We let $\mathbf{N}_o = \mathbf{N}(T_2, U_{p-1})$ with these choices, noting that $\mathbf{N}_o$ is odd.

3.2 Relation to coding theory

We can obtain the correspondence with coding theory by taking p coordinates as $\boldsymbol{e}_i = \boldsymbol{w}_1 \oplus \big[l\zeta_p^i\big]$ for $0 \le i \le p-1$ and an additional one $\boldsymbol{e}_\infty = j\boldsymbol{w}_1 - l\boldsymbol{w}_2$, from which a computation shows that these $\boldsymbol{e}_i$ form a scaled root system of type $80A_1$ in $\mathbf{N}_o$, that is, each $\boldsymbol{e}_i$ has the same norm, and they are all mutually orthogonal. Indeed, for all $0 \le i \le p-1$ we have $\|\boldsymbol{e}_i\| = \big[Q_0(\boldsymbol{w}_1) + (p-1)\cdot(l^2/l)\big]/p = l$ since $Q_0(\boldsymbol{w}_1) = l$, while $\|\boldsymbol{e}_\infty\| = Q_0(j\boldsymbol{w}_1 - l\boldsymbol{w}_2)/p = l(8ml - j^2)/p = l$. For the inner products, we have

$$\begin{aligned}
\langle \boldsymbol{e}_i, \boldsymbol{e}_k \rangle &= \|\boldsymbol{e}_i + \boldsymbol{e}_k\| - \|\boldsymbol{e}_i\| - \|\boldsymbol{e}_k\| \\
&= \frac{1}{p}\Big(Q_0(2\boldsymbol{w}_1) + (l^2/l)\cdot \mathrm{tr}_{\mathbf{Q}}^E\big[(\zeta^i + \zeta^k)(\bar{\zeta}^i + \bar{\zeta}^k)\big]\Big) - 2l \\
&= \frac{1}{p}\Big(4l + l\cdot \mathrm{tr}_{\mathbf{Q}}^E\big[2 + \zeta^{i-k} + \zeta^{i+k}\big]\Big) - 2l \\
&= \frac{1}{p}\big(4l + l\cdot[2(p-1) - 1 - 1]\big) - 2l = 0
\end{aligned}$$

when $i \ne k$ and $i, k \ne \infty$, while for $i \ne \infty$ we have

$$\begin{aligned}
\langle \boldsymbol{e}_i, \boldsymbol{e}_\infty \rangle &= \|\boldsymbol{e}_i + \boldsymbol{e}_\infty\| - 2l \\
&= \frac{1}{p}\Big[Q_0\big((j+1)\boldsymbol{w}_1 - l\boldsymbol{w}_2\big) + (p-1)\cdot(l^2/l)\Big] - 2l \\
&= \frac{1}{p}\big[l(1 + 8ml - j^2) + l(p-1)\big] - 2l = 0.
\end{aligned}$$

Using this root system, it follows that the extended quadratic residue code $C \subseteq \mathbf{F}_l^{80}$ (or indeed, any self-dual code) gives an integral unimodular lattice via

$$\mathbf{N}_C = \left\{ \frac{1}{l}\sum_i a_i \boldsymbol{e}_i \;\middle|\; (\bar{a}_i) \in C \right\} \tag{1}$$

where the sum is over all 80 coordinates, and $\bar{a}_i$ is reduction mod l of a_i. The proof that $\mathbf{N}_C$ is the same lattice as our lattice $\mathbf{N}_o$ is given in [40, Proposition 1], using the generator matrix and idempotent of the code.[6] The appearance of the value $y = 33$ with the Gauss sum is of relevance therein.

One nicety of this re-visioning is that the code automorphism (of order 4) given by $a_\infty \to a_0$, $a_0 \to -a_\infty$, $a_i \to -\chi_p(i)a_j$, where $ij \equiv -1 \pmod p$, can

[6] We have taken a sublattice of index l^{p+1} via the scaled root system, and then taken a superlattice of the same index via the construction from coding theory, and so just have to check that these operations are compatible.

be seen to lift to the lattice. Combined with the order p automorphism induced via ζ_p, which fixes a_∞ and cycles $a_0 \to a_1 \to \cdots \to a_{p-1} \to a_0$, this gives $\mathbf{SL}_2(\mathbf{F}_p)$ as a subgroup of the automorphism group $\mathrm{Aut}(\mathbf{N}_o)$ of the lattice.

In an appendix, we use the classification of finite simple groups to show that this realisation of $\mathbf{SL}_2(\mathbf{F}_{79})$ is within a factor of 4 of being a maximal finite subgroup of $\mathbf{GL}_{80}(\mathbf{Z})$, so that $[\mathrm{Aut}(\mathbf{N}_o) : \mathbf{SL}_2(\mathbf{F}_{79})] \leq 4$.

3.3 The even 2-neighbours

The above lattice $\mathbf{N}_o$ is odd, while we wish to get an even unimodular lattice. The method of passing to this is given by the neighbouring method of Kneser [26]. Again following Schulze-Pillot, we want to find $\boldsymbol{v} \in \mathbf{N}_o$ with $Q(\boldsymbol{v}) \in 4\mathbf{Z}$, and then take the lattice spanned by $\boldsymbol{v}/2$ and the sublattice of $\mathbf{N}_o$ whose inner product with $\boldsymbol{v}$ is even. Via linear algebra over $\mathbf{F}_2$, we find that there is a 2-dimensional space of such $\boldsymbol{v}$ satisfying the conditions (Schulze-Pillot notes this in general via genus theory). Obviously $\boldsymbol{v} = \mathbf{0}$ does not help us, while we also need $Q(\boldsymbol{v}) \in 8\mathbf{Z}$ if the resulting neighbouring lattice is to be even, and this eliminates another of the initial 4 possibilities. This leaves but 2 choices for $\boldsymbol{v}$, one of which gives a lattice with many vectors of norm 4 (note that $\boldsymbol{v}$ itself must have norm at least 32 if the new lattice is to have minimum 8) and the other of which is our desired lattice $\mathbf{N}_{80}$.

As in [40, Proposition 2], we could construct $\mathbf{N}_{80}$ directly using a different choice with T_2 in the cyclotomic construction, though the relation to coding theory then becomes less clear. For instance, [40, Example 3] takes $l = 5$ and $Q_0 = \begin{pmatrix} 8 & 1 \\ 1 & 10 \end{pmatrix}$ to get the same $\mathbf{N}_{80}$. Finally, the last Remark of [40] notes the automorphisms of $\mathbf{N}_o$ given by $\mathbf{SL}_2(\mathbf{F}_p)$ all transfer to $\mathbf{N}_{80}$. As noted above, we show in an appendix that $[\mathrm{Aut}(\mathbf{N}_{80}) : \mathbf{SL}_2(\mathbf{F}_{79})] \leq 4$ so that in particular $\mathbf{N}_{80}$ and $\mathbf{M}_{80}$ are not isometric, but our proof of extremality does not use this.

4 Nice bases for $\mathbf{N_{80}}$

We next link $\mathbf{N}_{80}$ to the construction given in [1] that modifies the method of Gross. The authors of [1] construct the lattice from a representation that is irreducible away from 2. In particular, in the basis they obtain, all the coordinates are of the same parity. Furthermore, the automorphisms are given by a doubly transitive signed permutation action on the coordinates.

From our construction, we have a lattice $\mathbf{N}_{80}$ with automorphisms generated by two matrices O_{79} and O_4. We wish to transform this so that the automorphisms are generated by signed permutations σ_{79} and σ_4 (as in the end of Section 3.2), thus giving a doubly transitive coordinate action. One way to achieve this is just to solve the 80^2-dimensional linear algebra problem given by equating the automorphisms, that is, solve $O_{79}X = X\sigma_{79}$ and $O_4X = X\sigma_4$ for the unknown matrix X (we try solving this with both σ_4 and σ_4^3).

It turns out that the resulting solution space is 2-dimensional, and if we write X_1 and X_2 for generators of it, then the determinant of the matrix $\big(X_1 t + X_2 u\big)$ is given by $2^{40} f(t,u)^{40}$ where f is a binary quadratic form of discriminant -79 corresponding to the ideal of above. To obtain the representation of [1] we choose the pair (t,u) so that $f(t,u) = 8$, so that the transform maps vectors of norm 10 in $\mathbf{N}_{80}$ to vectors of norm $16 \cdot 10$ in the resulting sublattice of $\mathbf{Z}^{80}$. The resulting basis has the property that every vector has coordinates all of the same parity. We denote this transform matrix from $\mathbf{N}_{80}$ to $\mathbf{Z}^{80}$ by T_{16}, and the resulting lattice basis by B_{80}.

4.1 Identifying orbits

As noted above, the action of σ_{79} and σ_4 is doubly transitive, and we can exploit this to expedite the finding of a canonical representative for a given orbit. We first find the largest coordinate in absolute value, and move it to the front, and then cycle the latter 79 coordinates until the second largest is in the second position. This movement uses $80 \cdot 79$ elements of the group, and after modding out by the centre $\{\pm 1\}$, we only have 39 possibilities left to check for their 78 latter coordinates (we use a lexicographic ordering). Of course, we could have many ties amongst the two largest coordinates (this is basis-dependent, and we can map to another choice of (t,u) if desired), but this method will still be much faster than looping over all 492 960 possibilities.

5 Method of proof

We now describe how we shall show that $\mathbf{N}_{80}$ is indeed extremal. Since the lattice $\mathbf{N}_{80}$ is even and unimodular, its Θ-series Θ_{80} lies in the vector space of modular forms of level 1 and weight 40 (see [30]). This space has dimension 4, and a triangular integral basis is:

$$\begin{aligned}
f_0 &= 1 + 1\,250\,172\,000\,q^4 + 7\,541\,401\,190\,400\,q^5 + O(q^6),\\
f_1 &= q + 19\,291\,168\,q^4 + 37\,956\,369\,150\,q^5 + O(q^6),\\
f_2 &= q^2 + 156\,024\,q^4 + 57\,085\,952\,q^5 + O(q^6),\\
f_3 &= q^3 + 168\,q^4 - 12\,636\,q^5 + O(q^6).
\end{aligned}$$

We thus know that $\Theta_{80} = f_0 + a_1 f_1 + a_2 f_2 + a_3 f_3$ for some integers a_i. We shall derive that $a_1 = a_2 = 0$ by showing that there are no vectors of norm 2 or 4 in the lattice. We will then have

$$\Theta_{80} = 1 + a_3 q^3 + (\cdots) q^4 + (7\,541\,401\,190\,400 - 12\,636\,a_3)\,q^5 + O(q^6).$$

By positivity we have $a_3 \geq 0$, and so by finding 7 541 401 190 400 vectors of norm 10 in the lattice, we deduce that $a_3 = 0$ so that $\mathbf{N}_{80}$ is extremal as claimed.

The reader might wonder why we do not simply search for norm 6 vectors, but instead aim to find all those of norm 10, as the latter (at first glance) seems much

harder. However, the search in norm 6 has to be exhaustive, while with norm 10 it need not be: we find one vector in each orbit, and apply automorphisms to get the whole set. We estimate an exhaustive search for norm 6 vectors would take more than 1 000 times as much work as our method using norm 10 vectors.

5.1 The lattice $\mathbf{N_{80}}$ has no vectors of norm 2 or 4

As we noted above in Section 4, we can change the basis by a transform T_{16} so that each vector has its norm multiplied by 16, with the resulting basis having the property that all the coordinates of any vector will have the same parity. In particular, a vector of norm 2 or 4 will have the square-sum of its coordinates as 32 or 64, with necessarily all coordinates being even. Also, the inner product of any two vectors in this basis will need to be a multiple of 16, a fact we exploit below. Finally, the lattice automorphisms in this new basis are given by signed permutations, with the action doubly transitive.

No vectors of norm 2 (roots). One proof (from Elkies) first notes that the only root systems with compatible automorphisms are A_1^{80} and D_{80}. With the former, any automorphism of order 79 would necessarily fix at least one of the 160 roots, but the 2-dimensional sublattice of $\mathbf{N}_{80}$ fixed by a 79-cycle has no roots. The latter is similarly impossible; a 39-cycle must fix a root since $\gcd(39, 12\,640) = 1$, but the 4-dimensional sublattice therein lacks roots.

Another way (similar to a comment in [40, Example 3]) would be to use $l = 5$ and note that we must have $\sum_i a_i^2 = 2l = 10$ in (1), while the minimal distance[7] of the extended quadratic residue code of length 80 over $\mathbf{F}_5$ is > 10, though care needs to be made here when working with both $\mathbf{N}_{80}$ and the odd lattice L.

A direct computation also easily shows that $\mathbf{N}_{80}$ has no roots. After applying suitable reduction, the verification typically takes less than 30 minutes. We did not try a similar computation with norm 4, as we estimate that it would likely take a few months.

No vectors of norm 2 or 4. We let B_{80}^e be the sublattice of B_{80} given by vectors with even coordinates in the T_{16} basis, and map $B_{80}^e \to B_{80}^e/2 \to \mathbf{F}_2^{80}$ via the additive coordinate map generated by $\pm 2 \to \pm 1 \to 1$. The image in $\mathbf{F}_2^{80}$ is a binary code C_2, and this inherits the automorphisms from the lattice.

We have $16 | \langle \boldsymbol{v}, \boldsymbol{w} \rangle$ for any $\boldsymbol{v}, \boldsymbol{w} \in B_{80}^e$, which implies that C_2 is doubly-even, that is, each codeword has weight divisible by 4. Similarly, we see that $C_2 \subseteq C_2^\perp$, as the inner product between any two codewords is 0 (in $\mathbf{F}_2$). We then show equality here by finding enough vectors in B_{80}^e to show that $\dim(\mathrm{C}_2) \geq 40$.

As C_2 is self-dual and has automorphism group $\mathbf{PSL}_2(\mathbf{F}_{79})$, it follows from either [25, Theorem 6.2] or [24, Satz 3.4] that C_2 is equivalent to the extended

[7] It seems that showing the minimal distance exceeds 20 would take about 58 days, though the computation should parallelise.

binary quadratic residue code,[8] and thus has minimal weight of 16 with 97 565 minimal codewords which lie in 3 orbits under the automorphisms.[9]

We now check that the preimages of codewords of weight 0 and 16 in C_2 do not yield vectors of norm 2 or 4 in $\mathbf{N}_{80}$.[10] This is done using the explicit form of T_{16}^{-1}. For weight 0, we need to check that $T_{16}^{-1}\boldsymbol{w}$ is non-integral for

$$\boldsymbol{w} = \langle 8, 0, \ldots, 0\rangle, \langle 4, \pm 4, 0, \ldots, 0\rangle, \langle 4, \pm 4, (\ldots)\rangle$$

where in this third expression exactly two of the latter 78 coordinates have size 4. By the doubly transitive nature of the automorphism action, this suffices. There are thus $3 + 2^3\binom{78}{2} = 24\,027$ possibilities to check here.

For weight 16, we have 3 orbits of codewords. For each orbit we take a representative, and lift its nonzero coordinates in 2^{16} ways to every choice of sign for ± 2. We then apply T_{16}^{-1} to each, and note that none are integral. This completes the proof that there are no vectors of norm 2 or 4 in the lattice $\mathbf{N}_{80}$. Presumably we could similarly show that B_{80}^e has no vectors of norm 96, but extending our observations to odd-coordinate vectors in B_{80} looks more difficult.

5.2 Vectors with a nontrivial stabiliser

We now describe how to use the known automorphisms to reduce our vector-finding quota from 7.5 trillion vectors down to about 15.3 million. We make a separate computation of the norm 10 vectors that have nontrivial stabiliser. If a vector $\boldsymbol{v}$ has a nontrivial stabiliser under the above action of $G = \mathbf{SL}_2(\mathbf{F}_{79})$, there is some nontrivial element $g \in G$ such that the kernel of $\big(g - \mathrm{id}\big)$ contains $\boldsymbol{v}$. So we loop over nontrivial elements (or conjugacy classes) of G, compute this kernel (which is a sublattice), and then search for short vectors in it. The elements of order 3 give a kernel sublattice of dimension 28, for which it takes a few seconds to find the vectors of norm ≤ 10. These yield 465 orbit classes under the action. The elements of order 5, 39, and 79 give lattices of dimensions 16, 4, and 2, and yield 15, 2, and 1 orbits respectively. Upon computing the stabilisers, we obtain

- 1 orbit with stabiliser size $79 \cdot 39 = 3081$ (order 79),
- 2 orbits with stabiliser size 39 (order 39),
- 15 orbits with stabiliser size 5 (order 5),

[8] We thank Elkies for recalling this fact, and J. Cannon for the Klemm reference.

[9] Here is an alternative method. Assume first that there is a codeword $\boldsymbol{w}$ of weight 4 or 8. Take a 79-cycle σ and note that since $(8-1)^2 < 79$ there is some iterate of σ such that $\boldsymbol{w}$ and $\sigma\boldsymbol{w}$ intersect only in the fixed coordinate. This implies that $\langle \boldsymbol{w}, \sigma\boldsymbol{w}\rangle = 1$, which contradicts that C_2 is self-dual. Since there are no codewords of weight 4 or 8, we can then apply Gleason's theorem [16] and get that the weight enumerator is of the form $q^0 + (a + 15\,200)\,q^{12} + (127\,965 + 2a)\,q^{16} + (11\,347\,488 - 101a)\,q^{20} + \ldots$ for some $a \in \mathbf{Z}$, and in an echo of our proof of lattice extermality, show code extremality (no codewords of weight 12) via finding 12 882 688 codewords of weight 20; for this, we find short vectors in the lattice, map to the code, and apply automorphisms.

[10] We do not explicitly need the fact that the code is extremal for this step, but only that we have all codewords of length 16 or less.

– 465 orbits with stabiliser size 3 (order 3).

None of the other 78 nontrivial conjugacy classes of $\mathbf{SL}_2(\mathbf{F}_{79})$ yields an orbit with vectors of norm 10. We can also note that there no vectors of norm 6 with a nontrivial stabiliser (though this is not strictly necessary for our proof).

An accounting then tells us that there are presumably 7 541 323 277 280 vectors of norm 10 yet unfound, and dividing by $\#\mathbf{SL}_2(\mathbf{F}_{79}) = 492\,960$ predicts 15 298 043 orbits with trivial stabiliser. Via a standard coupon-collecting analysis [11, p. 213] we expect that about 250 million suitably random vectors of norm 10 should suffice to hit each orbit at least once.

In fact, for the purposes of proving the lattice extremal, we need only find $(15\,298\,043 - 12\,635)$ orbits (see the q^5 coefficient of f_3, and use the fact that $492\,960|a_3$ as we find no vectors of norm 6 with nontrivial stabiliser), and due to the lengthy final part of coupon-collecting,[11] this reduces the expected running time by about 55%. However, for completeness, we still chose to find all orbits.

6 General search for vectors of norm 10

The general method to enumerate short vectors in a lattice is due to Kannan [21] and Fincke and Pohst [12]. This corresponds to the computation of the leaves of a huge tree. As noted by Schnorr and Euchner [38], this tree can be pruned to some extent. This can be thought of as searching first in the areas of the search region which are more likely to contain short vectors, or, equivalently, removing the tree nodes that are less likely to produce useful leaves. The initial pruning strategy was later improved in [39]. We describe below a further improvement.

6.1 The full KFP tree search

The basic method iteratively looks at the projections to the span of the first i coordinates for decreasing i. We have a basis given by $\{\boldsymbol{b}_i\}$ and wish to solve the inequality $\|\sum_i x_i \boldsymbol{b}_i\|^2 \leq 10$. Borrowing the common notation for lattice reduction, we take the Gram-Schmidt orthogonalisation, and translate the x_i's by the $\mu_{j,i}$'s:

$$\boldsymbol{b}_i^\star = \boldsymbol{b}_i - \sum_{j<i} \mu_{i,j}\boldsymbol{b}_j^\star \text{ so that } \mu_{i,j} = \frac{\langle \boldsymbol{b}_i, \boldsymbol{b}_j^\star\rangle}{\|\boldsymbol{b}_j^\star\|^2} \text{ for } i > j, \text{ and } y_i = x_i + \sum_{j=i+1}^{d} \mu_{j,i} x_j.$$

Here d is the dimension. By substituing y_i for x_i, we get $\sum_i y_i^2 \|\boldsymbol{b}_i^\star\|^2 \leq 10$, which by positivity leads to the series of inequalities:

$$\begin{aligned} y_d^2\|\boldsymbol{b}_d^\star\|^2 &\leq 10, \\ y_{d-1}^2\|\boldsymbol{b}_{d-1}^\star\|^2 &\leq 10 - y_d^2\|\boldsymbol{b}_d^\star\|^2, \\ &\cdots \\ y_1^2\|\boldsymbol{b}_1^\star\|^2 &\leq 10 - \sum_{i=2}^{d} y_i^2\|\boldsymbol{b}_i^\star\|^2. \end{aligned}$$

[11] The comparison is between $\sum_{n=1}^{N} \frac{N}{n}$ and $\sum_{n=12636}^{N} \frac{N}{n}$ for $N = 15\,298\,043$.

Note that for all i, the variable x_i is an integer, while y_i is a shift of x_i by a fixed amount (once $x_{i+1}, \ldots, x_d$ have been chosen). The KFP method proceeds by looking at all y_d's satisfying the first inequality, then all pairs (y_{d-1}, y_d) satisfying the second, etc. In particular, the vectors with $y_i \approx 0$ for all i up to a given point will be found most easily (and these often correspond to small x_i's). Also, to find more short vectors earlier in the search procedure, it is useful to run over the different possible x_i's from the centre of the interval implied by the inequality $y_i^2 \|\boldsymbol{b}_i^*\|^2 \leq 10 - \sum_{j>i} y_j^2 \|\boldsymbol{b}_j^*\|^2$: the variable x_i will run across the integers by decreasing proximity to $-\sum_{j>i} \mu_{j,i} x_j$. This "zig-zag" strategy, introduced by Schnorr and Euchner [38], allows one to split the search of the tree in different stages: in the first stage, we have $x_j = 0$ for all $j > 1$; then in the second stage we have $x_j = 0$ for all $j > 2$ but $x_2 \neq 0$; etc. We call stage i the period of time during which $x_j = 0$ for all $j > i$ but $x_i \neq 0$. Stage i means that we have already reached level i in the KFP tree but not yet been in level $i + 1$ (level 1 corresponding to the leaves).

The arithmetic operations corresponding to Gram-Schmidt orthogonalisation computations can be quite slow. The Magma [5] implementation of the KFP tree search replaces them by double precision floating-point arithmetic operations, in a fully reliable way (using [34]).

6.2 Tree pruning

Our pruning strategy consists in restricting the above inequalities by a "pruning factor" that depends on the level. So the above inequalities become

$$\sum_{i=j}^{d} y_i^2 \|\boldsymbol{b}_i^\star\|^2 \leq 10 \cdot P_j, \ \forall j$$

where P_j is the jth pruning factor. A version of this with a specific choice of P_j appears in [38, §7], and the general description as well as its analysis below have been independently obtained in [15, §4]. In the latter, the authors also introduce the concept of "extreme pruning", which resembles but differs from our bases switching strategy (see subsection below).

The "best" choice for the pruning factors appears to be something like $P_j = (d - j + 1)/d$. We happened to choose $P_j = 1 - (j - 1)/100$ in practise. The idea here can be phrased as follows: we have a given quantity of "norm" (here 10) to spend on a vector; if we spend a lot on the coordinates x_j to x_d, there will then be a lesser chance that we can form an integral vector via some possible choice of the other coordinates, due to positivity and the fact that most coordinates will have at least some nonzero contribution.

Efficacy of pruning. To give an idea of the efficacy of pruning, we can use the notion, from [19], of expected enumeration cost for a given lattice basis $\{\boldsymbol{b}_i\}$ and

for vectors of norm A (a function `EnumerationCost` is available in Magma [5]):

$$\sum_{j=1}^{d} \frac{\sqrt{\pi^{d-j+1} \prod_{k=j}^{d} A/\|\boldsymbol{b}_k^\star\|^2}}{\Gamma\big(1+(d-j+1)/2\big)}. \tag{2}$$

A typical enumeration cost for our bases with $\mathbf{N}_{80}$ was around 10^{23}. This is the expected number of nodes of the KFP tree. For comparison, the implementation in Magma [5] has a traversal rate of about 7.5 million nodes per second.

By comparing this enumeration cost estimate to the expected $7.5 \cdot 10^{12}$ vectors of norm 10, we find that more than 10^{10} nodes are expected to be searched for each vector found. In the case of the pruned enumeration, the jth summand in (2) should be multiplied by the volume of the truncated hypersphere $\{(z_j, \ldots, z_d) : \forall i \geq j, \sum_{k \geq i} z_k^2 \leq P_i\}$. By estimating these volumes with a Monte-Carlo rejection method (uniformly sampling points in the full hypersphere and counting how many belong to the truncation), we expect our pruning to gain a factor of around 10^4 here, at the cost of missing about 60% of the short vectors. These speedup and miss ratios are not constant across all levels of the search: they seem to be closer to 100 and 25% respectively for the levels of our interest (due to the early abort and perturbation strategy described below).

6.3 Switching bases

The early stages of the tree search can have a significantly better chance of providing short vectors, due primarily to the relative paucity of "uninteresting" branches that tend to become more numerous at higher levels. In practice, we would find 10^5 vectors in about 30 minutes, for a ratio of about 150 000 nodes searched for each vector found, more than an order of magnitude lower than the above estimate, even with the pruning included.

Every 15-30 minutes we would switch the basis by applying a random permutation to the coordinates of the current basis, and then multiplying by a random upper triangular matrix with ones on the diagonal and off-diagonal entries in $\{-1, 0, +1\}$. We then re-apply LLL (with a δ-value nearly 1) to the perturbed basis, and then LLL with deep insertions [38]. Overall, this takes only a few seconds. This basis switching also makes parallelisation essentially trivial.

A second reason for periodically changing the basis is that (a phenomenon we found experimentally) there are some bases which "hide" many of the orbits, in the sense that every vector in such an orbit would not be found until we reach one of the latter stages. We currently have no explanation of this.

7 Conclusion and related work

We implemented the above in a combination of Magma [5] and `C`. As we typically found 10^5 vectors of norm 10 in about 30 minutes, the estimated time was around 52 days. Using 14 processors in parallel, it took us about 4 days in April 2009.

7.1 Software to check our data

A verification of our proof can be done in much less time than the computation itself. We provide software[12] that takes less than 10 hours to verify that $\mathbf{N}_{80}$ is indeed extremal. The input consists of 15 298 526 entries that correspond to coordinate vectors in the T_{16} basis of Section 4. The following checks are run:

- Each entry lexicographically follows its predecessor
- Each entry has norm 160 and is integral when multiplied by T_{16}^{-1},
- Each entry is lexicographically the first in its orbit.

The first condition ensures that all entries are distinct, while the last ensures that each corresponds to a distinct orbit, with the middle condition implying that the vectors have norm 10 and are in $\mathbf{N}_{80}$. We can also list the 483 orbits with nontrivial stabiliser, whose provenance can be checked separately.

7.2 Three lattices of dimension 72

The work in progress [1] investigates three lattices of dimension 72. Two of these are 2-neighbours of a lattice constructed via the extended quadratic residue code over $\mathbf{F}_3$, and the other involves a code over $\mathbf{Z}/4\mathbf{Z}$. None of these turned out to be extremal (minimal norm of 8), and indeed, we know of no extremal lattice of this dimension. In fact, a recent preprint of Griess [17] claims to be the first to prove a minimal norm as large as 6 for an even unimodular lattice of dimension 72.

7.3 Other candidate lattices for extremality in dimension 80

In [3], the authors note three other candidates for extremality amongst even unimodular lattices in dimension 80. One candidate comes from a cyclo-quaternionic construction given in [31, Remark 5.2], and its automorphism group contains $\mathbf{SL}_2(\mathbf{F}_{41}) \otimes \tilde{S}_3$, which is of comparable size to our $\mathbf{SL}_2(\mathbf{F}_{79})$. We do not see how to facilitate the calculation of canonical orbit representatives as readily as in our case, but the fact that canonicalising took only about 5% of our running time indicates that our methods could work in this case, with sufficient effort.

The other two candidates come from a cyclotomic construction explored in [4], and have an automorphism group containing the general affine linear group $\mathbf{F}_{41}^{+} \rtimes \mathbf{F}_{41}^{*}$. Our initial opinion is that the automorphism group (even if augmented by an order 4 element) is too small for our method to work well here.

Acknowledgments. We thank the authors of [1], with whom we started this research, and S. R. Donnelly who shared some of his ideas with us. We also thank the anonymous reviewers for their recommendation to add a proof that the automorphism group of $\mathbf{N}_{80}$ differs from those of $\mathbf{L}_{80}$ and $\mathbf{M}_{80}$. The present work is part of the Australian Research Council Discovery Project DP0880724 "Integral lattices and their theta series".

[12] The code is `checkit80.c` (to be run with arguments "10 ⟨filename⟩") and the data is `LAT80.n10.sc16.bz2` in the directory `http://magma.maths.usyd.edu.au/~watkins`

References

1. Z. Abel, N. D. Elkies, S. D. Kominers, *On 72-dimensional lattices*, in preparation.
2. M. Aschbacher, *On the maximal subgroups of the finite classical groups.* Invent. Math. **76** (1984), no. 3, 469–514. See `http://dx.doi.org/10.1007/BF01388470`
3. C. Bachoc, G. Nebe, *Extremal lattices of minimum 8 related to the Mathieu group M_{22}.* J. Reine Angew. Math. **494** (1998), 155–171.
   Available from `http://dx.doi.org/10.1515/crll.1998.004`
4. C. Batut, H.-G. Quebbemann, R. Scharlau, *Computations of cyclotomic lattices.* Experiment. Math. **4** (1995), no. 3, 177–179.
   Available from `http://www.expmath.org/restricted/4/4.3/batut.ps`
5. W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language.* In *Computational algebra and number theory*, Proceedings of the 1st Magma Conference held at Queen Mary and Westfield College, London, August 23–27, 1993. Edited by J. Cannon and D. Holt, Elsevier Science B.V., Amsterdam (1997), 235–265. Cross-referenced as J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.
   Available from `http://magma.maths.usyd.edu.au`
6. J. H. Conway, A. M. Odlyzko, N. J. A. Sloane, *Extremal self-dual lattices exist only in dimensions* 1 *to* 8, 12, 14, 15, 23, *and* 24. Mathematika **25** (1978), no. 1, 36–43.
   Available from `http://dx.doi.org/10.1112/S0025579300009244`
7. J. H. Conway, N. J. A. Sloane, *Sphere packings, lattices and groups.* Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], **290**. Springer-Verlag, New York, 1988. xxviii+663pp.
8. J. H. Conway, N. J. A. Sloane, *A new upper bound on the minimal distance of self-dual codes.* IEEE Trans. Inform. Theory **36** (1990), no. 6, 1319–1333.
   Available from `http://dx.doi.org/10.1109/18.59931`
9. W. Feit, *On integral representations of finite groups.* Proc. London Math Soc. (3) **29** (1974), 633–683.
   Available from `http://plms.oxfordjournals.org/cgi/reprint/s3-29/4/633`
10. W. Feit, *Orders of finite linear groups.* In *Proceedings of the First Jamaican Conference on Group Theory and its Applications (Kingston, 1996),* January 9–12, Univ. West Indies, Kingston. Edited by T. Foguel and J. Minty. University of the West Indies, Mona Campus, Kingston, Jamaica, (1997), 9–11.
11. W. Feller, *Introduction to Probability Theory*, Vol. I, John Wiley & Sons, New York, 1950.
12. U. Fincke, M. Pohst, *A procedure for determining algebraic integers of given norm.* In *Computer Algebra* (London 1983), proceedings of the European computer algebra conference (EUROCAL), edited by J. A. van Hulzen, Lecture Notes in Computer Science **162**, Springer-Verlag, Berlin (1983), 194–202.
    Available from `http://dx.doi.org/10.1007/3-540-12868-9_103`
13. P. Gaborit, *A bound for certain s-extremal lattices and codes.* Arch. Math. (Basel) **89** (2007), no. 2, 143–151. See `http://dx.doi.org/10.1007/s00013-006-1164-5`
14. P. Gaborit, *Construction of new extremal unimodular lattices.* Eur. J. Combin. **25** (2004), no. 4, 549–564. See `http://dx.doi.org/10.1016/j.ejc.2003.07.005`
15. N. Gama, P. Q. Nguyen, O. Regev, *Lattice Enumeration Using Extreme Pruning.* To appear in *Advances in Cryptology - EUROCRYPT 2010*, proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Edited by H. Gilbert, Lecture Notes in Computer Science **6110**, Springer (2010).

16. A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities.* In *Actes du Congrès International des Mathématiciens* [Proceedings of the International Congress of Mathematicians] (Nice, 1970), Tome 3, Gauther-Villars, Paris (1971), 211–215.
17. R. L. Griess, Jr., *Rank 72 high minimum norm lattices*, preprint available from `http://arxiv.org/abs/0910.2055`
18. B. H. Gross, *Group representations and lattices.* J. Amer. Math. Soc. **3** (1990), no. 4, 929–960. Available from `http://dx.doi.org/10.2307/1990907`
19. G. Hanrot and D. Stehlé, *Improved Analysis of Kannan's Shortest Lattice Vector Algorithm.* In *Advances in Cryptology - CRYPTO 2007*, edited by A. Menezes, Lecture Notes in Computer Science **4622**, Springer-Verlag, Berlin (2007), 390–405. See `http://dx.doi.org/10.1007/978-3-540-74143-5_10`
20. G. Hiss and G. Malle, *Low-dimensional representations of quasi-simple groups.* LMS J. Comput. Math. **4** (2001), 22–63. Corrigenda: LMS J. Comput. Math. **5** (2002), 95–126.
See `http://www.lms.ac.uk/jcm/4/lms2000-014/sub/lms2000-014.pdf`
and `http://www.lms.ac.uk/jcm/5/lms2002-025/sub/lms2002-025.pdf`
21. R. Kannan, *Improved algorithms for integer programming and related lattice problems.* In *Proceedings of the fifteenth annual ACM symposium on the Theory of computing* (Boston MA, STOC 1983), 99–108, ACM order #508830. Available from `http://doi.acm.org/10.1145/800061.808749`
22. O. King, *A mass formula for unimodular lattices with no roots.* Math. Comp. **72** (2003), no. 242, 839–863. Available online from the publisher (the AMS) via `http://www.ams.org/mcom/2003-72-242/S0025-5718-02-01455-2`
23. P. B. Kleidman, M. W. Liebeck, *The subgroup structure of the finite classical groups.* London Mathematical Society Lecture Note Series, **129**. Cambridge University Press, Cambridge, 1990. x+303 pp.
24. M. Klemm, *Kennzeichnung der erweiterten quadrate-codes durch ihre* $\mathbf{PSL}(2,q)$*-zulässigkeit.* (German) [Characterising the extended quadratic-codes by their $\mathbf{PSL}(2,q)$-admissibility]. Communications in Algebra **11** (1983), no. 18, 2051–2068. Available from `http://dx.doi.org/10.1080/00927878308822949`
25. W. Knapp, P. Schmid, *Codes with prescribed permutation group.* J. Algebra **67** (1980), 415–435. See `http://dx.doi.org/10.1016/0021-8693(80)90169-6`
26. M. Kneser, *Klassenzahlen definiter quadratischer Formen.* (German) [Class numbers of definite quadratic forms]. Arch. Math. **8** (1957), 241–250.
Available from `http://dx.doi.org/10.1007/BF01898782`
27. I. Krasikov, S. Litsyn, *An improved upper bound on the minimum distance of doubly-even self-dual codes.* IEEE Trans. Inform. Theory, **46** (2000), no. 1, 274–278. Available from `http://dx.doi.org/10.1109/18.817527`
28. C. L. Mallows, A. M. Odlyzko, N. J. A. Sloane, *Upper bounds for modular forms, lattices, and codes.* J. Algebra **36** (1975), no. 1, 68–76.
Available from `http://dx.doi.org/10.1016/0021-8693(75)90155-6`
29. H. Minkowski, *Zur Theorie der positiven quadratischen Formen.* (German) [On the Theory of positive quadratic Forms]. J. reine angew. Math. **101** (1887), 196–202. See `http://resolver.sub.uni-goettingen.de/purl?GDZPPN002160390`
30. T. Miyake, *Modular Forms*. Springer-Verlag, Berlin, New York, 1989.
31. G. Nebe, *Some cyclo-quaternionic lattices.* J. Algebra **199** (1998), no. 2, 472–498. Available from `http://dx.doi.org/10.1006/jabr.1997.7163`
32. G. Nebe, K. Schindelar, *S-extremal strongly modular lattices.* J. Théor. Nombres Bordeaux **19** (2007), no. 3, 683–701.
Available from `http://jtnb.cedram.org/item?id=JTNB_2007__19_3_683_0`

33. M. Peters, *Definite unimodular 48-dimensional quadratic forms.* Bull. London Math. Soc. **15** (1983), no. 1, 18–20.
See http://blms.oxfordjournals.org/cgi/content/citation/15/1/18
34. X. Pujol, D. Stehlé, *Rigorous and efficient short lattice vectors enumeration.* In *Advances in Cryptology - ASIACRYPT 2008*, proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security (Melbourne), edited by J. P. Pieprzyk, Lecture Notes in Computer Science **5350**, Springer-Verlag, Berlin (2008), 390–405.
Available from http://www.springerlink.com/content/978-3-540-89254-0
35. H.-G. Quebbemann, *Zur Klassifikation unimodularer Gitter mit Isometrie von Primzahlordnung.* (German) [On the classification of unimodular lattices with an isometry of prime order]. J. Reine Angew. Math. **326** (1981), 158–170. Available from http://resolver.sub.uni-goettingen.de/purl?GDZPPN002198681
See also: ___ , *Unimodular lattices with isometries of large prime order. II.* Math. Nachr. **156** (1992), 219–224. See http://dx.doi.org/10.1002/mana.19921560114
36. H.-G. Quebbemann, *Atkin-Lehner eigenforms and strongly modular lattices.* Enseign. Math. (2) **43** (1997), no. 1-2, 55–65.
See http://retro.seals.ch/digbib/view?rid=ensmat-001:1997:43::263
37. E. M. Rains, *New asymptotic bounds for self-dual codes and lattices*, IEEE Trans. Inform. Theory **49** (2003), no. 5, 1261–1274.
Available from http://dx.doi.org/10.1109/TIT.2003.810623
38. C. P. Schnorr and M. Euchner, *Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems.* Math. Program. **66** (1994), 181–191.
Available from http://dx.doi.org/10.1007/BF01581144
39. C. P. Schnorr and H. H. Hörner, *Attacking the Chor-Rivest cryptosystem by improved lattice reduction.* In *Advances in Cryptology – EUROCRYPT 1995*, edited by G. Goos, J. Hartmanis, and J. van Leeuwen, Lecture Notes in Computer Science **921**, Springer-Verlag, Berlin (1995), 1–12.
Available from http://dx.doi.org/10.1007/3-540-49264-X_1
40. R. Schulze-Pillot, *Quadratic residue codes and cyclotomic lattices.* Arch. Math. (Basel) **60** (1993), no. 1, 40–45. See http://dx.doi.org/10.1007/BF01194237
41. B. Weisfeiler, *On the size of structure of finite linear groups.* Notes from 1984, Parts 1-17, A1-A10, totalling 91 typewritten and 63 handwritten pages.
Available from http://weisfeiler.com/boris/papers/papers.html
42. D. Zagier, *Elliptic modular forms and their applications.* In *The 1-2-3 of modular forms.* Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004. Edited by K. Ranestad, Universitext. Springer-Verlag, Berlin, 2008. x+266 pp.

A Appendix: proof that $\mathbf{M_{80}}$ and $\mathbf{N_{80}}$ are not isometric

We wish to show that $\mathbf{M}_{80}$ is not isometric to our lattice $\mathbf{N}_{80}$. Bachoc and Nebe list a subgroup of $\mathrm{Aut}(\mathbf{M}_{80})$ of order $2^{12}3^45^2$, while we have $S \cong \mathbf{SL}_2(\mathbf{F}_{79})$ as a subgroup of $\mathrm{Aut}(\mathbf{N}_{80})$. We wish to show that there is no finite matrix group in $\mathbf{GL}_{80}(\mathbf{Z})$ that is a supergroup of both of these (possibly after conjugation).

We let G be such a putative supergroup, and note that $[G : S] \geq 2^7 3^3 5$. From a classical theorem of Minkowski [29] on the modular reduction of matrix groups, we have injective maps $\iota_p : G \hookrightarrow \mathbf{GL}_{80}(\mathbf{F}_p)$ for all odd primes p. By

taking a gcd over all odd p this gives a bound of

$$\#G \mid 2^{198}3^{58}5^{24}7^{14}11^{8}13^{6}17^{5}19^{4}23^{3}29^{2}31^{2}37^{2}41^{2}\cdot 43\cdot 47\cdot 53\cdot 59\cdot 61\cdot 67\cdot 71\cdot 73\cdot 79,$$

though here we really only need such a divisibility result at a specific prime.[13]

We write $H = \iota_7\big(G \cap \mathbf{SL}_{80}(\mathbf{Z})\big)$, and since every matrix in $S \cong \mathbf{SL}_2(\mathbf{F}_{79})$ has determinant 1 we have $\iota_7(S) \subseteq H$. As every matrix in G has determinant ± 1, we get $[\iota_7(G) : H] \leq 2$, and since $[G : S] > 4$ and ι_7 is injective, this implies that $[H : \iota_7(S)] > 2$. The use of a theorem of Aschbacher (see below) now implies that $7^{780} \mid \#H$, which contradicts the above bound. Thus G cannot exist, and so $\mathbf{M}_{80}$ and $\mathbf{N}_{80}$ are not isometric. Indeed, this argument almost shows that S is maximal finite in $\mathbf{GL}_{80}(\mathbf{Z})$, though a low-index extension could still exist.

We now use Aschbacher's theorem [2] on maximal subgroups of finite classical groups (see also [23]). Let l be an odd prime (to be specified below) and suppose that $\iota_l(S) \subset H \subseteq \mathbf{SL}_{80}(\mathbf{F}_l)$. We note that S splits into a pair of conjugate absolutely irreducible unitary 40-dimensional representations defined over $\mathbf{Q}(\sqrt{-79})$.

We know that H lies in some maximal (proper) subgroup of $\mathbf{SL}_{80}(\mathbf{F}_l)$, and the theorem of Aschbacher lists the possibilities. For any inert prime l that does not divide $\#S$, we can eliminate class 1 of Aschbacher since $\iota_l(S)$ acts irreducibly (we could consider split primes also, but choosing an inert prime simplifies the argument slightly). Classes 2 and 4-7 are not possible simply because 79 must divide $\#H$. This leaves subgroups of class 3 (splitting as above) or class 8 (inclusions of classical groups), or class 9 (other simple groups, handled below). The inclusions of classical groups give us $\mathbf{G}_{80}(\mathbf{F}_l)$ for $\mathbf{G} = \mathbf{Sp}, \mathbf{SO}^{\pm}$ and $\mathbf{SU}_{40}(\mathbf{F}_l)$, while the splitting of class 3 yields $\mathbf{SL}_{40}(\mathbf{F}_{l^2}).2$. where the notation indicates that we have a 2-extension – in this case, we continue the analysis after replacing H by $H \cap \mathbf{SL}_{40}(\mathbf{F}_{l^2})$, where this subgroup has index at most 2 in H.

We iteratively apply Aschbacher's theorem to each classical group obtained; either H is isomorphic to this classical group, or is contained in a maximal subgroup of it. We again use $79|\#H$, and find that the only possible maximal subgroup of $\mathbf{Sp}_{80}(\mathbf{F}_l)$ that could contain H is $\mathbf{SU}_{40}(\mathbf{F}_l).2$, and similarly with the others. Any maximal subgroup chain of classical groups must end here, since H contains $\iota_l(S)$ and $S \to \mathbf{SU}_{40}(\mathbf{F}_l)$ is absolutely irreducible.

So we end in one of the following cases: H is isomorphic to one of

$$\mathbf{SU}_{40}(\mathbf{F}_l).\epsilon \text{ or } \mathbf{SL}_{40}(\mathbf{F}_{l^2}).\epsilon \text{ with } \epsilon = 1, 2, \text{ or } \mathbf{G}_{80}(\mathbf{F}_l) \text{ with } \mathbf{G} = \mathbf{Sp}, \mathbf{SO}^{\pm}, \mathbf{SL};$$

or $[H : \iota_l(S)] = 2$, in correspondence to a 2-extension as above; or (sometimes called "class 9" for Aschbacher) we have $\mathbf{PSL}_2(\mathbf{F}_{79}) \subset K \subset \mathbf{P}$, where K is simple and $\mathbf{P}$ is the associated simple group of one of the above classical groups.

There is sundry general knowledge for this latter situation, but for us a case-by-case analysis (with $l = 7$ for concreteness) using the known orders of the finite simple groups is sufficient to show that no such K can exist.[14] We conclude that either $[H : \iota_7(S)] = 2$, or that H contains a copy of $\mathbf{SU}_{40}(\mathbf{F}_7)$ and so $7^{780} \mid \#H$.

[13] We note in passing that the best upper bound on the size of a finite matrix group is due to Feit [10], relying on unpublished notes of Weisfeiler [41].

[14] One can also proceed via degrees of representations, and D. F. Holt indicated to us that the tables of Hiss and Malle [20] should suffice for this.