JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Mark WATKINS

Another 80-dimensional extremal lattice

Tome 24, nº 1 (2012), p. 237-255.

<http://jtnb.cedram.org/item?id=JTNB_2012__24_1_237_0>

Journal de Théorie des Nombres
de Bordeaux **24** (2012), 237-255

Another 80-dimensional extremal lattice

par Mark WATKINS

Résumé. Nous montrons que le réseau unimodulaire associé au groupe de matrices quaternioniques $\mathbf{SL}_2(\mathbf{F}_{41}) \otimes \tilde{S}_3 \subset \mathbf{GL}_{80}(\mathbf{Z})$ de rang 20 donne un quatrième exemple d'un réseau extrémal en dimension 80. Notre méthode utilise la positivié de la série Θ ainsi que l'énumération des vecteurs de norme 10. L'utilisation du théorème d'Aschbacher sur les sous-groupes de groupes finis classiques (qui dépend de la classification des groupes finis simples) permet de démontrer que ce réseau est différent des trois précédents. Une autre méthode est de calculer la distribution du produit scalaire des vecteurs minimaux. Cette dernière méthode nous permet également de déterminer complètement le groupe des automorphismes de ces quatre réseaux. Comme cela a déjà été noté par Nebe, ce quatrième réseau possède une 2-extension supplémentaire de son groupe d'automorphismes.

Abstract. We show that the unimodular lattice associated to the rank 20 quaternionic matrix group $\mathbf{SL}_2(\mathbf{F}_{41}) \otimes \tilde{S}_3 \subset \mathbf{GL}_{80}(\mathbf{Z})$ is a fourth example of an 80-dimensional extremal lattice. Our method is to use the positivity of the Θ-series in conjunction with an enumeration of all the norm 10 vectors. The use of Aschbacher's theorem on subgroups of finite classical groups (reliant on the classification of finite simple groups) provides one proof that this lattice is distinct from the previous three, while computing the inner product distribution of the minimal vectors is an alternative method. We give details of the latter, and this method also enables us to find the full automorphism group for each of the four lattices. As already noted by Nebe, this fourth lattice has an additional 2-extension in its automorphism group.

1. Introduction

Extremal unimodular lattices are of interest because they often have high packing densities and large kissing numbers. They can only exist in dimensions divisible by 8, the first example being E_8. Examples are known in each dimension up through 80, where three such lattices were known. In this dimension, being *extremal* means the smallest nonzero norm is 8.

Manuscrit reçu le 22 novembre 2010.

The topic of constructing extremal lattices has seen a recent surge in interest, in part due to Nebe's demonstration [25] of such a lattice in dimension 72, answering a question that had been open for some time (and indeed, various experts seemed to favour the opinion that such a lattice could not exist [8, p. 129, Remark]). Bachoc and Nebe [3] had previously constructed two extremal lattices in dimension 80, proving these were extremal using coding theory; and more recently Stehlé and the author [34] used a more computationally intensive method to show that the lattice associated to the (binary) extended quadratic residue code of length 80 is a third example in this dimension. We use techniques similar to those exposed in [34] to prove the extremality of a fourth lattice in this dimension. This lattice corresponds to the rank 20 quaternionic matrix group $\mathbf{SL}_2(\mathbf{F}_{41})\otimes\tilde{S}_3$ as constructed by Nebe in [22, §3], and in [22, Lemma 4.3(i)] it is noted that there is an additional 2-extension in the automorphism group.

1.1. Overview. Similar to the proof in [34], we show extremality by enumerating all the vectors of norm 10 and using the positivity of the Θ-series. We indicate various improvements over the methods used in [34], in particular those which allowed us to work with an automorphism group that does not have such a nice representation as with $\mathbf{SL}_2(\mathbf{F}_{79})$.

We can show our lattice is distinct from the other 3 extremal lattices in two different ways. The first is group-theoretical and is an exercise in applying Aschbacher's theorem [2]. On the advice of the referee we omit almost all the details herein. The second method is computational, as we compute the inner product distribution of the minimal vectors. We provide statistics about such inner product distributions for all 4 known 80-dimensional extremal lattices. Finally, we comment on some dimension 64 examples, and our failure to find any new extremal examples in dimension 48.

2. Our lattice

Our lattice L is given by Nebe [22, Remark 5.2] via a construction over the quaternion algebra $\mathcal{Q}_{\sqrt{41},\infty,\infty}$. There are two non-conjugate maximal orders, and the one of interest for us contains the maximal order of $\mathcal{Q}_{\infty,3}$,

Unwinding this notation, we find that it corresponds to writing one of the (complex-conjugate) 20-dimensional representations of $\mathbf{SL}_2(\mathbf{F}_{41})$ over a quaternion algebra, with the two possibilities being either the Hurwitz quaternions $\mathcal{Q}_{\infty,2}$, or our case of $\mathcal{Q}_{\infty,3}$. In either case we augment the automorphism group by the units of the quaternion ring, so $\tilde{S}_3$ for us.

2.1. A computation to realise L. Nebe gives one method for constructing L, namely by constructing a representation of a metacyclic group, and then solving norm equations in abelian fields (see [22, §3]). We chose to construct the lattice via a different, perhaps more circuitous route, via the representation theory and G-module functionality in Magma [6]. Instead of starting from $\mathbf{SL}_2(\mathbf{F}_{41})$ as in [22], we worked directly with the group $G = \mathbf{SL}_2(\mathbf{F}_{41}) \otimes \tilde{S}_3$, and considered the rational 80-dimensional representations of it.[1] In particular, we wrote $\mathbf{SL}_2(\mathbf{F}_{41})$ and $\tilde{S}_3$ as permutation groups, and took their direct product. We then computed the rational characters of degree 80, and limited ourselves to those with a kernel given by identifying the central -1 elements in the two groups. This left two characters, and as is noted in [22, §5], the representation we seek is reducible over the reals, so we reject the remaining irreducible character. We computed a $\mathbf{Q}G$-module that affords this character using the `GModule` command[2] of Magma [6], and found that there is indeed a 2-dimensional space of symmetric forms fixed by this matrix group. Writing f, g for a basis of these, the determinant of $fx + gy$ is of the form $q(x, y)^{40}$ for some homogeneous quadratic polynomial q (depending on f, g), and so we solved the conic $q(x, y) = 1$. With minimal effort we found a solution (x, y) which made $fx + gy$ integral, and this gives a Gram matrix of our lattice L.

An alternative method to construct L would be: take the sum of the two 20-dimensional characters of $\mathbf{SL}_2(\mathbf{F}_{41})$, and write the resulting representation in degree 20 over $\mathcal{Q}_{3,\infty}$ (one can take the "tensor product" of this with the degree 1 quaternionic representation of the faithful irreducible degree 2 character of $\tilde{S}_3$, but this is just the action of the units). However, it seems that the best way to do this is to first write the G-module in dimension 80 over $\mathbf{Z}$, and then find i, j in the endomorphism ring with $i^2 = -1, j^2 = -3, ij = -ji$ to realise the module over $\mathcal{Q}_{3,\infty}$. In either case, we get not only the relevant Gram matrix but also the action of G on it.

3. Proving L is extremal

We use the general method outlined in [34], which was adapted from an idea in [1], and indeed is essentially already in [20]. We first note that an even lattice has a Θ-series $\Theta(L) = \sum_{\vec{v}} q^{\vec{v}\cdot\vec{v}/2}$ that is a modular form, and for a unimodular lattice L of dimension 80 this has weight 40 and level 1. The space of such modular forms has dimension 4, and a basis is given by

$$\begin{aligned}
f_0 &= 1 + 1250172000q^4 + 7541401190400q^5 + O(q^6),\\
f_1 &= q + 19291168q^4 + 37956369150q^5 + O(q^6),\\
f_2 &= q^2 + 156024q^4 + 57085952q^5 + O(q^6),\\
f_3 &= q^3 + 168q^4 - 12636q^5 + O(q^6).
\end{aligned}$$

[1] The additional 2-extension was not considered for two reasons: firstly, while the construction of G is relatively straightforward, it was not clear to me how the additional extension could be appended; and secondly, it was only belatedly that I found out about this 2-extension anyway.

[2] This took about 15 minutes, but this could vary as the underlying methods are in flux.

The Θ-series of L is then given by $\Theta(L) = f_0 + a_1 f_1 + a_2 f_2 + a_3 f_3$ for some integers $a_i \geq 0$. A lattice is said to be *extremal* when all the a_i are zero. Indeed, in this case the minimal norm is as large as possible, and the Θ-series is given simply by the first element in the above basis. We show that $\Theta(L) = f_0$ by first showing that $a_1 = a_2 = 0$ via a brute-force search (relying on parallel enumeration code of Pujol [29]), which implies

$$\Theta(L) = f_0 + a_3 f_3 = 1 + a_3 q^3 + (\cdots)q^4 + (7541401190400 - 12636a_3)q^5 + O(q^6).$$

We then proceed to search for 7541401190400 vectors of norm 10, and upon finding this amount, will have shown extremality because positivity then implies that $a_3 = 0$. The capacity to find this many vectors depends on a number of factors. We find one representative in each orbit under the known automorphisms, but this still leaves about 18.6 million orbits to be found in our case. By a coupon-collecting analysis, this implies that a bit over 300 million "random" vectors of norm 10 will need to be found, and below we give two methods that are able to achieve this. The reason why we find vectors of norm 10 rather than search for norm 6 vectors directly is that the latter would need to be exhaustive, and there is no apparent way to exploit the automorphisms in such a search.

3.1. No vectors of norm 2 or 4. Unlike the case of [34, §5.1], we are not able to relate our lattice to a coding theory construction so as to eliminate the possibility of vectors of norm 2 or 4. However, after finding a sufficiently good basis for the lattice using block Korkine-Zolotareff (BKZ) reduction [32] (with a dimension parameter of about 30 — this is usually all that is useful, and takes less than 10 minutes), it only takes only a couple of cpu-months to do an exhaustive search, and parallel code for this is now available from Pujol [29] (described in [10], and see also [9]). Using 12 cpus and Pujol's code, it took about 4 days to show that our lattice has no vectors of norm 2 or 4. We had to make a slight modification to the code to allow an integral Gram matrix (rather than a basis) as the input.[3]

3.2. Vectors of norm 10 with nontrivial stabiliser. First we find all the vectors of norm 10 that have a nontrivial stabiliser. To do this, we compute the conjugacy classes of G, and then for each nontrivial conjugacy class, take a representative g of it and search for vectors in the sublattice fixed by g. We find that there are 140 nontrivial conjugacy classes, and the largest sublattice fixed by any of these is of dimension 40. We are able to find all vectors of norm up to 10 in such sublattices in about 15 minutes. For the orbits of vectors of norm 10, we find:

- 34342 orbits with stabiliser of size 2,
- 260 orbits with stabiliser of size 3,

[3] This induces minor changes in the error analysis [30] of the floating point computations.

- 56 orbits with stabiliser of size 6,
- 10 orbits with stabiliser of size 10.

See Section 3.4 for how to recognise orbits. Assuming the lattice is extremal, this leaves 18230412 free orbits to be found.

3.3. Finding vectors via pruning. As described in [34], the idea of pruning (perhaps first noted in [33, p. 195]) is to follow the standard enumeration technique of Kannan [16] or Fincke-Pohst [11], but to limit the search region to areas which are considered more likely to possess short vectors. Explicitly, using the standard notation for lattices (as found in e.g. [34, §6]), rather than solve the series of inequalities

$$\sum_{i=j}^{80} y_i^2 \|\vec{b}_i^\star\|^2 \leq 10 \quad \text{for all } 1 \leq j \leq 80,$$

we introduce a pruning array $P_j = 1 - \frac{(j-1)}{80}$ and solve

$$\sum_{i=j}^{80} y_i^2 \|\vec{b}_i^\star\|^2 \leq 10 \cdot P_j \quad \text{for all } 1 \leq j \leq 80.$$

To describe this loosely, this ensures that any initial segment of the coordinates does not take up more than its "fair share" of the available norm.

The first step in any lattice-searching method is to obtain a good basis. Here LLL [18] by itself is not completely satisfactory, but after applying BKZ [32] with a dimension parameter of 30, we have a reasonable basis. We would run the pruned-enumeration code for 100 seconds on a given basis, before making a perturbation of it as in [34]. With the above choice of P_j we obtained about 400 norm 10 vectors per cpu-second using the Magma implementation of Stehlé.

Recent work appearing in [12, Appendix D] has improved the tree traversal process; while we do not have exact timings, a guess is that it would be 30-40% faster at the cost of increasing the memory usage slightly.

3.3.1. *An alternative method to find vectors of norm 10.* As noted in [1], an alternative method to try to find vectors of norm 10 is to take random pairs of (known) norm 8 vectors, hoping that their inner product is of size 3.

We do not have a complete analysis of this method, but can note that the primary step will be the computation of an inner product. Done in the most obvious manner, this would take about 80^2 multiply-and-adds; but by (say) first diagonalising the Gram matrix over the reals, we are able to reduce the calculation to 80 such operations. The distribution given in Section 4 indicates that a random inner product between two vectors of norm 8 will have about a 1-in-380 chance of having size 3. We can thus achieve about 10000 norm 10 vectors per cpu-second, which is notably faster than the pruning techniques. However, see Section 6.2 below for some difficulties with this method.

3.4. Recognising orbits. One difficulty in mimicking the strategy of [34] for our lattice L is that it is not so clear how to find orbit representatives as easily as with $\mathbf{SL}_2(\mathbf{F}_{79})$ (for which there is a doubly transitive action of signed permutations on the coordinates). We overcome many of the difficulties by noting that an orbit can be recognised via a baby-steps giant-steps technique involving subgroups (or even subsets). Indeed, suppose we have two vectors $\vec{v}$ and $\vec{w}$ in the same orbit, so that $\vec{v}g = \vec{w}$ for some element $g \in G$. We assume that we have G written as BA, where in practise this decomposition will be exact with A a subgroup and B just representatives of the cosets of A. Then we have $\vec{v}ba = \vec{w}$ for some elements $a \in A$, $b \in B$, and so by comparing $\vec{v}B$ with $\vec{w}A$ we will detect whether $\vec{v}$ and $\vec{w}$ are in the same orbit.

In our case, we take A to be a subgroup of size 820 in G, and further mod out by $-1 \in A$. This means that the set B is of size 504. For every vector $\vec{v}$ we find, we compute $\vec{v}b$ for each $b \in B$ and use a hash table to detect if it is the same as any $\vec{w}a$ that was seen previously. If so, then we have already counted this orbit. If not, we compute $\vec{v}A$ and store these vectors (we can also compute the stabiliser of $\vec{v}$ at this step from $\vec{v}A$ and $\vec{v}B$).

3.4.1. ***A minor generalisation.*** This method could be generalised to handle the case of sets A, B such that BA^{-1} as a set covers G, and so even in a case where there are no subgroups of useful size, one can still choose A and B of size about $\sqrt{\#G \log \#G}$ if desired. We can note that the expected time to find V vectors under an automorphism group G is thus roughly proportional to $V \log V/\sqrt{\#G}$.

3.4.2. ***Computational data.*** We chose a subgroup A of size 820 in G and so $\#B = 504$, with $-1 \in A$ reducing computations by a factor of 2. For each vector $\vec{v} \in L$ that we find, the computation of the set $\vec{v}B$ will take about $504 \cdot 80^2 \sim 3.22 \cdot 10^6$ multiply-and-add operations. We can stop computing $\vec{v}B$ immediately when we run across a saved $\vec{w}A$ vector, and this saves a factor of about two on average when an orbit is already known.

When we find a new orbit we compute $\vec{v}A$, which again requires around 3 million multiply-and-add operations. We save each vector in $\vec{v}A$ as a 64-bit hash – in the worst case we could erroneously regard two distinct orbits as equivalent (in which case we should just find this orbit later), but this hash will never incorrectly claim that a previously seen orbit is new.

Even with this hashing, we still need a storage space of $18265080 \cdot 410 \cdot 8$ bytes, or about 64 gigabytes. We chose A of the given size to push the memory limits as much as we could, so that the time to compute the $\vec{v}B$

would be as small as possible. It turns out that we can process nearly 200 vectors per cpu-second, and so distinguishing the orbits of 305 million vectors takes about 3 cpu-weeks.

We can check our proof in less time than it took in the first place, as we only need run through 18.6 million vectors rather than 305 million. We provide code[4] that can check that our list does indeed provide 7541401190400 distinct vectors of norm 10, but this still requires around 3 cpu-days (we ran it on 10 cpus in 7 hours) and 64GB of memory.

4. Inner product distributions

We are able to analyse the inner product distribution of the minimal vectors by weighting with respect to Gegenbauer polynomials (see [35], or [4, §4-5]). Given an extremal 80-dimensional lattice, for any fixed $\vec{w}$ with norm 8 and any $d = 1, 2, 3$ (and also $d = 5$, though it gives no new information in dimension 80), we have that

$$\sum_{\|\vec{v}\|=8} G_{2d}\left(\frac{\vec{v}\cdot\vec{w}}{8}\right) = 0$$

where the G_{2d} are related to the Gegenbauer polynomials. This is a special case of the more general fact that for any fixed nonzero $\vec{w}$ and positive integer d, the sum

$$\sum_{\vec{v}\neq 0} G_{2d}\left(\frac{\vec{v}\cdot\vec{w}}{\sqrt{\|\vec{v}\|\,\|\vec{w}\|}}\right) q^{\vec{v}\cdot\vec{v}/2}$$

is a modular form, and extremality forces some of the coefficients to vanish.[5]

Explicitly, in the case of dimension 80 we have $\frac{1}{(1-2xt+t^2)^{39}} = \sum_k G_k(x)t^k$, so that

$$G_2(x) = 760x^2 - 19,\ \ G_4(x) = 117040x^4 - 15960x^2 + 190,$$
$$\text{and}\ \ G_6(x) = 8614144x^6 - 2691920x^4 + 175560x^2 - 1330.$$

Furthermore, the signs of the $\vec{v}\cdot\vec{w}$ are equi-distributed, and except for the cases when $\vec{v} = \pm\vec{w}$, we have $|\vec{v}\cdot\vec{w}| \le 4$. We have 5 unknowns, namely the number b_i of vectors $\vec{v}$ with $\vec{v}\cdot\vec{w} = i$ for $i = 0\ldots 4$, and 4 linear equations, given by the three above for $d = 1, 2, 3$ plus the accounting

$$b_0 + 2(b_1 + b_2 + b_3 + b_4) = 1250172000 - 2,$$

where this comes from noting that an extremal lattice in dimension 80 has 1250172000 vectors of norm 8. We solve these and get

$$b_0 = 2(35y + 275885775),\ \ b_1 = 301716800 - 56y,$$

[4] This is available from `http://magma.maths.usyd.edu.au/~watkins/sl241dim80.tar.bz2`

[5] There is a slight reworking of this for extremal lattices in dimensions $24k$ and $24k+16$, where in the first case we get vanishing for $d = 1, 2, 3, 4, 5, 7$, and in the latter case only for $d = 1, 3$.

$$b_2 = 28y + 45799776,\ \ b_3 = 1683648 - 8y,\ \ b_4 = y,$$

for some integer y with $0 \le y \le 210456$. We do not know if the parameter y can be related to a type of "Nachbareffekt" as in [4, §5, Example 1]. Unlike for the case of dimension 32, with extremal lattices of dimension 80 the Siegel modular form given by

$$\Theta_2(L) = \sum_{\vec{v}\in L}\sum_{\vec{w}\in L} q_{1,1}^{\vec{v}\cdot\vec{v}/2} \cdot\ q_{1,2}^{\vec{v}\cdot\vec{w}} \cdot q_{2,2}^{\vec{w}\cdot\vec{w}/2}$$

is not uniquely determined (see [27]), with the indeterminate factor being a multiple of χ_{10}^4.

Below we shall use the computation of the inner product distributions as one of the methods to show that our lattice L is not isometric to any of the previously known extremal lattices in dimension 80. None of the material in this section is strictly necessary for that, but we provide it for context.

5. Computational results

5.1. Minimal vectors. The vectors of norm 8 in the lattice L split as follows under the known automorphism group $G = \mathbf{SL}_2(\mathbf{F}_{41}) \otimes \tilde{S}_3$:

- 2788 orbits with trivial stabiliser,
- 464 orbits with stabiliser of size 2,
- 8 orbits with stabiliser of size 3,
- 14 orbits with stabiliser of size 6.

As there are 3274 orbits and 1250172000/2 minimal vectors up to sign, we need to compute about 2 trillion inner products to find the complete distribution. Each inner product can be computed in 80 multiply-and-adds upon switching the minimal vectors to a basis (over $\mathbf{R}$) in which the Gram matrix is diagonal. Our code ran in about 4 cpu-days.

Using the notation of the previous section, for each vector $\vec{v}$ we write y for the number of vectors that have inner product 4 with it. This value is preserved by automorphisms, and so is constant for all vectors in the same orbit. We find that the smallest y-value is 8092 (obtained for 2 free orbits), while the largest is 9220 (obtained for 4 orbits, all of stabiliser of size 6). The average is slightly above 8574. Each y-value appears in our data an even number of times; this is to be expected due to the 2-extension of G that is noted in [22, Lemma 4.3(i)]. Via a slight modification of the methods given in Section 5.3 below, we are able to determine the complete automorphism group $G^+ \cong (\mathbf{SL}_2(\mathbf{F}_{41}) \circ \tilde{S}_3).2$ with $[G^+ : G] = 2$. The 80-dimensional representation of G^+ corresponding to L is absolutely irreducible. We can also note that the matrix group $G^+ \subset \mathbf{SL}_{80}(\mathbf{Z})$ is uniform, that is, it fixes a unique symmetric form (up to scalars), unlike G for which the space of symmetric fixed forms has dimension 2 (see [22, §5]).

5.2. Comparison to other lattices. We can make the same computation with the other known 80-dimensional extremal lattices. For the Bachoc-Nebe lattice with automorphism group $2.M_{22}.2 \otimes 2.A_7$, there are 10 orbits, and we compute the following data:

- an orbit with stabiliser of size 6 and $y = 8728$,
- an orbit with stabiliser of size 16 and $y = 9400$,
- an orbit with stabiliser of size 48 and $y = 9688$,
- an orbit with stabiliser of size 96 and $y = 8728$ (as above),
- an orbit with stabiliser of size 112 and $y = 13336$,
- an orbit with stabiliser of size 192 and $y = 14872$,
- an orbit with stabiliser of size 384 and $y = 12184$,
- an orbit with stabiliser of size 432 and $y = 8248$,
- an orbit with stabiliser of size 8064 and $y = 24088$,
- and an orbit with stabiliser of size 24192 and $y = 15256$.

As can be seen, the average of the y-value is a bit over 9247.

For the second Bachoc-Nebe lattice [3, Lemma 4.11], the known automorphism group of size $2^{12}3^4 5^2$ yields 333 orbits. The smallest y-value is 8268 (from a free orbit), and the largest is 24088 (the same as in the above data), coming from three orbits whose stabilisers are of sizes 288, 384, and 576. The second largest y-value is 17944, from an orbit with stabiliser of size 96. We find that the average y-value is a little above 8855. All of the y-values are divisible by 4.

Finally, for the lattice proven extremal in [34] with known automorphism group $\mathbf{SL}_2(\mathbf{F}_{79})$, there are 2555 minimal orbits, with a minimal y-value of 8048, a maximum of 9406, and an average of nearly 8537.

This gives one proof that the four lattices are all distinct up to isometry. The complete data for the inner products are included in the download from the address given in Footnote 4.

5.3. Maximality of automorphism groups. We can also use the above y-value distributions to show in each case that the known automorphism group is the full automorphism group. The idea is simple.[6] We assume that σ is an unknown automorphism and that we know the images of the vectors $\vec{v}_i \in S$ under σ. Then we use the fact that σ preserves inner products. We will either show that the set of images is inconsistent, or that σ fixes all the vectors in S. In the latter case, when S is so large that it generates the lattice, we conclude that σ fixes every vector, and so must be the identity.

The only difficulty is in getting a large enough set S of vectors for which we know the image. Here is a probabilistic argument on what we might expect. First we take an orbit whose y-value is unique, and choose a vector $\vec{v}$

[6] It is also well-known — see [28] for improvements that can be applied in more difficult cases.

in it. We know that σ must map this orbit to itself, and so $\vec{v}\sigma = \vec{w}$ for some $\vec{w}$ in the orbit. There is also some known g such that $\vec{v}g = \vec{w}$. Thus by considering $g\sigma^{-1}$, we can assume that $\vec{v}$ is fixed by a new automorphism.

This gives us one fixed vector $\vec{v}$. We then use the rarity of vectors with inner product 4 to break up the current orbit classes. For instance, in the case of our lattice L, we can take $y = 8048$ and expect each of the 2528 free orbits to have maybe 3 or 4 vectors whose inner product with $\vec{v}$ is 4. In particular, this should be true for orbits whose y-value is unique (including $y = 8048$). Then we iterate through each of these possible image vectors, seeing if it can preserve inner products. We have no control over inner products except the first, but each additional member of S should only give approximately a 1/4 chance of having a matching inner product. Thus once S has more than just a few elements, there is little chance that we will accidentally get the inner products to match.

5.3.1. *Results for the four lattices.* The automorphism group for the first Bachoc-Nebe automorphism group was proven maximal in [3, Theorem 3.2].

Their second lattice has 81 free orbits under the known automorphism group, and 22 of them have unique y-values ($y = 8268, 8292, \ldots, 8852$). This is the toughest case for our procedure, as a given free orbit would typically have about 30 vectors of inner product 4 with our initial fixed vector. However, we can exploit the classes with unique y-value and non-trivial stabiliser in this case. In particular, if the stabiliser is of size about 30, there is a decent chance of obtaining a unique vector of inner product 4. For instance, given a vector $\vec{v}$ with $y = 8268$, there is a unique vector with each $y \in \{9808, 9976, 16152\}$ whose inner product with $\vec{v}$ is 4. The stabilisers here are respectively of sizes 36, 24, and 32. This then gives us 4 fixed vectors, and the process is fairly mechanical after that. For instance, the vectors with $y = 8272$ (stabiliser of size 6) which have inner product 4 with $\vec{v}$ then split, giving us 7 new fixed vectors, then $y = 8292$ gives 56 more, and so on. We conclude that the group listed by Bachoc and Nebe is indeed the full automorphism group.

The extremal lattice associated to the length 80 extended quadratic residue code has 2528 free orbits of which 51 have a unique y-value. Fixing a vector with $y = 8048$, there is a unique vector with inner product 4 in each of the $y = 8120, 8126, 8130$ classes (and indeed with some other classes). These four vectors then yield three more with $y = 8154$, and in this manner we quickly generate the whole lattice. Thus we conclude that $\mathbf{SL}_2(\mathbf{F}_{79})$ is the full automorphism group.

As noted above, for the new extremal lattice L we first need to find the 2-extension G^+. This is expedited by taking a y-value with exactly 2 orbits under G, and (as above) composing with a known automorphism to get that a specific vector $\vec{v}$ in one of them maps to a specific vector $\vec{w}$ in the other. Then we proceed as above, enlarging the set S until we have definite images for a set S that generates L; this then gives us an automorphism of the lattice that was not previously known. Upon finding this 2-extension, we then prove it is the full automorphism group in the same manner as above. For instance, a fixed vector in the $y = 8092$ class yields a unique vector with inner product 4 in both the $y = 8098$ and $y = 8138$ classes, which then split the four such vectors with $y = 8180$, etc.

5.4. Another proof that L is not isometric to the known lattices. We could give a second proof of the non-isometry of L with the previously known lattices via the Classification of Finite Simple Groups by imitating and expanding/correcting the appendix of [34], As the above argument from inner-product distributions suffices, on the advice of the referee we omit almost all of the details herein. The problem is that we need to rule out the possibility of a finite matrix group M in $\mathbf{GL}_{80}(\mathbf{Z})$ that contains both a copy of G and a copy of one of the other groups.

We take a suitable prime $p = 101$ and by Minkowski's theorem [21] inject M into $\mathbf{GL}_{80}(\mathbf{F}_p)$. The use of Aschbacher's theorem on maximal subgroups [2, 17] of finite classical groups gives an iterative framework for inclusions of M. For instance, a class 3 reduction gives that $M \subseteq \mathbf{\Gamma L}_{40}(\mathbf{F}_{p^2})$, and a consideration of normal subgroups allows one to remove the semi-linear part and iteratively consider maximal subgroups of $\mathbf{GL}_{40}(\mathbf{F}_{p^2})$. To exclude possible class 9 inclusions $M \subset K \subset \mathbf{GL}_d(\mathbf{F}_{p^r})$ with K quasi-simple, we note that $\mathbf{SL}_2(\mathbf{F}_{41}) \subset G \subset M$, and that $\mathbf{SL}_2(\mathbf{F}_{41})$ has an absolutely irreducible 20-dimensional representation. This implies $20|d$ and $d|80$, whence we can apply the tables in [15] and [19].

The end result is that every subgroup of $\mathbf{GL}_{80}(\mathbf{F}_p)$ that contains both a copy of G and of one of the other groups must itself be a classical group; ergo, $p = 101$ divides the order, and this contradicts the Minkowski bound [21] for the image of a finite matrix group of degree 80.

6. Extremal lattices in dimension 64

We were able to construct a new extremal lattice of dimension 64 as follows. Writing $K = \mathbf{Q}(\sqrt{-11})$ and letting $w = \frac{-1+\sqrt{-11}}{2}$, we used the unimodular matrix $M_2 = \begin{pmatrix} 2 & w \\ \bar{w} & 2 \end{pmatrix}$ and took the tensor product (over K) of it with each of Hentschel's six ϑ-lattices [14] of rank 8 over $\mathbf{Q}(\sqrt{-11})$. Upon expanding to a basis over $\mathbf{Q}$, four of these six yielded extremal lattices of dimension 32. We then took a few "random" neighbours of these 16-dimensional lattices over K, and again tensored these with M_2. One of these, namely a $(5 + 4w)$-neighbour of $M_2 \otimes H_3$ where H_3 is the third of Hentschel's ϑ-lattices, upon expanding the basis to $\mathbf{Q}$ yielded a

64-dimensional lattice with minimum 6. It took only about 40 cpu-minutes for an exhaustive search (after a suitable BKZ reduction) to show that the lattice had no vectors of minimum 4. The Hermitian automorphism group of the 32-dimensional K-lattice is isomorphic to the dihedral group D_6 on six symbols (which is already that for M_2).

Remark 6.0.1. *In some metric, this is the "best possible" case for doing such tensor products, as extremal lattices are thought to be more common in dimensions* $(24k + 16)$ *than in dimension* $24k$*. The fact that the lattice has minimal automorphisms is perhaps uninteresting from the standpoint of group theory, but does show that the behaviour is "generic" in a suitable sense. Also, the rank 16 lattice over* K *we first constructed is computationally tricky to handle. For instance, it takes a couple of hours to compute the automorphism group. As already noted in* [28]*, computing isometries in dimension 32 is somewhat difficult, due to the large number of extremal lattices (and a lack of easily computed invariants for isometry).*

6.1. Comparison to known extremal lattices in dimension 64. The first known extremal lattice in dimension 64 was constructed by Quebbemann [31]. As noted in [7, §8], the construction can be modified in various ways, and it not exactly clear how many non-isometric lattices can be produced. We have chosen to ignore these lattices for our discussion here.

A second extremal lattice T_{64} in dimension 64 was constructed from coding theory by Ozeki [26] (see also [13]). Finally, using an anti-identification of two maximal orders of associated quaternionic endomorphism rings, Nebe [22, Remark 5.2] constructed a (unimodular) lattice N_{64} with automorphism group containing $(\mathbf{SL}_2(\mathbf{F}_{17}) \circ \mathbf{SL}_2(\mathbf{F}_5)).2^2$, where the factors in the central product correspond respectively to quaternionic representations of degree 8 and 2. This was later proven to be extremal in [24].

In order to show the lattice constructed here differs from N_{64} and T_{64}, we can proceed by computing inner product distributions. As in Section 4, we can compute that for a given vector $\vec{v}$ of norm 6, there is some integer t with $0 \le t \le 17826$ such that the distribution of inner products is:

- $2(26t + 680792)$ vectors $\vec{w}$ with $\vec{v} \cdot \vec{w} = 0$,
- $-33t + 588288$ vectors $\vec{w}$ with $\vec{v} \cdot \vec{w} = 1$,
- $6t + 36519$ vectors $\vec{w}$ with $\vec{v} \cdot \vec{w} = 2$,
- t vectors $\vec{w}$ with $\vec{v} \cdot \vec{w} = 3$,
- 1 vector $\vec{w}$ with $\vec{v} \cdot \vec{w} = 6$.

6.1.1. ***Nebe's lattice.*** With Nebe's lattice N_{64}, there are 8 orbits of the 2611200 minimal vectors (under the automorphism group of order 1175040), divided as:

- an orbit with stabiliser of size 2 and $t = 254$,
- an orbit with stabiliser of size 2 and $t = 284$,

- an orbit with stabiliser of size 2 and $t = 318$,
- an orbit with stabiliser of size 4 and $t = 336$,
- an orbit with stabiliser of size 4 and $t = 344$,
- an orbit with stabiliser of size 12 and $t = 272$,
- an orbit with stabiliser of size 12 and $t = 452$,
- and an orbit with stabiliser of size 18 and $t = 218$.

As can be seen, the average t-value is $301\frac{7}{10}$.

6.1.2. ***Ozeki's lattice.*** In order to find the minimal vectors for Ozeki's lattice T_{64}, we used the method for the generic lattice given in Section 6.2 below, as it was not completely obvious whether there would be nontrivial automorphisms.[7] However, it turns out that the automorphism group for T_{64} is isomorphic to the 2-extension of $\mathbf{SL}_2(\mathbf{F}_{31})$ that is given by $2 \cdot \mathbf{Aut}(\mathbf{PSL}_2(\mathbf{F}_{31}))$; this can be computed in a few minutes with the Magma command `AutomorphismGroup` (due to W. R. Unger) once the minimal vectors are known.

There are 41 free orbits, six with a stabiliser of size 3, three with a stabiliser of size 5, four with a stabiliser of size 15, and two with a stabiliser of size 465. There are 36 distinct t-values, ranging from 158 to 308 with an average around 222.6 and a most common value of 206. See Table 6.1 for more complete data, which gives orbit counts weighted by automorphisms.

TABLE 6.1. t-distribution for Ozeki's lattice T_{64}

158	$\frac{1}{3}$	198	1	214	1	228	3	244	$1+\frac{1}{5}$	258	1
174	$\frac{1}{5}$	200	$2+\frac{1}{3}$	216	1	230	$\frac{1}{3}$	246	2	272	1
184	1	206	5	218	3	234	1	248	$\frac{2}{15}+\frac{2}{465}$	278	$\frac{1}{15}$
188	$\frac{1}{3}$	208	3	220	2	236	1	252	1	280	1
190	1	210	1	222	1	240	1	254	1	294	$\frac{1}{5}$
194	1	212	1	224	$2+\frac{1}{3}$	242	$\frac{1}{3}$	256	1	308	$\frac{1}{15}$

6.1.3. ***The new lattice.*** The new lattice H_{64} has 217600 orbits (each with trivial stabiliser), and to show its distinctness we can simply note that it has (say) a minimal vector with $t = 124$. Indeed, we found all the minimal vectors via the search strategy given in Sections 3.3 and 3.3.1, and computed the complete inner product distribution. All the t-values are even, the minimum is 124, the maximum is 304, the average is just over 214, and the most common value (8530 orbits) is 210. See Table 6.2 for the complete distribution.

[7]For instance, the $\mathbf{F}_3$ reduction of the original $\mathbf{Z}_6$ code has C_4 as its automorphism group.

Table 6.2. t-distribution for Hermitian H_{64}

124	2	162	274	192	4991	222	7691	252	1469	282	46
126	1	164	375	194	5315	224	7348	254	1276	284	30
136	3	166	461	196	5871	226	6937	256	1095	286	28
138	2	168	626	198	6460	228	6559	258	884	288	17
140	2	170	787	200	6980	230	6074	260	730	290	19
142	4	172	969	202	7452	232	5675	262	590	292	7
144	21	174	1234	204	7694	234	5125	264	505	294	12
146	13	176	1445	206	8087	236	4737	266	376	296	8
148	26	178	1760	208	8332	238	4235	268	271	298	7
150	42	180	2121	210	8530	240	3583	270	217	300	3
152	48	182	2486	212	8476	242	3214	272	165	302	1
154	85	184	2920	214	8513	244	2765	274	123		
156	110	186	3363	216	8494	246	2398	276	110		
158	171	188	3898	218	8245	248	2106	278	90		
160	210	190	4289	220	7964	250	1857	280	65		

6.2. Another extremal lattice in dimension 64. We were also able to find a generic (with only the trivial automorphisms) extremal lattice G_{64} in dimension 64 via more neighbouring. We started with the new extremal lattice of above, and then took random neighbours (over $\mathbf{Q}$). After some effort, this succeeded. One difficulty is that many of the obtained lattices had a vector of norm 4, but this was only detected near the end of the search, after taking over an hour in some instances. However, it still took less than 10 cpu-hours to find one which turned out to be extremal.

We then turned to the listing of minimal vectors. As there are no known nontrivial automorphisms, we need to find 1305600 vectors of norm 6. The method of Section 3.3.1 above showed a few problems for this lattice. The idea is to start with a collection of norm 6 vectors, and then expand this collection via looking for pairs in it that have an inner product of size 3. From the above analysis, there is presumably around a 1/6000 chance of this happening for a random pair. At the outset, we thus need a sufficiently large "seeding" set. For instance, 1000 vectors is probably not enough, as they would only produce about $\binom{1000}{2}/6000 \approx 80$ new vectors of norm 6, and we would quickly reach a state where no new norm 6 vectors could be obtained from the current set. We used a pruning-based method as in Section 3.3 in order to start with enough vectors so as to circumvent this.

However, we can still run into problems later on. In our actual run, we hit a wall at 686824 vectors, and so returned to the device of making various perturbations of the basis, followed by reduction and pruning-based enumeration. Note that such a difficulty is much less likely to occur in a case where automorphisms are extant, as applying them to known vectors is an alternative method to generate additional vectors of norm 6.

Finally, it not altogether clear that the method of Section 3.3.1 is really faster for our 64-dimensional lattices, as we could often find more norm 6 vectors per second using the pruning method when a sufficiently sharp choice for the pruning function was used (the exact yield also depends upon the goodness of the BKZ-basis).

After obtaining all the minimal vectors, we then computed the inner product distribution, which is given in Table 6.3. As can be seen, the average t-value is slightly less than 212. When comparing to the previous table, recall that the numbers in Table 6.2 should be multiplied by 6 to account for the known automorphisms.

TABLE 6.3. t-distribution for generic G_{64}

124	1	158	757	190	28683	222	47073	254	4668	286	47
128	1	160	986	192	32565	224	44255	256	3866	288	24
130	1	162	1436	194	35707	226	40988	258	2997	290	14
132	3	164	1833	196	39516	228	37526	260	2306	292	13
134	6	166	2617	198	42830	230	33999	262	1796	294	9
136	4	168	3273	200	46093	232	30787	264	1415	296	6
138	14	170	4313	202	49257	234	27068	266	1118	298	2
140	21	172	5569	204	51197	236	24176	268	769	300	2
142	33	174	6981	206	53101	238	20569	270	594	302	2
144	46	176	8730	208	54441	240	17922	272	466	304	3
146	82	178	10804	210	55288	242	15290	274	311	306	1
148	112	180	13023	212	55679	244	13229	276	243	308	1
150	175	182	15729	214	54915	246	10955	278	174		
152	263	184	18774	216	53687	248	8858	280	121		
154	382	186	21722	218	52355	250	7340	282	89		
156	474	188	25170	220	49973	252	5825	284	61		

For each of these lattices we are able to show that the known automorphism group is complete using the method of Section 5.3.

6.3. Tensor products from quaternionic 32-dimensional lattices. The list given by Nebe [23, Theorem 18.1] contains two 32-dimensional lattices that have a quaternionic structure into which we can embed $\mathbf{Q}(\sqrt{-11})$. The first one is $L_{32} = [2_-^{1+8}.\mathbf{O}_8^-(2)]_8$, and upon tensoring with M_2, the resulting $\mathbf{Q}$-lattice splits into two copies of the $\mathbf{Q}$-expansion of L_{32}. The other compatible quaternionic lattice is $[\mathbf{SL}_2(17).2]_8$, which when tensored with M_2 gives Nebe's lattice N_{64}.

7. Sundry

7.1. No new extremal lattices of dimension 48. We were unable to find any new extremal lattices of dimension 48 via such methods. One attempt was made via $\mathfrak{p}_3$-neighbour computations starting with a rank 12 Hermitian matrix over $\mathbf{Q}(\sqrt{-2})$. It is difficult to tell how many lattices we stepped through, as we did not check isometry but at best merely counted the number of norm 4 vectors upon tensoring with the unimodular matrix $M_2' = \begin{pmatrix} 2 & 1+\sqrt{-2} \\ 1-\sqrt{-2} & 2 \end{pmatrix}$ and expanding to a $\mathbf{Q}$-basis, though it seems that we looked at hundreds or even thousands of such examples. The "typical" resulting 48-dimensional lattice had approximately 3000 pairs of vectors of norm 4.

The only 48-dimensional extremal lattice that was found was a lattice whose Hermitian automorphism group was $\mathbf{SL}_2(\mathbf{F}_{13})$, presumably inherited from a quaternionic structure over $\mathbf{Q}(\sqrt{13})$ ramified at the two infinite places; given that M_2' has $\mathbf{GL}_2(\mathbf{F}_3)$ as its automorphism group, it seems likely that our lattice is isometric to the one already found by Nebe [22]. The arrangement is similar over $\mathbf{Q}(\sqrt{-11})$.

Additionally, in each case, any other quaternionic structure on the Leech lattice Λ_{24} which descends to the imaginary quadratic field will yield two copies of Λ_{24} upon tensoring with M_2' and expanding to a $\mathbf{Q}$-basis. It is notable that while our "random neighbouring" on Hermitian lattices would produce lattices with typically around 3000 pairs of vectors of norm 4, the quaternionic structures induced the extremes: namely, 196560 pairs of norm 4 vectors when it splits as $\Lambda_{24} \oplus \Lambda_{24}$; or zero when the lattice is extremal. The second largest number of pairs of norm 4 vectors we found was 30672 (and indeed comes from a neighbour of the quaternionic basis that induces $\Lambda_{24} \oplus \Lambda_{24}$).

7.2. Further directions. It seems possible to compute the inner product distribution of the minimal vectors for Nebe's extremal lattice [25] of dimension 72, though we have not done so. There are about 5 times as many minimal vectors as with an extremal lattice of dimension 80, but the known automorphism group has more than 10 times as many elements as G does. Via this, we could presumably show that $\big(\mathbf{PSL}_2(\mathbf{F}_7) \times \mathbf{SL}_2(\mathbf{F}_{25})\big) : 2$ is the full automorphism group.

The use of neighbouring to find extremal lattices in dimension 56 could also be investigated. We could either start with an arbitrary even unimodular lattice in this dimension,[8] or we could take a (possibly decomposable)

[8] There is no particular reason to start with an extremal lattice; four are known (to me) in this dimension, namely $B^{(4)}_{56,1}$ in [5], T_{56} from [26], and $L_{56,2}(\mathcal{M})$ and $L_{56,2}(\tilde{\mathcal{M}})$ in [22, Table I], though I do not know if anyone has verified these are all distinct.

rank 28 ϑ-lattice over some imaginary quadratic field, and do neighbouring in this field.

Finally, there are two lattices in dimension 80 given at the end of [5] which remain candidates for extremality, namely $B_{80,1}^{(4)}$ and $B_{80,1}^{(5)}$. As the automorphism group (of either lattice) presumably only has 6560 elements, the methods used here do not seem to be readily applicable.

8. Acknowledgments

The present work is part of the Australian Research Council Discovery Project DP0880724 "Integral lattices and their theta series". The author thanks W. R. Unger for help with simple groups, A. K. Steel for aid with G-modules in Magma, X.-F. Roblot for French translations, and X. Pujol for the parallel enumeration code. Computer hardware obtained under National Science Foundation Grant No. DMS-0821725 (W. A. Stein) was also used. The author visited the Tokyo Institute of Technology during part of the period in which this research took place, and was supported therein in part by the Global COE grant *Computationism as a Foundation for the Sciences.*

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. Available from `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. Bachoc, B. Venkov, *Modular forms, lattices and spherical designs.* In *Réseaux euclidiens, designs sphériques et formes modulaires. Autour des travaux de Boris Venkov.* Edited by J. Martinet, Monogr. Enseign. Math., **37**, Enseignement Math., Geneva (2001), 87–111.

[5] 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`

[6] 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 (London 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`

[7] J. H. Conway, N. J. A. Sloane, *Sphere packings, lattices and groups.* With contributions by E. Bannai, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], **290**. Springer-Verlag, New York, 1988. xxviii+663pp.

[8] R. Coulangeon, *Tensor products of Hermitian lattices.* Acta Arith. **XCII**, no. 2 (2000), 115–130. Online at `http://matwbn.icm.edu.pl/ksiazki/aa/aa92/aa9224.pdf`

[9] Ö. Dagdelen, M. Schneider, *Parallel Enumeration of Shortest Lattice Vector.* In *Proceedings of EURO-PAR 2010* (Ischia 2010), Part II. Edited by P. D'Ambra, M. R. Guarracino, and D. Talia, Lecture Notes in Computer Science **6272**, Springer (2010), 211–222. Available from `http://dx.doi.org/10.1007/978-3-642-15291-7_21`

[10] J. Detrey, G. Hanrot, X. Pujol, D. Stehlé, *Accelerating Lattice Reduction with FPGAs.* In *Progress in Cryptology - LATINCRYPT 2010*, Proceedings of the First International

Conference on Cryptology and Information Security in Latin America (Puebla 2010). Edited by M. Abdalla and P. S. L. M. Barretto, Lecture Notes in Computer Science **6212**, Springer (2010), 124–143. Available from `http://dx.doi.org/10.1007/978-3-642-14712-8_8`

[11] 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. Online at `http://dx.doi.org/10.1007/3-540-12868-9_103`

[12] N. GAMA, P. Q. NGUYEN, O. REGEV, *Lattice Enumeration Using Extreme Pruning.* In *Advances in Cryptology - EUROCRYPT 2010*, Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (French Riviera 2010). Edited by H. Gilbert, Lecture Notes in Computer Science **6110**, Springer (2010), 257–278. Online at `http://dx.doi.org/10.1007/978-3-642-13190-5_13`

[13] M. HARADA, M. KITAZUME, M. OZEKI, *Ternary Code Construction of Unimodular Lattices and Self-Dual Codes over* $\mathbf{Z}_6$. J. Alg. Combin. **16**, no. 2 (2002), 209–223. Online from `http://dx.doi.org/10.1023/A:1021185314365`

[14] M. HENTSCHEL, *On Hermitian theta series and modular forms.* Dissertation, RWTH Aachen University 2009. Online at `http://darwin.bth.rwth-aachen.de/opus3/volltexte/2009/2903/pdf/Hentschel_Michael.pdf`

[15] 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`

[16] 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`

[17] 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.

[18] A. K. LENSTRA, H. W. LENSTRA JR., L. LOVÁSZ, *Factoring polynomial with rational coefficients.* Math. Ann. **261**, no. 4 (1982), 515–534. See `http://dx.doi.org/10.1007/2FBF01457454`

[19] F. LÜBECK, *Small degree representation of finite Chevalley groups in defining characteristic.* LMS Journal of Computation and Mathematics **4** (2001), 135–169. Available from `http://dx.doi.org/10.1112/S1461157000000838`

[20] 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`

[21] 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`

[22] 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`

[23] G. NEBE, *Finite quaternionic matrix groups.* Represent. Theory **2** (1998), 106–223. Online at `http://www.ams.org/ert/1998-002-05/S1088-4165-98-00011-9`

[24] G. NEBE, *Construction and investigation of lattices with matrix groups.* In *Integral quadratic forms and lattices*, Proceedings of the International Conference on Integral Quadratic Forms and Lattices (Seoul 1998). Edited by M.-H. Kim, J. S. Hsia, Y. Kitaoka, and R. Schulze-Pillot, Contemp. Math. **249**, Amer. Math. Soc., Providence, RI (1999), 205–219.

[25] G. NEBE, *An even unimodular 72-dimensional lattice of minimum 8.* Preprint, 2010.

[26] M. OZEKI, *Ternary code construction of even unimodular lattices.* In *Théorie des nombres* [Number theory]. Proceedings of the International Conference at the Université Laval (Quebec 1987). Edited by J.-M. De Koninck and C. Levesque, de Gruyter (1989), 772–784.

[27] M. PETERS, *Siegel theta series of degree* 2 *of extremal lattices.* J. Number Theory **35** (1990), no. 1, 58–61. Available from `http://dx.doi.org/10.1016/0022-314X(90)90103-X`

[28] W. Plesken, B. Souvignier, *Computing isometries of lattices.* In *Computational algebra and number theory*, Proceedings of the 1st Magma Conference (London 1993). Edited by J. Cannon and D. Holt, Elsevier Science B.V., Amsterdam (1997), 327–334. Cross-referenced as J. Symbolic Comput. **24** (1997), no. 3-4, 327–334. Available from `http://dx.doi.org/10.1006/jsco.1996.0130`

[29] X. Pujol, `LatEnum 0.3`, implementation of parallel enumeration code. Online at `http://perso.ens-lyon.fr/xavier.pujol/latenum/latenum-0.3.tar.gz`

[30] X. Pujol, D. Stehlé, *Rigorous and Efficient Short Lattice Vectors Enumeration.* In *Advances in Cryptology - ASIACRYPT 2008*. Proceedings of the 14th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Melbourne 2008). Edited by J. Perprzyk, Lecture Notes in Computer Science **5350**, Springer (2008), 390–405. Online at `http://dx.doi.org/10.1007/978-3-540-89255-7_24`

[31] H.-G. Quebbemann, *A construction of integral lattices.* Mathematika **31** (1984), 137–140. Online at `http://dx.doi.org/10.1112/S0025579300010731`

[32] C. P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms.* Theoret. Comput. Sci. **53** (1987), 201–224. See `http://dx.doi.org/10.1016/0304-3975(87)90064-8`

[33] 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`

[34] D. Stehlé, M. Watkins, *On the Extremality of an 80-Dimensional Lattice.* In *Algorithmic Number Theory,* Ninth International Symposium, ANTS-IX (Nancy 2010). Edited by G. Hanrot, F. Morain, and E. Thomé, Lecture Notes in Computer Science **6197**, Springer (2010), 340–356. Available from `http://dx.doi.org/10.1007/978-3-642-14518-6_27`

[35] B. Venkov, *Réseaux et designs sphériques.* (French) [Lattices and spherical designs]. In *Réseaux euclidiens, designs sphériques et formes modulaires. Autour des travaux de Boris Venkov.* Edited by J. Martinet, Monogr. Enseign. Math., **37**, Enseignement Math., Geneva (2001), 10–86.

Mark Watkins
Magma Computer Algebra Group
Department of Mathematics, Carslaw Building
University of Sydney, NSW 2006 AUSTRALIA
E-mail: `watkins@maths.usyd.edu.au`