PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 103, Number 3, July 1988

A NEW LATTICE FOR THE HALL-JANKO GROUP

J. H. LINDSEY II

(Communicated by Bhama Srinivasan)

ABSTRACT. Six by six matrix generators with entries in the rational numbers adjoined by a fifth root of unity, and most of these entries 0, are given for the proper central extension of the cyclic group of order 2 by the Hall-Janko group. They are found to preserve a 24-dimensional lattice giving a packing of unit spheres with density about one fourth that of the Leach lattice.

Neat 6 by 6 matrix generators written in $\mathbf{Q}(\mu)$ for μ a primitive fifth root of unity, μ, are found for the proper central extension of Z_2 by the Hall-Janko group of order 604,800. While here the representation is written in $\mathbf{Q}(\mu)$, it could have been written in $\mathbf{Q}(\sqrt{5}, \sqrt{-3})$ or, more generally, in any field containing $\sqrt{5}$ and in which -1 is a sum of two squares, but that is not shown here. A 24-dimensional lattice giving a packing of unit spheres with density about one fourth that of the Leach lattice is preserved by the above group and also by the field automorphisms of $\mathbf{Q}(\mu)$ and scalar multiplication by μ. The field automorphism gives the outer automorphism of the Hall-Janko group. Together, all these operations above generate a group of order (10)(604,800)(4) which acts transitively on the 37,800 points closest to the origin. There are five orbits of oriented equilateral triangles with the origin and closest lattice points to the origin as vertices. The lengths of the orbits are 20, 80, 80, 160, and 320, when an edge is left fixed.

1. Generators and the lattice. Let μ be a primitive fifth root of unity, $\beta = (\mu^4 + \mu - \mu^2 - \mu^3)/5$ (so $\beta^2 = 1/5$), $p = \beta(\mu^4 - \mu)$, and $q = \beta(\mu^2 - \mu^3)$. Then the following matrices turn out to generate the proper central extension of Z_2 by the Hall-Janko group.

Let G be the group generated by the following 6 by 6 unitary matrices (C and D are given in block diagonal form):

$$A = \operatorname{diag}(\mu, \mu, \mu^4, \mu^4, 1, 1),$$

$$B = \operatorname{diag}(\mu, \mu^4, \mu, \mu^4, \mu^2, \mu^3),$$

$$C = \begin{pmatrix} p & q \\ q & -p \end{pmatrix} \oplus \begin{pmatrix} p & q \\ q & -p \end{pmatrix} \oplus \begin{pmatrix} q & -p \\ -p & -q \end{pmatrix},$$

$$D = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$E =$ the permutation matrix corresponding to $(1,6)\ (4,5)$.

These matrices act on the column vectors $v = (v_1, v_2, v_3, v_4, v_5, v_6)^t$ with entries v_i lying in $\mathbf{Q}[\mu]$. Let L be the lattice consisting of these vectors satisfying the following conditions: (Here equal mod $5^{i/4}$ means that the difference lies in

Received by the editors June 1, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20G20; Secondary 20G05.

$(\mu-1)^i Z[\mu]$, that is has valuation at least i with respect to the valuation of the ring $Z[i]$ that takes 5 to 4 and $\mu-1$ to 1.)

(1) The entries v_i lie in $Z[\mu]$.

(2) The vector is a $Z[\mu]$ multiple of $(1,-2,-1,2,2,1)^t \pmod{5^{1/4}}$.

$$2v_1+v_2+2v_3+v_4 \equiv 0 \pmod{5^{2/4}}, \tag{3}$$

$$v_2+2v_3+v_5+2v_6 \equiv 0 \pmod{5^{2/4}}, \tag{4}$$

$$v_1-2v_2-v_3+2v_4+2v_5+v_6 \equiv 0 \pmod{5^{3/4}}. \tag{5}$$

It is easy to check that the matrices D and E preserve this lattice. This amounts to showing that they take the vector or vector of coefficients in equations (2) and (5) to multiples of the original (mod 5) and take the vectors of coefficients in equations (3), (4), and (5) into the 3-dimensional space over the field of 5 elements generated by the original three vectors. To check that A and B preserve L (we need not check B since $B=A(E^{-1}AE)^3$) the following lemma is useful:

2. Congruences in $Z[\mu]$.

LEMMA. *Let μ be a primitive pth root of unity for p an odd prime. Let a_i lie in $Z[\mu]$ for $i=0,\dots,m$. Let n be a nonnegative integer. Then for $\sum_i a_i\mu^i \equiv 0 \pmod{p^{n/(p-1)}}$ it suffices that*

$$\sum_i a_i \binom{i}{k} \equiv 0 \pmod{p^{(n-k)/(p-1)}} \tag{6}$$

for $k=0,\dots,n-1$. We define the binomial coefficient to be 0 if the bottom entry is greater than the top.

When $n \le p$ the lemma still holds if in equation (6) we replace $\binom{i}{k}$ by i^k.

PROOF. Allow the same exponent i to occur in different terms. Use induction on n, the case $n=0$ being trivial. It suffices to prove the difference of the congruence in the conclusion and that of the hypothesis for $k=0$. After dividing by $\mu-1$ this becomes

$$\sum_i \sum_{j=0}^{i-1} a_i \mu^j \equiv 0 \pmod{p^{(n-1)/(p-1)}}.$$

By induction hypothesis, for this it suffices to show

$$\sum_i \sum_{j=0}^{i-1} a_i \binom{j}{k} \equiv 0 \pmod{p^{(n-1-k)/(p-1)}}$$

for $k=0,\dots,(n-1)-1$. Using

$$\sum_{j=0}^{i-1} \binom{j}{k} = \binom{i}{k+1},$$

the above congruence becomes

$$\sum_i a_i \binom{i}{k+1} \equiv 0 \pmod{p^{(n-(k+1))/(p-1)}}$$

for $k+1 = 1, \ldots, n-1$ which is part of our hypothesis.

As $\binom{i}{k}$ is a polynomial of degree k in i with denominators invertible modulo p^2 when $k < p$ the last statement follows.

Suppose that v satisfies our conditions, equation (1) through (5). Then $Av \equiv v \pmod{5^{1/4}}$ and satisfies equations (1) and (2). We use the last sentence of the lemma to show Av satisfies equations (3), (4), and (5). The $k = 0$ hypothesis follows from v satisfying the equations. For equations (3) and (4) we need only check $k = 1$. For equation (3) this becomes $2(1)v_1 + (1)v_2 + 2(-1)v_3 + (-1)v_4 \equiv 0 \pmod{5^{1/4}}$. By equation (2) we need only check this for $v = (1, -2, -1, 2, 2, 1)^t$. Checking equation (4) is similar. The $k = 2$ hypothesis for equation (5) becomes just the $k = 0$ hypothesis with a weaker modulus, so it follows. The $k = 1$ hypothesis follows from equation (3).

Finally we assume that v satisfies (1) through (5) and show that then Cv does. For this we use

$$3p - q = \beta(\mu^3 - 3\mu + 3\mu^{-1} - \mu^{-3}) = \beta(\mu - \mu^{-1})^3 \equiv 0 \pmod{5^{1/4}} \tag{7}$$

since the above has valuation $-2+3$ since β^2 has valuation -4. When Cv replaces v in the left-hand side of equation (5) we get $p(v_1 + 2v_2 - v_3 - 2v_4 - v_5 - 2v_6)$ $+q(-2v_1 + v_2 + 2v_3 - v_4 + 2v_5 - v_6)$. The coefficients in the coefficient of q here are the same as subtracting the coefficients of equation (3) from twice the coefficients of equation (4). Thus the coefficient of q is 0 mod $5^{2/4}$ and so by equation (7) q may be replaced by $3p$ without changing the above mod $5^{(2+1)/4}$. Then after combining terms above the coefficients of the pv_i are all divisible by 5 and congruent to 0 mod $5^{(-1+4)/4}$ so equation (5) follows for Cv. Equations (3) and (4) are similar except that here in changing q to $3p$ we need only check that the coefficient of q is 0 mod $5^{1/4}$ and by equation (2) this follows by seeing that it is true if v were replaced by $(1, -2, -1, 2, 2, 1)^t$. For equation (4) after changing q to $3p$ and combining, we use equation (5) to get 0 mod $5^{(-1+3)/4}$.

3. A norm for the lattice and the lattice density. Let f be the $\mathbf{Q}$-linear function on $\mathbf{Q}[\mu]$ well defined by $f(a+b\mu+c\mu^2+d\mu^3+e\mu^4) = a-(b+c+d+e)/4$ (so $f = (1/4)Tr$). Let M be any one of the matrices A, B, C, D, E generating G. Then M is unitary and $f((Mv)^t(Mu)^*) = f(v^t u^*)$ where * is complex conjugation and so the $\mathbf{Q}$-bilinear form defined by $(v, u) = f(v^t u^*)$ is preserved by G. Using equation (1), using divisibility of $1^2+(-2)^2+(-1)^2+2^2+2^2 = 1^2$ by 5, and using divisibility of $f(x) - x$ by $(\mu - 1)/4$ for x in $Z[\mu]$, we have $(L, L) \subseteq \mathbf{Q} \cap (\mu - 1)Z[\mu]/4 = 5Z/4$. Let $g_i = (\mu^i, 0, 0, 0, 0, 0)$ and e_i be the ith column of the identity matrix $i = 1, \ldots, 4$. Then the matrix of the g_i for (,) is the symmetric matrix (and so (,) is symmetric) $(5/4)I_4 - J$ where J is the 4 by 4 matrix all of whose entries are $1/4$. Then J is symmetric with eigenvalue space $\{(x, y, z, w)^t | x+y+z+w = 0\}$ of dimension 3 with eigenvalue 0 and eigenvector $(1, 1, 1, 1)^t$ with eigenvalue 1. Therefore there exists an orthogonal matrix P with $P^t J P = \mathrm{diag}(k_m)$ with $k_1 = k_2 = k_3 = 0$ and $k_4 = 1$. Let $f_i = (g_1, g_2, g_3, g_4)Pe_i$ be the linear combination of the g_i with Pe_i's entries for coefficients. As P is orthogonal and hence has determinant ± 1 the parallelopiped

with edges $g_i, i = 1, \ldots, 4$, emanating from the origin has the same volume as the parallelopiped with f_i for edges. As

$$\begin{aligned}(f_i, f_j) &= (Pe_i)^t(\tfrac{5}{4}I_4 - J)(Pe_j) = {e_i}^t(P^t(\tfrac{5}{4}I_4 - J)P)e_j \\ &= {e_i}^t(\tfrac{5}{4}I_4 - \operatorname{diag}(k_m))e_j = e_i^t(\operatorname{diag}(\tfrac{5}{4}, \tfrac{5}{4}, \tfrac{5}{4}, \tfrac{1}{4}))e_j \\ &= \delta_{ij}(\tfrac{5}{4} - k_i),\end{aligned}$$

the latter parallelopiped is a $(5/4)^{1/2}$ by $(5/4)^{1/2}$ by $(5/4)^{1/2}$ by $(1/4)^{1/2}$ rectangular box and has volume $(5/4)^{3/2}(1/4)^{1/2} = 5^{3/2}2^{-4}$. Also this shows that $(\ ,\ )$ is positive definite. We add to the g_i 20 additional vectors using the second through sixth coordinates the same way the g_i used the first. These twenty-four vectors are a basis for $L \otimes \mathbf{Q}$ and their matrix for $(\ ,\ )$ is the previous direct summed with itself six times. Thus they generate a parallelopiped of volume $(5^{3/2}2^{-4})^6 = 5^9 2^{-24}$. By equation (1), L is a sublattice of the lattice generated by our 24 vectors, which had one point per volume $5^9 2^{-24}$. Invoking equation (2) imposes an index 5^5. Equations (3), (4), (5) taken mod $5^{2/4}$ are independent and impose another factor 5^3. The stronger modulus in equation (5) imposes another factor 5, so finally we see that the index of L is $5^5 5^3 5 = 5^9$ and so L has one point per volume $(5^9 2^{-24})5^9 = 5^{18}2^{-24}$.

4. Identifying the group. When we let G act on $L \otimes R$ with real inner product $(\ ,\ )$ extended by real linearity, G is orthogonal and preserves L and so G is finite. Now go back to considering G as a 6-dimensional group over C, the complex numbers, with our original matrices for generators. Suppose that the group is imprimitive (possibly reducible). Suppose that A does not fix the spaces of imprimitivity. Then it must cycle around five linear spaces and have eigenvalues including the fifth roots of unity possibly all multiplied by the same constant, but it does not. Thus A and similarly B fix the spaces of imprimitivity. Then these spaces must be sums of eigenvalue spaces for $\langle A, B\rangle$. The coordinate axes give six $\langle A, B\rangle$-invariant linear spaces and they give all different characters. Thus any space of imprimitivity is a sum of coordinate axes. The underlying permutation of DE is $(1, 2, 6, 4, 3, 5)$ so DE is transitive on the spaces of imprimitivity and $(DE)^6$ fixes them. One case is DE is a 6-cycle on the spaces of imprimitivity in which case they are the coordinate axes. Another case of DE is a 3-cycle on all of them in which case $(DE)^3$ with $(1,4)(2,3)(6,5)$ underlying fixes the spaces, the first and fourth coordinate axes V_1 and V_4 lie in the same space, second and third in the same, and sixth and fifth in the same. In this case there are three different spaces, so there must be $V_1 \oplus V_4$, $V_2 \oplus V_3$, and $V_6 \oplus V_5$. A third case is that DE is a 2-cycle on all of them. Then $(DE)^2$ fixes then and as in the previous case the spaces are $V_1 \oplus V_6 \oplus V_3$, and $V_2 \oplus V_4 \oplus V_5$. In each of these cases C takes $(1, 0, 0, 0, 0, 0)^t$ in a space of imprimitivity into $(p, q, 0, 0, 0, 0)^t$ in none of the spaces so these cases are all impossible. Thus DE fixes the spaces of imprimitivity, there is only one space, and G is primitive. If G is not strongly primitive its projective group is a subdirect product of a tensor product of a 2-dimensional primitive projective group and a 3-dimensional projective group. By the unimodular subgroup $\langle A, B\rangle$ the groups are both A_5 and $\langle A, B\rangle$ is a subgroup of the projective group, contrary to the fact that it does not contain an element with the eigenvalues of $c\operatorname{diag}(\mu, \mu^{-1}) \otimes I_3$ for any c. Then as 5^2 divides the order of the projective group given by G, by the

classification of 6-dimensional groups in [2] the projective group is the Hall-Janko group.

5. Closest points to the origin. Of course $F = \mu I_6$ also preserves L and $(\ ,\ )$. So does H, the operation of applying the field automorphism of $\mathbf{Q}(\mu)$ taking μ to μ^2 to all the entries, except that H is only $\mathbf{Q}$-linear, not $\mathbf{Q}[\mu]$-linear. Therefore, when we expand G to, say K, by throwing in F and H we have to consider K to be a 24-dimensional group over $\mathbf{Q}$. I classified the orbits for the points of L closest to the origin by the monomial group $\langle A, B, D, E, F, H\rangle$. A representative of the orbit is preceded by a label for the orbit and the number of elements in the orbit.

$$
\begin{array}{lll}
A & 3000 & (1,-2,-1,\mu+\mu^{-1},\mu^2+\mu^{-2},1)\\
B & 6000 & (1,2\mu+\mu^{-2},-1,\mu^2+\mu^{-2},\mu^2+\mu^{-2},1)\\
C & 3000 & (\mu+\mu^{-1}-1,-\mu^2-\mu^{-2},-1,\mu^2+\mu^{-2},\mu^2+\mu^{-2},1)\\
D & 12000 & (\mu+\mu^2-\mu^3,-\mu-\mu^{-1},-1,\mu+\mu^{-1},\mu^2+\mu^{-2},1)\\
E & 6000 & (\mu+\mu^2-\mu^3,-\mu-\mu^{-1},-1,\mu^2+\mu^{-2},\mu+\mu^{-1},1)\\
F & 3000 & (0,0,\mu^2-\mu^{-2},\mu-\mu^{-1},\mu^3-\mu^{-3},\mu^{-1}-\mu)\\
G & 3000 & (0,\mu^2-\mu^{-2},0,\mu^{-2}-\mu^2,\mu-\mu^{-1},\mu-\mu^{-1})\\
H & 1500 & (0,\mu^{-2}-\mu^2,\mu-\mu^{-1},0,\mu^{-2}-\mu^2,\mu-\mu^{-1})\\
I & 300 & (\mu^2+\mu^{-2}-\mu-\mu^{-1},0,\mu^2+\mu^{-2}-\mu-\mu^{-1},0,0,0)
\end{array}
$$

These orbits are first separated by the shape of the vector which is the set of forms of the six entries. The form of an entry is the set of coefficients of the distinct μ^i terms modulo adding a multiple of $1+\mu+\mu^2+\mu^3+\mu^4$. The underlying permutation group of coordinate axes for the monomial group is D_6 acting on the regular hexagon with vertices in order 1, 2, 6, 4, 3, 5. Thus the orbits $\{1,6,3\}$ and $\{2,4,5\}$ are sets of imprimitivity, as are $\{1,4\}$, $\{2,3\}$, and $\{6,5\}$. The 6 unordered pairs of adjacent vertices form an orbit of pairs as do the 6 pairs of vertices separated by a vertex between them. The 6 unordered triples of consecutive (in some order) vertices form an orbit as do the 12 triples containing just one pair of adjacent vertices. Along with the above sets of imprimitivity this accounts for all pairs and triples. The orbits F, G, and H are distinguished by where the pair of zeros lies. In finding a representative of these orbits given the shapes of the nonzeros and the orbit of the pair of zeros, $\langle D, E\rangle$ was used to put the zeros in specific places, say the first two entries in F. Then multiplying by an appropriate element of our diagonal group $\langle A, B, F\rangle$ the $\mu^i - \mu^j$ in entries three, four, and five were taken to have $j = -i$. Equation (5) with the last sentence of the converse lemma (The converse holds at least when the hypotheses a_i rational and $n < p$ are added.) for $k = 2$ then force $j^2 = i^2$ for the sixth term. Assume $j = -i$ since $\mu^i - \mu^i = \mu^0 - \mu^{-0}$. By applying a power of the field automorphism I assumed the fourth entry was $\mu - \mu^{-1}$. Then equations (3), (4), and (5) and the converse lemma were used to calculate other parameters. In the other cases singly-occurring forms were put in specific places and I proceeded similarly. In C the μ^i/μ^j ratios of the $\pm\mu^i \pm \mu^j$ terms modulo reciprocation were the same, which distinguished C from D and E where they were different. In E the singly-occurring ratio was in the fourth entry which was antipodal to the first entry which held the singly-occurring form. This distinguishes E from D where they were not antipodal.

Here is the classification of orbits of vectors of the common shape of C, D, and E. After using $\langle D, E\rangle$ to put $\mu^i+\mu^j-\mu^k$ (which, when $k=j$, is unitary monomial. This will turn out to be impossible. This helps preclude square norm 7.5 for a vector which would show it must be at least 10 since 5/2 divides it.) In the first entry, equation (2) and square length no larger than 10 force monomials with coefficient ± 1 in the third and sixth extries and determine the sign of the coefficient. The exponents of the $(1,1)$, $(3,3)$, and $(6,6)$ entries of the diagonal matrices A, B, and F form a nonsingular 3 by 3 matrix over the field of 5 elements, so applying an appropriate element in $\langle A, B, F\rangle$, we may assume $i+j-k=0$ and the monomials $\pm\mu^q$ are ± 1. Then the converse of the lemma and nonsingularity of the 3 by 3 matrix formed by the coefficients of v_2, v_4, and v_5 in equations (3), (4), and (5) force the $\pm(\mu^a+\mu^b)$ in the second, fourth, and fifth terms to have $b=-a$. We are down to $(\mu^i+\mu^j-\mu^{i+j}, -\mu^a-\mu^{-a}, -1, \mu^b+\mu^{-b}, \mu^c+\mu^{-c}, 1)$. By equation (5) and the $k=2$ in the last sentence of the converse lemma

$$\begin{aligned} 0 &\equiv i^2+j^2-(i+j)^2-2(-a^2-(-a)^2)+2(b^2+(-b)^2)+2(c^2+(-c)^2) \\ &= -2ij+4(a^2+b^2+c^2). \end{aligned}$$

The sign of a does not matter since $-\mu^a$ is paired with $-\mu^{-a}$, similarly for b and c. Suppose that the a, b, and c are the same within sign and mod 5. Possibly applying H, assume $a=b=c=2$. Then $ij\equiv(2)(3)2^2\equiv -1$. When $i=\pm 1$ we have the vector in C. When $i=j=\pm 2$, the form is $2\mu^{\pm 2}-\mu^{\mp 1}$ and the square norm is 12.5. In the other case for a, b, and c we may assume that 1 occurs twice and 2 occurs once by using $\langle H\rangle$. By applying the element in $\langle D, E\rangle$ corresponding to reflecting our hexagon about the diameter connecting vertices 1 and 4, we see $a=b=1$, $c=2$ is the same as $b=c=1$, $a=2$. We are left with the vectors in D and E except possibly for i and j. Here $ij=2(1+1-1)=2$. The cases $i=1$, $j=2$, and $i=2$, $j=1$ give the same vector which is transformed by H^2 into $i=-1$, $j=-2$ and $i=-2$, $j=-1$.

It was easy to see that all orbits were equivalent under the equivalence relation generated by: orbits are equivalent if the matrix C takes some member of one into the other. Thus the closest points to the origin in L, of which there are $37800=(7)(5^2)(3^3)(2^3)$, are permuted transitively by K. The number of points in L which form an equilateral triangle with the origin and the specific point given in orbit I is 660. These points are split up into five orbits of length 20, 80, 80, 160, and 320 under the subgroup fixing the specific point. The orbits respectively contain $(-\mu+\mu^3, \mu-1, -\mu+\mu^3, \mu-1, 0, 0,)$, $(-\mu+\mu^3-\mu^4, \mu+1, \mu^2, -\mu^2-\mu^4, -\mu-\mu^2, -\mu)$, $(-\mu-\mu^4, -1, \mu^2+\mu^3, \mu+\mu^3-\mu^4, 1, -\mu^2-\mu^3)$, $(-\mu+\mu^2+\mu^3-\mu^4, 0, 0, 0, 0, \mu-\mu^2-\mu^3+\mu^4)$, and $(-\mu+\mu^3, -\mu^2+1, \mu^3-\mu^4, 0, \mu^4-1, 0)$.

Let K be the monomial matrix $(DE)^3=(1,4,-1,-4)(2,-3,-2,3)(6,5,-6,-5)$. Then $K^{-1}LK=L^*$, the complex conjugate of L for $L=A$, B, C, D, or E. Thus, if J is the operation of complex conjugation of a vector v, then K and J commute and KJ commutes with A, B, C, D, E, and H since $AKJv=AK(v^*)=K(A^*)v^*=K(Av)^*=KJAv$. Thus $v\leftrightarrow KJv$ is a polarity on vectors preserved by the group $\langle A, B, C, D, E, H\rangle$.

Our lattice L has one point per $5^{18}2^{-24}$ volume. Multiplying by the scale factor $2/5^{3/4}$ makes this one point per unit volume. The scale factor changes the original minimal square distnace from the origin of points in L, which was 10 to

$(10)(2/5^{3/4})^2 = 8/5^{1/2}$, so our lattice is not the Leech lattice since there the minimal square distance is 4 with one point per unit volume. As originally (L, L) lay in $5Z/4$, after the scale factor it lies in $Z/5^{1/2}$. If instead we changed by the scale factor $2/5^{1/2}$, (L, L) would lie in Z, there would be one point per 5^6 volume and the minimal square distance would be 8.

REFERENCES

1. J. H. Lindsey II, *On a six dimensional projective representation of the Hall-Janko group*, Pacific J. Math. **35** (1970), 175–186.
2. ——, *Finite linear groups of degree six*, Canad. J. Math. **23** (1971), 771–790.
3. J. Tits, *Quaternions over* $Q(5^{1/2})$, *Leech's lattice and the sporadic group of Hall-Janko*, J. Algebra **63** (1980), 56–75.

DEPARTMENT OF MATHEMATICAL SCIENCES, NORTHERN ILLINOIS UNIVERSITY, DEKALB, ILLINOIS 60115-2888