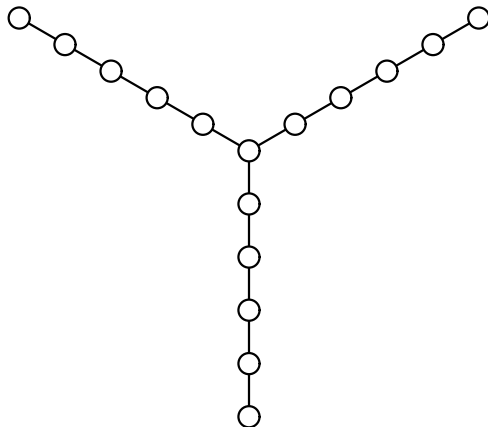


ON THE Y_{555} COMPLEX REFLECTION GROUP

DANIEL ALLCOCK

ABSTRACT. We give a computer-free proof of a theorem of Basak, describing the group generated by 16 complex reflections of order 3, satisfying the braid and commutation relations of the Y_{555} diagram. The group is the full isometry group of a certain lattice of signature $(13, 1)$ over the Eisenstein integers $\mathbb{Z}[\sqrt[3]{1}]$. Along the way we enumerate the cusps of this lattice and classify the root and Niemeier lattices over $\mathbb{Z}[\sqrt[3]{1}]$

The author has conjectured [3] that the largest sporadic finite simple group, the monster, is related to complex algebraic geometry, with a certain complex hyperbolic orbifold acting as a sort of intermediary. Specifically, the bimonster $(M \times M):2$ and a certain group $P\Gamma$ acting on complex hyperbolic 13-space are conjecturally both quotients of $\pi_1((\mathbb{C}H^{13} - \Delta)/P\Gamma)$ for a certain hyperplane arrangement Δ in $\mathbb{C}H^{13}$, got by adjoining very simple relations. If the conjecture is true then it has the consequence that $P\Gamma$ is generated by 16 complex reflections of order 3, satisfying the braid and commutation relations of the Y_{555} diagram



That is, two generators braid ($aba = bab$) or commute ($ab = ba$) when the corresponding nodes are joined or unjoined. Basak [4] has proven this, his proof making essential use of a computer. Our purpose is to

Date: February 6, 2008.

2000 Mathematics Subject Classification. 22E40, 20F55.

Partly supported by NSF grant DMS-0600112.

give a conceptual, computer-free proof. We hope that it will clarify which structures will be important for further work on the conjecture of [3].

We will describe the players in the main theorem, state the theorem, and then summarize the sections. Γ is the group of all isometries of a certain lattice $L_{13,1}$ over the Eisenstein integers $\mathcal{E} = \mathbb{Z}[\omega = \sqrt[3]{1}]$. This lattice has the property that $L_{13,1} = \theta L'_{13,1}$, where $\theta = \omega - \bar{\omega} = \sqrt{-3}$ and the prime indicates the dual lattice. Also, $L_{13,1}$ is the unique \mathcal{E} -lattice of signature $(13, 1)$ with this property. An explicit model for it appears in section 3. The Artin group of the Y_{555} diagram means the abstract group with one generator for each node of the diagram, with the braid and commutation relations described above. Such groups arise naturally in the fundamental groups of hyperplane complements. A triflection means a complex reflection of order 3, where a complex reflection means a nontrivial isometry of a Hermitian vector space that fixes a hyperplane pointwise. Complex reflections arise naturally when studying branched covers, in a manner explained in [3].

Theorem 1 ([4]). *Up to complex conjugation, there is a unique irreducible action of the Y_{555} Artin group on a Hermitian vector space of dimension > 1 in which the generators act by triflections. The image of this representation is $\text{Aut } L_{13,1}$.*

In section 1 we give background on Eisenstein lattices, and in section 2 we classify two types of such lattices, the root lattices (analogous to the ADE lattices over \mathbb{Z}) and the Eisenstein Niemeier lattices (equivalently, \mathcal{E} -lattice structures on the Niemeier lattices). The point of this is to enumerate the 5 cusps of $\mathbb{C}H^{13}/P\Gamma$ and be able to recognize one as having ‘‘Leech type’’. Section 3 describes $L_{13,1}$ in a manner convenient for the proof of the theorem, which appears in section 4. Throughout, we use ATLAS notation [6] for group extensions: $A.B$, $A:B$ and $A \cdot B$.

1. EISENSTEIN LATTICES

We have already introduced the Eisenstein integers $\mathcal{E} = \mathbb{Z}[\omega]$ and defined $\theta = \omega - \bar{\omega} = \sqrt{-3}$. An \mathcal{E} -lattice L means a free \mathcal{E} -module equipped with an \mathcal{E} -valued Hermitian form $\langle | \rangle$, linear in its first argument and antilinear in its second. The norm $|x|^2$ of a vector means $\langle x|x \rangle$. We call L nondegenerate if $L^\perp = 0$; in this case the dual lattice L' means the set of all $v \in L \otimes \mathbb{C}$ with $\langle L|v \rangle \subseteq \mathcal{E}$. All the lattices we will meet satisfy $L \subseteq \theta L' := \theta \cdot (L')$, which is to say that all inner products are divisible by θ . This should be thought of as an ordinary integrality condition, because it means that the underlying \mathbb{Z} -lattice

$L^{\mathbb{Z}}$, with $x \cdot y = \frac{2}{3} \operatorname{Re}\langle x|y\rangle$, is integral and even. The rescaling by $\frac{2}{3}$ is not important; it is a nuisance arising from the fact that the smallest scale at which L is integral as an \mathcal{E} -lattice is different from the smallest scale at which it is an integral \mathbb{Z} -lattice. Most of our lattices will also satisfy $L = \theta L'$, which is the same as the unimodularity of $L^{\mathbb{Z}}$. If $L = \theta L'$ then $\det L = \pm \theta^{\dim L}$ (which makes sense since $\dim L$ turns out to be even).

Examples of L with $L = \theta L'$ are the Eisenstein versions of the E_8 lattice ([7, ch. 7, example 11b] or theorem 3 below) and the Leech lattice ([9], scaled to have minimal norm 6). It is well-known that an indefinite even unimodular \mathbb{Z} -lattice is determined by its signature, and there is a corresponding result for \mathcal{E} -lattices. Namely, an \mathcal{E} -lattice L of signature (p, n) satisfying $L = \theta L'$ exists if and only if $p - n \equiv 0$ modulo 4, and L is unique when this signature is indefinite. A proof appears in [4]. The main player in this paper is this lattice of signature $(13, 1)$, for which we will write $L_{13,1}$. We studied it in [2], using slightly different conventions (signature $(1, 13)$ and $\langle | \rangle$ linear in its second argument rather than its first) and a particular explicit model. In section 3 we will give a different explicit model.

If L is an \mathcal{E} -lattice satisfying $L \subseteq \theta L'$, then $r \in L$ is called a root of L if $|r|^2 = 3$. The language reflects two things. First, r becomes a root in the usual sense (a vector of norm 2) when we pass to $L^{\mathbb{Z}}$. Second, the complex reflection

$$(1) \quad x \mapsto x + (\omega - 1) \frac{\langle x|r\rangle}{|r|^2} r$$

is an isometry of L , so that roots give reflections, analogously to roots in \mathbb{Z} -lattices. But this is a triflection; we call it the ω -reflection in r , since it multiplies r by ω and fixes r^\perp pointwise. If r and r' are nonproportional roots, then their ω -reflections braid if and only if $|\langle r|r'\rangle|^2 = 3$. One can check this by multiplying out 2×2 matrices.

2. ROOT LATTICES; NIEMEIER LATTICES; NULL VECTORS OF $L_{13,1}$

At a key point in section 4 we will need to recognize a particular null vector ρ of $L_{13,1}$ as having “Leech type”, which is to say that $\rho^\perp / \langle \rho \rangle$ is a copy of the complex Leech lattice. The reader may skip this section if he is prepared to accept one consequence of theorem 4 below: a primitive null vector of $L_{13,1}$ whose stabilizer contains a copy of $L_3(3)$ has Leech type. There is a quicker-and-dirtier proof than the one we give, but we think the \mathcal{E} -lattice classifications are interesting in themselves.

We will need to understand the orbits of primitive null vectors in $L_{13,1}$. These turn out to be in bijection with the positive-definite 12-dimensional lattices L satisfying $L = \theta L'$; we will call such lattices Eisenstein Niemeier lattices, since their real forms are positive-definite 24-dimensional even unimodular lattices, classified by Niemeier. Since root lattices play a major role in Niemeier's classification, they do in ours too, so we define an Eisenstein root lattice to be a positive-definite \mathcal{E} -lattice L satisfying $L \subseteq \theta L'$ and spanned by its roots.

We will establish the bijection between Eisenstein Niemeier lattices and orbits of primitive null vectors in $L_{13,1}$, then classify the Eisenstein root lattices, and then use this to classify the Eisenstein Niemeier lattices. The root lattice classification is similar to and simpler than the well-known ADE classification of root lattices over \mathbb{Z} . The Eisenstein Niemeier lattices turn out to correspond to five of the classical Niemeier lattices.

Lemma 2. *Suppose $p, n > 0$, $p - n \equiv 0 \pmod{4}$, and $L_{p,n}$ is the unique \mathcal{E} -lattice of signature (p, n) satisfying $L_{p,n} = \theta L'_{p,n}$. If ρ is a primitive null vector then $L := \rho^\perp / \langle \rho \rangle$ is a lattice of signature $(p - 1, n - 1)$ that satisfies $L = \theta L'$. Every such L arises this way. Two primitive null vectors ρ_1, ρ_2 of $L_{p,n}$ are equivalent under $\text{Aut } L_{p,n}$ if and only if $\rho_1^\perp / \langle \rho_1 \rangle \cong \rho_2^\perp / \langle \rho_2 \rangle$.*

Proof. (This is essentially the same as for even unimodular \mathbb{Z} -lattices.) By $L_{p,n} = \theta L'_{p,n}$, there exists $w \in L$ with $\langle \rho | w \rangle = \theta$. Adding a multiple of ρ to w allows us to also assume $|w|^2 = 0$, so $\langle \rho, w \rangle \cong \begin{pmatrix} 0 & \theta \\ \theta & 0 \end{pmatrix}$. Therefore $\langle \rho, w \rangle = \theta \langle \rho, w \rangle'$, so $\langle \rho, w \rangle$ is a summand of $L_{p,n}$. The other summand $\langle \rho, w \rangle^\perp$ must also satisfy $\langle \rho, w \rangle^\perp = \theta (\langle \rho, w \rangle^\perp)'$, and it projects isometrically to $\rho^\perp / \langle \rho \rangle$. This establishes the first claim. For the second, given L of signature $(p - 1, n - 1)$ satisfying $L = \theta L'$, we have $L \oplus \begin{pmatrix} 0 & \theta \\ \theta & 0 \end{pmatrix} \cong L_{p,n}$, and it is now obvious that L is $\rho^\perp / \langle \rho \rangle$ for a suitable null vector ρ . In the last claim, if ρ_1 and ρ_2 are equivalent, then obviously $\rho_1^\perp / \langle \rho_1 \rangle \cong \rho_2^\perp / \langle \rho_2 \rangle$, so it suffices to show the converse. The argument for the first claim implies that there is a direct sum decomposition $L_{p,n} \cong M_1 \oplus \begin{pmatrix} 0 & \theta \\ \theta & 0 \end{pmatrix}$ with $M_1 \cong \rho_1^\perp / \langle \rho_1 \rangle$ and ρ_1 corresponding to one of the coordinate vectors of the 2×2 block. And there is a similar decomposition with ρ_2 in place of ρ_1 . Then, given an isomorphism $M_1 \cong M_2$, it is easy to write down an automorphism of $L_{p,n}$ sending ρ_1 to ρ_2 . \square

L	R	$\text{Aut } L$	$ \text{Aut } L $	$\theta L' - L$	
				$\theta L'/L$	min. norm
$A_2^\mathcal{E}$	$\mathbb{Z}/3$	$\times \mathbb{Z}/2$	6	\mathbb{F}_3^1	1
$D_4^\mathcal{E}$	$\text{SL}_2(3)$	$\times \mathbb{Z}/3$	72	\mathbb{F}_4^1	3/2
$E_6^\mathcal{E}$	$3^{1+2}:\text{SL}_2(3)$	$\times \mathbb{Z}/2$	1,296	\mathbb{F}_3^1	2
$E_8^\mathcal{E}$	$3 \times \text{Sp}_4(3)$	$\times 1$	155,520	0	

TABLE 1. The indecomposable Eisenstein root lattices. The second column gives the structure of the group R generated by the triflections in the roots of L , in ATLAS notation [6]. $\text{Aut } L$ is the product of this group with the cyclic group of scalars given in the third column. The fifth column describes $\theta L'/L$ as a vector space over $\mathcal{E}/\theta\mathcal{E} = \mathbb{F}_3$ or $\mathcal{E}/2\mathcal{E} = \mathbb{F}_4$. Every nonzero element of $\theta L'/L$ has minimal representatives of norm given in the last column.

Theorem 3. *Any Eisenstein root lattice is a direct sum of copies of the following 4 lattices:*

$$A_2^\mathcal{E} = \theta\mathcal{E}$$

$$D_4^\mathcal{E} = \{(x, x, y) \in \mathcal{E}^3 : x \equiv y \pmod{\theta}\}$$

$$E_6^\mathcal{E} = \{(x, y, z) \in \mathcal{E}^3 : x \equiv y \equiv z \pmod{\theta}\}$$

$$E_8^\mathcal{E} = \{(x_1, \dots, x_4) \in \mathcal{E}^4 : \pi(x_1, \dots, x_4) \in \mathcal{C}_4 \subseteq \mathbb{F}_3^4\},$$

which have the properties listed in table 2. (We use the standard inner product on \mathbb{C}^n . Also, the description of $E_8^\mathcal{E}$ refers to the map $\pi : \mathcal{E}^4 \rightarrow \mathcal{E}^4/\theta\mathcal{E}^4 = \mathbb{F}_3^4$ and the tetracode \mathcal{C}_4 , i.e., the subspace of \mathbb{F}_3^4 spanned by $(0, 1, 1, 1)$ and $(1, 0, 1, -1)$.)

Proof. The data in the table will be helpful in the classification, so we begin there. The claims for $L = A_2^\mathcal{E}$ are obvious; we remark that the smallest elements of $\theta L' - L$ are the units of \mathcal{E} , and all others have norm > 3 .

Now let $L = D_4^\mathcal{E}$. Its 24 roots are the scalar multiples of $(\omega^i, \omega^i, 1)$ and $(0, 0, \theta)$. It is easy to see that conjugation by each of the $24/6 = 4$ cyclic groups generated by triflections permutes the other 3 cyclically. Therefore R is generated by two triflections that braid, so it is an image of $\langle a, b \mid aba = bab, a^3 = b^3 = 1 \rangle$, which is a presentation for $\text{SL}_2(3)$. To see that R is $\text{SL}_2(3)$ rather than a proper quotient, consider its action on $L/\theta L \cong \mathbb{F}_3^2$. Now, R permutes the scalar classes of roots as the

alternating group A_4 , so if we choose any 2 non-proportional roots r and s , then $\text{Aut } L$ is generated by R together with the transformations sending r to a multiple of itself and s to a multiple of itself. Since $\langle r|s \rangle \neq 0$, such a transformation must be a scalar. So $\text{Aut } L = R \times \langle \omega \rangle$. Finally, it is easy to see that the norm 6 vectors of L are the scalar multiples of $(\omega^i, \omega^i, 1 + \theta)$ and $(\theta, \theta, 0)$, and that the halves of these vectors span $\theta L'$. In fact, the halves of these vectors account for all the elements of $\theta L' - L$ of norm ≤ 3 , and are all equivalent under $\text{Aut } L$. Representatives for $\theta L'/L$ are 0 and $\frac{\omega^i}{2}(\theta, \theta, 0)$, so $\theta L'/L \cong \mathbb{F}_4^1$.

Now let $L = E_8^\mathcal{E}$. Because it is got from $(A_2^\mathcal{E})^4$ by gluing along the 2-dimensional code $\mathcal{C}_4 \subseteq (\theta(A_2^\mathcal{E})'/A_2^\mathcal{E})^4 \cong \mathbb{F}_3^4$, it satisfies $L = \theta L'$, justifying the last two entries in the table. The descriptions of R and $\text{Aut } L$ are justified by theorem 5.2 of [2]. (The proof in [2] appeals to a coset enumeration to establish that L contains the scalars of order 3; this may be avoided by observing that L contains 4 mutually orthogonal roots.)

Now let $L = E_6^\mathcal{E}$ and note that the following symmetries are visible: permutation of coordinates, multiplication of coordinates by cube roots of unity, and the scalar -1 . It is easy to see that $\theta L' = \{(x, y, z) \in \mathcal{E}^3 : x + y + z \equiv 0 \pmod{\theta}\}$, whose 54 minimal vectors are got from $(1, -1, 0)$ by applying these symmetries. Note also that these are the only elements of $\theta L' - L$ of norm ≤ 3 . It is easy to see that $\theta L'/L \cong \mathbb{F}_3^1$. Also, L is the orthogonal complement of $r = (0, 0, 0, \theta) \in E_8^\mathcal{E}$, and every automorphism ϕ of $E_6^\mathcal{E}$ extends uniquely to an automorphism of $E_8^\mathcal{E}$ that either fixes or negates r . (The extension fixes or negates r according to whether ϕ fixes or negates $\theta L'/L \cong \theta \langle r \rangle' / \langle r \rangle \cong \mathbb{F}_3^1$.) It follows that $|\text{Aut } L| \leq 2 \times \frac{1}{240} \times 155,520 = 1296$. Since triplefections must act trivially on \mathbb{F}_3^1 , we also have $|R| \leq 648$. We will show that R has structure $3^{1+2}:\text{SL}_2(3)$; this will justify the first column of the table, and (since $-1 \notin R$) also the second.

To see the map $R \rightarrow \text{SL}_2(3)$, consider the action on $L/3L' \cong \mathbb{F}_3^2$. All roots are equivalent under $\text{Aut } L$ (since any two root in a $D_4^\mathcal{E}$ are R -equivalent), and the 72 roots fall into 8 classes of size 9, accounting for all 8 nonzero elements of $L/3L'$. This space supports a symplectic form, given by dividing inner products by θ and then reducing mod θ . The ω -reflection in a root projects to the symplectic transvection in the image of the root. Now we study the kernel K of $R \rightarrow \text{SL}_2(3)$. If r and s are orthogonal roots then their ω -reflections map to the same transvection $L/3L'$ (since they map to commuting transvections), so the quotient of the reflections lies in K . This shows: if an automorphism of L has 3 roots as eigenvectors, with eigenvalues 1, ω and $\bar{\omega}$, then it lies

in K . For example, $\text{diag}[1, w, \bar{w}] \in K$. Also, the cyclic permutation of coordinates lies in K . These two elements of K generate an extraspecial group 3^{1+2} . Since $27 \cdot |\text{SL}_2(3)| = 648$, we have shown $R = 3^{1+2} \cdot \text{SL}_2(3)$. The extension splits because the reflection group of a $D_4^\mathcal{E}$ sublattice provides a complement.

Having established the table, we will now classify the Eisenstein root lattices. Call such a lattice decomposable if its roots fall into two or more nonempty classes, with members of distinct classes being orthogonal. In this case it is a direct sum of lower-dimensional root lattices, so it suffices to show that $A_2^\mathcal{E}$, $D_4^\mathcal{E}$, $E_6^\mathcal{E}$ and $E_8^\mathcal{E}$ are the only indecomposable Eisenstein root lattices. We will use the following facts, established above. (i) If $L = A_2^\mathcal{E}$, $D_4^\mathcal{E}$ or $E_6^\mathcal{E}$, then $\text{Aut } L$ acts transitively on the vectors of $\theta L' - L$ of norm ≤ 3 . (ii) $E_8^\mathcal{E} = \theta(E_8^\mathcal{E})'$.

Suppose M is an indecomposable Eisenstein root lattice. If $\dim M = 1$ then obviously $M \cong A_2^\mathcal{E}$. If $\dim M = 2$ then it contains a 1-dimensional indecomposable root lattice L , and we know $L \cong A_2^\mathcal{E}$. Also, M contains a root r not in $L \otimes \mathbb{C}$, whose projection to $L \otimes \mathbb{C}$ is nonzero. Since this projection is an element r of $\theta L' - \{0\}$ of norm < 3 , and $\text{Aut } L$ acts transitively on such vectors, there is an essentially unique possibility for $\langle L, r \rangle$. Since $D_4^\mathcal{E}$ arises by this construction, $\langle L, r \rangle \cong D_4^\mathcal{E}$. Therefore M lies between $\theta(D_4^\mathcal{E})'$ and $D_4^\mathcal{E}$. Since every norm 3 vector of $\theta(D_4^\mathcal{E})'$ lies in $D_4^\mathcal{E}$, we have $M \cong D_4^\mathcal{E}$. If $\dim M = 3$ then the same argument, with $L = D_4^\mathcal{E}$, shows that $M \cong E_6^\mathcal{E}$. If $\dim M > 3$, then the same argument, with $L = E_6^\mathcal{E}$, shows that M contains $E_8^\mathcal{E}$. Then $E_8 = \theta(E_8^\mathcal{E})'$ implies that $E_8^\mathcal{E}$ is a summand of M , and indecomposability implies $M \cong E_8^\mathcal{E}$. \square

Theorem 4. *There are exactly 5 Eisenstein Niemeier lattices:*

- $(A_2^\mathcal{E})^{12}$ glued along the ternary Golay code, with group $3^{12}:2M_{12}$;
- $(D_4^\mathcal{E})^6$ glued along the hexacode, with group $\text{SL}_2(3)^6:3A_6$;
- $(E_6^\mathcal{E})^4$ glued along the tetracode, with group $(3^{1+2}:\text{SL}_2(3))^4:\text{SL}_2(3)$;
- $(E_8^\mathcal{E})^3$, with group $(3 \times \text{Sp}_4(3))^3:S_3$; and
- the complex Leech lattice $\Lambda_{24}^\mathcal{E}$, with group 6Suz .

Here, M_{12} and Suz are the sporadic finite simple groups of Mathieu and Suzuki.

Proof. Our argument is similar in spirit to Venkov's treatment [8] of Niemeier's classification. Suppose L is an Eisenstein Niemeier lattice and $L^\mathbb{Z}$ its underlying real lattice. By Niemeier's classification, there are 24 possibilities for $L^\mathbb{Z}$; in 23 cases the roots span $L^\mathbb{Z}$ up to finite index, and in the last case $L^\mathbb{Z}$ has no roots and is the Leech lattice.

By theorem 3, the root system of $L^{\mathbb{Z}}$ must be a sum of A_2 , D_4 , E_6 and E_8 root systems. Considering Niemeier's list shows that $L^{\mathbb{Z}}$'s root system is A_2^{12} , D_4^6 , E_6^4 , E_8^3 or empty. We treat the first four cases first. Theorem 3 shows that there is a unique Eisenstein structure on the root sublattice of $L^{\mathbb{Z}}$, so the sublattice L_0 of L spanned by its roots is $(A_2^{\mathcal{E}})^{12}$, $(D_4^{\mathcal{E}})^6$, $(E_6^{\mathcal{E}})^4$ or $(E_8^{\mathcal{E}})^3$. In the last case we have $L = L_0$ and are done. In the other cases, L lies between $\theta L'_0$ and L_0 , so it is determined by its image \mathcal{C} in $\theta L'_0/L_0 \cong \mathbb{F}_3^{12}$, \mathbb{F}_4^6 or \mathbb{F}_3^4 in the three cases. We must have $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ (with respect to the usual quadratic form on \mathbb{F}_3^n or Hermitian form on \mathbb{F}_4^6), in order to have $L \subseteq \theta L'$. Also, \mathcal{C} must be half-dimensional in $\theta L'_0/L_0$, in order to have $L = \theta L'$. Finally, all roots of L already lie in L_0 , by definition.

In the A_2 case, these conditions imply that \mathcal{C} is a selfdual code of length 12 with no codewords of weight 3. The ternary Golay code is the unique such code, up to monomial transformations of \mathbb{F}_3^{12} , so \mathcal{C} is it and L is as described. In the D_4 case, \mathcal{C} is a selfdual subspace of \mathbb{F}_4^6 with no codewords of weight 2. The hexacode is the unique such code, up to monomial transformations, so \mathcal{C} is it and L is as described. In the E_6 case, \mathcal{C} is a 2-dimensional subspace of \mathbb{F}_3^4 having no codewords of weight < 3 . Again there is a unique candidate, the tetracode, and L is as described.

Next we treat the case that $L^{\mathbb{Z}}$ is the Leech lattice; we must show that L is the complex Leech lattice. I know of 3 completely independent approaches. (1) The uniqueness of the \mathcal{E} -module structure on the Leech lattice is the same as the uniqueness of the conjugacy class in $Co_0 = \text{Aut}(L^{\mathbb{Z}})$ of elements of order 3 with no fixed vectors. This can be checked by consulting the character table [6] for Co_0 . (2) Use lemma 2, together with theorem 4.1 of [2], which contains the statement that $L_{13,1}$ has a unique orbit of primitive null vectors orthogonal to no roots. (3) Presumably one can mimic Conway's characterization of the Leech lattice [5], applying analogues of his counting argument to $L/\theta L$.

The automorphism group of $\Lambda_{24}^{\mathcal{E}}$ is treated in detail in [9]. The other automorphism groups are easy to work out. Let $L_0 = M^n$ be the decomposition of L_0 into its indecomposable summands and let R be the group generated by triflections in the roots of M . Recall from theorem 3 that $\text{Aut } M$ splits as $R \times C$, where C denotes the group of scalars from column 3 of table 2. Obviously $\text{Aut } L \subseteq \text{Aut } L_0 = (R^n \times C^n):S_n$; indeed it is the subgroup of this that preserves $\mathcal{C} \subseteq (\theta M'/M)^n$. Now, R acts trivially and $C^n:S_n$ acts by monomial transformations. Therefore $\text{Aut } L$ is the semidirect product of R^n by the subgroup of $C^n:S_n$ whose action preserves \mathcal{C} . This latter group is $2M_{12}$, $3A_6$, $\text{SL}_2(3)$ or S_3 in the four cases. (The automorphism group of the hexacode is

support	coordinates	description	number
0	0^{13}		1
6	$+^3-^30^7$	difference of lines	156
9	$\pm(+^90^4)$	affine plane	26
9	$\pm(+^6-^30^4)$	sum of 3 general lines	468
12	$+^6-^60$	$l_1 + l_2 - l_3 - l_3$ for 4 concurrent lines	78

TABLE 2. The elements of \mathcal{C} .

sometimes given as $3 \cdot S_6$, but the elements not in $3A_6$ are \mathbb{F}_4 -antilinear, so they arise from antilinear maps $L \rightarrow L$. \square

3. A MODEL OF $L_{13,1}$

In this section we describe $L_{13,1}$ with $3^{13}:L_3(3)$ among its visible symmetries. We begin with the vector space \mathbb{F}_3^{13} , with coordinates indexed by the points of $P^2\mathbb{F}_3$, and proceed to define two codes. The first is the “line difference code” \mathcal{C} , spanned by the differences of (characteristic functions of) lines of $P^2\mathbb{F}_3$, and the second is the “line code”, which derives its name from the fact that it is spanned by lines, but is formally defined (and written) as \mathcal{C}^\perp (with respect to the usual inner product).

Two lines of $P^2\mathbb{F}_3$ meet in 1 point (or 4), and it follows that \mathcal{C} is orthogonal to every line, hence orthogonal to itself. Therefore $\dim \mathcal{C} \leq 6$. On the other hand, it is easy to enumerate some elements of \mathcal{C} (table 2). This shows that $\dim \mathcal{C} = 6$ and also that the enumeration is complete. Therefore $\dim \mathcal{C}^\perp = 7$, and since a line lies in \mathcal{C}^\perp but not \mathcal{C} , we see that \mathcal{C}^\perp is indeed spanned by lines. It will be useful to have a list of the elements of \mathcal{C}^\perp : these are the codewords in table 3, their negatives, and the elements of \mathcal{C} . We compiled table 3 by adding the all 1’s vector (the sum of all 13 lines) to the elements of \mathcal{C} .

We work with the usual inner product of signature $(13, 1)$ on \mathbb{C}^{14} ,

$$\langle x|y \rangle = -x_0\bar{y}_0 + x_1\bar{y}_1 + \cdots + x_{13}\bar{y}_{13},$$

index the last 13 coordinates by the points of $P^2\mathbb{F}_3$, and define L as the set of vectors $(x_0; x_1, \dots, x_{13})$ such that $x_0 \equiv x_1 + \cdots + x_{13} \pmod{\theta}$ and that (x_1, \dots, x_{13}) , modulo θ , is an element of \mathcal{C}^\perp .

Theorem 5. *L is isomorphic to $L_{13,1}$ and is spanned by the 13 “point roots” $(0; \theta, 0^{12})$, with the θ in any of the last 13 spots, and the 13 “line roots” $(1; 1^4, 0^9)$, with the 1’s along a line of $P^2\mathbb{F}_3$.*

Proof. It is easy to see that the point and line roots span L . If p is a point root and ℓ a line root, then $\langle p|\ell \rangle = \theta$ or 0 according to whether

support	coordinates	description	number
4	$+^4 0^9$	line	13
7	$+^1 -^6 0^6$	sum of two lines (negated)	78
7	$+^4 -^3 0^6$	-1 on vertices, 0 on edges, 1 elsewhere	234
10	$+^4 -^6 0^3$	0 on vertices, -1 on edges, 1 elsewhere	234
10	$+^7 -^3 0^3$	-1 on $l_1 - l_2$, 0 on $l_2 - l_1$, 1 elsewhere	156
13	$+^4 -^9$	1 on a line, -1 elsewhere	13
13	$+^{13}$		1

TABLE 3. The elements of \mathcal{C}^\perp with coordinate sum 1. The entries that refer to “vertices” and “edges” refer to three general lines—a vertex means a point on two of the lines, and an edge means a point on just one of them.

the point lies on the line. Also, any two point roots are orthogonal, as are any two line roots. Therefore $L \subseteq \theta L'$. To see $L = \theta L'$, check that L contains $(\theta; 0^{13})$ and consider the span M of it and the point roots. Then $\theta M'/M \cong \mathbb{F}_3^{14}$, and we need to check that the image of L therein is 7-dimensional. This is easy because we know $\dim \mathcal{C}^\perp = 7$ and the 0th coordinate of an element of L is determined modulo θ by the others. \square

The promised group $3^{13}:L_3(3)$ is generated by the triflections in the point roots and the permutations of the last 13 coordinates by $L_3(3)$.

The following lemma is not central; it is used only to establish the equality of two lattices in the proof of lemma 9.

Lemma 6. *Let M be the 12-dimensional lattice consisting of all vectors in $(\theta\mathcal{E})^{13}$ with coordinate sum zero. Then there is a unique lattice N preserved by $L_3(3)$, strictly containing M , and satisfying $N \subseteq \theta N'$.*

Proof sketch: Any lattice N containing M and satisfying $N \subseteq \theta N'$ lies in $\theta M'$, so that it corresponds to a subspace of $Z := \theta M'/M$. And Z is the coordinate-sum-zero subspace of \mathbb{F}_3^{13} . The lemma follows from the fact that \mathcal{C} is the unique nontrivial $L_3(3)$ -invariant subspace. To see this, one checks that \mathcal{C} is irreducible under $L_3(3)$, so that Z/\mathcal{C} is also irreducible (being the dual), and that \mathcal{C} has no invariant complement. \square

4. GENERATION OF $\text{Aut}(L_{13,1})$ BY THE Y_{555} TRIFLECTIONS

In this section we prove the main theorem, theorem 1. First we prove uniqueness. Label the generators by g_1, \dots, g_{16} . The argument of [2,

sec. 5] shows that without loss we may take the g_i to be the ω -reflections in pairwise linearly independent vectors r_1, \dots, r_{16} of norm 3, satisfying $|\langle r_i | r_j \rangle|^2 = 3$ or 0 according to whether g_i and g_j braid or commute. It is convenient to 2-color Y_{555} and suppose $\langle r_i | r_j \rangle = \theta$ (resp. $-\theta$) when g_i and g_j braid and g_i is black (resp. white). The inner product matrix of the r_i turns out to have rank 14 (by direct computation or the realization below), so V must have dimension 14 (by irreducibility of V and connectedness of Y_{555}). The r_i are determined up to isometries of V by their inner products, so their configuration is unique.

Having proven uniqueness of the representation, we can define R as its image. To identify R with $\text{Aut } L_{13,1}$, we will use the model for $L_{13,1}$ from the previous section, and write L for it. Let Δ be the incidence graph of the points and lines of $P^2\mathbb{F}_3$, and color the nodes corresponding to points black and lines white. Then the point and line roots from theorem 5 satisfy the same inner product conditions as the r_i chosen above. It is possible (uniquely up to $L_3(3)$) to embed the Y_{555} diagram into Δ , preserving node colors. So the 16 roots for Y_{555} may be taken to be 16 of the point and line roots. It would be annoying to make a choice of which 16, and we are saved from this by the following lemma.

Lemma 7. *The 16 roots for Y_{555} span L , and R contains $L_3(3)$ and the triflections in all the point and line roots.*

Proof. First observe that Y_{555} contains an 11-chain E and a 4-chain F not joined to it. By [2, fig. 5.1], the roots of E span a copy of $L_{9,1}$ and those of F a copy of $E_8^\mathcal{E}$, so together they span L . This proves our first assertion.

One can check that for any 11-chain E in Δ , E has a unique extension to a 12-cycle C , and that the nodes of Δ not joined to C form a 4-chain F . (E is unique up to $L_3(3):2$, so checking a single example suffices.) We claim that if R contains the triflections in the roots of E , then it also contains the triflections in the root extending E to C . We use a computation-free variation of the proof of [4, lemma 3.2]. First use the fact that the roots of F span a copy of $E_8^\mathcal{E}$, whose orthogonal complement in L must be a copy of $L_{9,1}$. By [2, thm. 5.2], $\text{Aut } L_{9,1}$ is generated by the triflections of E and hence lies in R . And since the extending root is orthogonal to $E_8^\mathcal{E}$, it also lies in $L_{9,1}$, so its triflections also lie in R . This proves the claim. Now, starting with the three 11-chains in Y_{555} and repeatedly applying the claim shows that R contains the triflections in all 26 roots.

We use a similar trick to show $L_3(3) \subseteq R$. Consider any $Y_{555} \subseteq \Delta$, and let E be one of its 11-chains and F the 4-chain in Y_{555} not joined to it. Let ϕ be the diagram automorphism of Y_{555} that fixes each node

of F and exchanges the ends of E . One can check that ϕ extends to an automorphism of Δ , preserving node colors since it has a fixed point. Therefore ϕ defines an automorphism of L , permuting the point and line roots as it permutes the points and lines of $P^2\mathbb{F}_3$. Since ϕ fixes F pointwise, it is an automorphism of the $L_{9,1}$ spanned by the roots of E . We already know that R contains $\text{Aut } L_{9,1}$, so it contains ϕ . So each $Y_{555} \subseteq \Delta$ gives rise to an $S_3 \subseteq R \cap L_3(3)$. The set of elements of $R \cap L_3(3)$ so obtained, from all Y_{555} subdiagrams, is clearly normal in $L_3(3)$. Since $L_3(3)$ is simple, $R \cap L_3(3)$ is all of $L_3(3)$. (This diagram-automorphism trick was also used in [2, thm. 5.1] and [4, thm. 5.8].) \square

The next lemma shows that if R contains certain triflections, then it contains a well-understood group, of finite index in the stabilizer of a null vector. The lemma after that shows that R does indeed contain these triflections, and then we can complete the proof of theorem 1 by showing $R = \text{Aut } L$.

Lemma 8. *Suppose L is an \mathcal{E} -lattice of dimension > 2 satisfying $L = \theta L'$. Suppose ρ is a primitive null vector and r_i are roots satisfying $\langle r_i | \rho \rangle = \theta$, such that the span of their differences projects onto $\rho^\perp / \langle \rho \rangle$. Let G be the group generated by the triflections in the r_i and $\rho + r_i$. Then G contains every element of $\text{Aut } L$ that acts by a scalar on $\langle \rho \rangle$ and trivially on $\rho^\perp / \langle \rho \rangle$*

Remark. The hypothesis $\dim L > 2$ is necessary and should also have been imposed in theorem 3.2 of [2].

Proof. This is implicit in the proofs of theorem 3.1 and 3.2 of [2]; since the argument is slightly different and our conventions there were different, we phrase the argument in coordinate-free language and refer to [2] for the supporting calculations. By the unipotent radical U of the stabilizer of ρ we mean the automorphisms of L that fix ρ and act trivially on $M := \rho^\perp / \langle \rho \rangle$. It is a Heisenberg group, with center Z equal to its commutator subgroup and isomorphic to \mathbb{Z} , with U/Z a copy of the additive group of M . The set X of scalar classes of roots r with $|\langle r | \rho \rangle| = |\theta|$ is a principal homogeneous space for U , and the set X/Z of its Z -orbits is a principal homogeneous space for $U/Z \cong M$. If r is a root with $\langle r | \rho \rangle = \theta$, then the triflections in r and $\rho + r$ can be composed to yield a transformation multiplying ρ by a primitive 6th root of unity and acting on X/Z by scalar multiplication by a primitive 6th root of unity, where X/Z is identified with M by taking rZ as the origin. Write ϕ_r for this transformation (which depends only on rZ , though we don't need this).

Suppose r' is another root with $\langle r'|\rho \rangle = \theta$. Since X/Z is a principal homogeneous space modeled on M , there exists $m \in M$ with $m \cdot rZ = r'Z$. Then $\phi_r \circ \phi_{r'}^{-1}$ turns out to be an element of U , acting on X/Z by translation by a unit times m . Under the hypothesis of the lemma, G contains elements of U for sufficiently many m to span M as an \mathcal{E} -lattice. Taking conjugates by (any) ϕ_r gives the unit scalar multiples of these m , so G contains enough elements of U to generate M as a group. Taking commutators shows that G contains Z , so it contains all of U . And $\langle U, \phi_r \rangle$ consists of all the elements of $\text{Aut } L$ that we are asserting to lie in G . \square

Lemma 9. *Let ρ be the primitive null vector $(-4 - \omega; 1^{13}) \in L$. If r is one of the 156 roots $(2 + \theta; 0^3, \bar{\omega}^3, -1^7)$ or one of the 234 roots $(-2\bar{\omega}; \bar{\omega}^4, -1^3, 0^6)$, then $\langle r|\rho \rangle = \theta$ and R contains the triflections in r and $\rho + r$. The differences of these 390 roots span ρ^\perp .*

Remarks. The exact placement of the coordinates can be determined up to $L_3(3)$ by reducing the last 13 coordinates modulo θ and comparing with the list of elements of \mathcal{C}^\perp . For example, for one of the 156 roots, the 0's lie on one line of $P^2\mathbb{F}_3$, the $\bar{\omega}$'s lie on another, and the -1 's are everywhere else, including the point where the lines intersect. (There are $13 \cdot 12 = 156$ ways to choose the two lines.) The same method applies to all vectors referred to in the proof. Also, R contains the triflections in some less-complicated roots r satisfying $\langle r|\rho \rangle = \theta$, for example the point roots. But for these, showing that R contains the triflections in $\rho + r$ is harder. We chose these roots because both r and $\rho + r$ have small 0th coordinate.

Proof. Checking $\langle r|\rho \rangle = \theta$ is just a computation. Now we show that R has various roots r (meaning that it contains the triflections in them). We will use the following fact repeatedly: if R has roots a and b , and $\langle a|b \rangle = \omega - 1$ or $\bar{\omega} - 1$, then $a + b$ is a root and R has it too. (This is because $\langle a, b \rangle \cong D_4^\mathcal{E}$, and the reflections in any two independent roots of $D_4^\mathcal{E}$ generate the whole reflection group of $D_4^\mathcal{E}$.) We know already that R has the line roots and their images under scalars and $3^{13}:L_3(3)$.

Step 1: R has the roots $(\theta; 1^3, -1^3, 0^7)$ with the 1's collinear and the -1 's collinear. Take b to be the line root $(1; 1^4, 0^9)$, and try a having the form $(-\omega; ?, 0^3, ?^3, 0^6)$, where the ?'s are negated cube roots of 1, lying along a different line. We try this a because $a + b = (1 - \omega; \dots)$, so if we can choose the ?'s with $\langle a|b \rangle = \omega^{\pm 1} - 1$, then we can conclude that R has a root $a + b = (1 - \omega; \dots)$, which we didn't know before. We may in fact achieve $\langle a|b \rangle = \omega - 1$, by taking (say) all the ?'s to be -1 . Then R has the root $(1 - \omega; 0, 1^3, -1^3, 0^6)$. Applying a scalar and

an element of $3^{13}:L_3(3)$ finishes step 1 (this part of the argument will be left implicit in steps 2–5).

Step 2: R has the roots $(2; -1^4, 1^3, 0^6)$ with the 1's at three non-collinear points, the 0's on the lines joining them, and the -1 's everywhere else. Take $b = (\theta; 1^3, -1^3, 0^7)$ from step 1, and try $a = (1; ?, 0^2, ?, 0^2, ?^2, 0^5)$, with the ?'s lying on a line that meets a 1 and a -1 of b . Solving for the ?'s as before reveals that $a = (1; \bar{\omega}, 0^2, 1, 0^2, ?^2, 0^5)$ satisfies $\langle a|b \rangle = \omega - 1$. So R has the root $(\theta + 1; -\omega, 1^2, 0, -1^2, ?^2, 0^5)$ where the ?'s are cube roots of 1—exactly which ones is unimportant.

Step 3: R has the roots $(2; 1^6, -1, 0^6)$, where the 1's all lie on two lines through the -1 . Take $b = (1; 1^4, 0^9)$ and try $a = (1; ?, 0^3, ?^3, 0^6)$. Solving for the ?'s reveals that $a = (1; \omega, 0^3, ?^3, 0^6)$ satisfies $\langle a|b \rangle = \omega - 1$. So R has the root $a + b = (2; -\bar{\omega}, 1^3, ?^3, 0^6)$ with the ?'s being cube roots of 1.

Step 4: R has the roots $(2 - \bar{\omega}; -1^3, 0^3, 1^7)$, with the -1 's collinear and the 0's collinear. Take $b = (2; 1^6, -1, 0^6)$ from step 3, and try $a = (-\bar{\omega}; 0^6, ?, ?^3, 0^3)$ where the ?'s all lie on a line through the -1 of b . Solving for the ?'s reveals that $a = (-\bar{\omega}; 0^6, -\omega, ?^3, 0^3)$ satisfies $\langle a|b \rangle = \bar{\omega} - 1$. So R has the root $a + b = (2 - \bar{\omega}; 1^6, \bar{\omega}, ?^3, 0^3)$, where the ?'s are negated cube roots of 1.

Step 5: R has the roots $(2 + \theta; -1^4, 1^6, 0^3)$ with the 0's at non-collinear points, the 1's on the lines joining them and the -1 's everywhere else. Take $b = (2 - \bar{\omega}; -1^3, 0^3, 1^7)$ from step 4, and try $a = (\omega; ?, 0^2, ?, 0^2, ?^2, 0^5)$. Solving for ?'s reveals that $a = (\omega; 1, 0^2, \omega, 0^2, \omega^2, 0^5)$ satisfies $\langle a|b \rangle = \bar{\omega} - 1$, so R has the root $a + b = (2 + \theta; 0, -1^2, \omega, 0^2, -\bar{\omega}^2, 1^5)$.

Now we can prove the second claim of the lemma. If r is in the first set of roots specified, then R has r by step 4 and $\rho + r = (\bar{\theta}\bar{\omega}; 1^3, -\omega^3, 0^7)$ by step 1. If r is in the second set of roots, then R has r by step 2 and $\rho + r = (-2 + \omega; -\omega^4, 0^3, 1^6)$ by step 5.

Finally, we prove that the differences of the r 's span ρ^\perp . We will only need the second batch of roots briefly, so we define N to be the span of the differences of the pairs of roots from the first batch. It consists of vectors of the form $(0; \dots)$. Now we note that a root from the first batch, minus one from the second, has the form $(1; \dots)$. Therefore it suffices to show that N equals the set X of all vectors $(0; x_1, \dots, x_{13}) \in L$ that are orthogonal to ρ , which is to say that $x_1 + \dots + x_{13} = 0$. We will restrict attention to the last 13 coordinates.

Begin by labeling the lines of $P^2\mathbb{F}_3$ by l_1, \dots, l_{13} , and write r_{ij} for the root $(2 + \theta; 0^3, \bar{\omega}^3, -1^7)$ from the first batch, with the 0's on l_i and the $\bar{\omega}$'s on l_j . Then N contains the vectors $\delta_{ij} = -\omega(r_{ij} - r_{ji}) = (0; 1^3, -1^3, 0^7)$. The span of the δ_{ij} is easy to understand, because if i, j, k and l are

all distinct, then $\delta_{ij} = -\delta_{ji}$, $|\delta_{ij}|^2 = 6$, $\langle \delta_{ij} | \delta_{jk} \rangle = -3$ and $\langle \delta_{ij} | \delta_{kl} \rangle = 0$. It follows that $N \otimes \mathbb{C}$ admits a coordinate system using 13 coordinates summing to 0, in which $\delta_{ij} = (\theta, \bar{\theta}, 0^{11})$ with θ in the i th spot and $\bar{\theta}$ in the j th. (One just checks that the inner products of these vectors, under the standard pairing, are the same as those of the δ_{ij} .) Write M for the span of the δ_{ij} ; $L_3(3)$ acts on this coordinate system by permuting coordinates as it permutes the lines of $P^2\mathbb{F}_3$.

Now, N is strictly larger than M , because computation shows that if i, j and k are general lines, then $\langle r_{ij} - r_{jk} | \delta_{ik} \rangle \notin 3\mathcal{E}$. We can apply lemma 6 to both N and X and conclude from the uniqueness proven there that $N = X$. (We have also shown that $N = X$ admits an automorphism exchanging the vectors of the form $(\theta, \bar{\theta}, 0^{11})$ with those of the form $(1^3, -1^3, 0^7)$.) \square

Proof of theorem 1: It remains only to prove $R = \text{Aut } L$. The primitive null vector ρ of lemma 9 has Leech type, because theorem 4 tells us that the complex Leech lattice is the only Eisenstein Niemeier lattice whose automorphism group contains $L_3(3)$. Lemmas 8 and 9 assure us that R contains the unipotent radical of the stabilizer of ρ (U from the proof of lemma 8). This acts transitively on the roots $r \in L$ with $\langle r | \rho \rangle = \theta$, so R contains all their triflections. Then the proof of theorem 4.1 of [2] shows that R acts transitively on null vectors of Leech type, so R contains the triflections in every root having inner product θ with some null vector of Leech type. (These are all the roots of L by [4, prop. 4.3], but we don't need this.) The triflections in the point roots obviously have this property, and those in the line roots do too (by conjugacy). Therefore R is exactly the group generated by triflections in the roots with this property, so R is normal in $\text{Aut } L$.

Therefore R 's intersection with the stabilizer H of ρ is normal in H . Since we already know that R contains $U \triangleleft H$, R is determined by its image in $H/U \cong 6Suz$. We also know (lemma 7) that $R \cap H$ contains $L_3(3)$. By the simplicity of Suz , $(R \cap H)/U \subseteq 6Suz$ surjects to Suz . Since $6Suz$ is a perfect central extension of Suz , its only subgroup surjecting to Suz is itself. Therefore $(R \cap H)/U = 6Suz$. It follows that $R \cap H$ is all of H . We have shown that R acts transitively on the primitive null vectors of Leech type, and contains the full stabilizer of one of them. So $R = \text{Aut } L$. \square

Remark. One can recover Wilson's $L_3(3)$ -invariant description of the complex Leech lattice $\Lambda_{24}^{\mathcal{E}}$ (see the end of [9]) by writing down generators for ρ^\perp and then adding suitable multiples of ρ to shift them into $M \otimes_{\mathcal{E}} \mathbb{C}$, where M is from the proof of lemma 9.

Remark. We observed that ρ has Leech type. One can show by patient calculation that $(\theta; \theta, 0^{12})$ has E_6 type, $(\theta; \bar{\theta}, 0^{12})$ has A_2 type, $(3 + \omega; 1^4, -1^3, 0^6)$ has D_4 type, and $(2\theta; \theta^4, 0^9)$ has E_8 type. (In the last case, we specify that the four θ 's are at 4 points of $P^2\mathbb{F}_3$ in general position.)

REFERENCES

- [1] D. Allcock, New complex- and quaternion-hyperbolic reflection groups, *Duke Math. J.* **103** (2000) 303–333.
- [2] D. Allcock, The Leech lattice and complex hyperbolic reflections, *Inv. Math.* **140** (2000) 283–301.
- [3] D. Allcock, A monstrous proposal, to appear in *Groups and Symmetries: From the Neolithic Scots to John McKay*, ed. J. Harnad, AMS.
- [4] T. Basak, The complex Lorentzian Leech lattice and the bimonster, *J. Alg.* **309** (2007) 32–56.
- [5] J. H. Conway, A characterization of Leech's lattice, *Inv. Math.* **7** (1969) 137–142. Also, ch. 12 of [7].
- [6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *ATLAS of finite groups*, Oxford 1985.
- [7] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer 1993.
- [8] B. B. Venkov, The classification of integral even unimodular 24-dimensional quadratic forms, ch. 18 of [7].
- [9] R. A. Wilson, The complex Leech lattice and maximal subgroups of the Suzuki group, *J. Alg.* **77** (1982) 449–462.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS, AUSTIN

E-mail address: allcock@math.utexas.edu

URL: <http://www.math.utexas.edu/~allcock>