

THE CONWAY-SLOANE CALCULUS FOR 2-ADIC LATTICES

DANIEL ALLCOCK, ITAMAR GAL, AND ALICE MARK

ABSTRACT. We develop the notational system developed by Conway and Sloane for working with quadratic forms over the 2-adic integers, and prove its validity. Their system is far better for actual calculations than earlier methods, and has been used for many years, but it seems that no proof has been published before now.

Throughout, an *integer* means an element of the ring \mathbb{Z}_2 of 2-adic integers, and we write \mathbb{Q}_2 for \mathbb{Z}_2 's fraction field. A *lattice* means a finite-dimensional free module over \mathbb{Z}_2 equipped with a \mathbb{Q}_2 -valued symmetric bilinear form. Our goal is to develop the Conway-Sloane notational system for such lattices [4, ch. 15]. This calculus is widely used and much simpler than previous systems, but the literature contains no proof of its validity. Conway and Sloane merely mention that they established the correctness of their system of moves by “showing that they suffice to put every form into B. W. Jones’ canonical form [5] yet are consistent with G. Pall’s complete system of invariants [6]”. The only written proof is Bartels’ dissertation [2], which remains unpublished and lacks the elementary character of [4, ch. 15]. And although the foundations are correct, Conway and Sloane made an error defining their canonical form, resolved in [1]. We hope that the present self-contained treatment will make their calculus more accessible.

Briefly, the Conway-Sloane notation attaches a “2-adic symbol” to each Jordan decomposition of a lattice; a complicated example is

$$1_{\mathbb{I}}^2 [2^{-2}4^3]_3 16_1^1 32_{\mathbb{I}}^2 64_{\mathbb{I}}^{-2} [128^1 256^1]_0 512_{\mathbb{I}}^{-4}$$

A term $1_{\mathbb{I}}^{\pm n}$ or $1_t^{\pm n}$ represents a unimodular lattice of dimension n , with the decorations specifying which such lattice. (\mathbb{I} is a formal symbol and t is an integer mod 8.) If q is a power of 2 then we replace $1_{\mathbb{I}}^{\pm n}$ and $1_t^{\pm n}$ by $q_{\mathbb{I}}^{\pm n}$ and $q_t^{\pm n}$ for the lattice got by scaling inner products by q . The chain of symbols represents a direct sum. Terms gathered in brackets “share” their values of the invariant (oddity) appearing in subscripts,

Date: November 14, 2015.

2010 Mathematics Subject Classification. 11E08.

First author supported by NSF grant DMS-1101566.

so that together they have only a single subscript. The 2-adic symbol of a lattice is unique up to “sign-walking” operations, which negate some signs and alter some subscripts by 4 mod 8. These operations are very easy to use: they form an elementary abelian 2-group (as in the proof of theorem 4.3). Walking all the signs as far left as possible gives a canonical form, in the sense that two symbols in canonical form are equal if and only if they represent isometric lattices.

The main virtues of the notation are that (i) it allows easy passage between the notation and the lattices, (ii) the quantities displayed behave well under direct sum, scaling and duality, (iii) no more information is displayed for each constituent than strictly necessary, and (iv) rather than being constrained to a single canonical form, one can easily pass between all possible Jordan decompositions. The main theorem is 4.2.

This note developed from part of a course on quadratic forms given by the first author at the University of Texas at Austin, with his lecture treatment greatly improved by the second and third authors.

1. PRELIMINARIES

We assume known that two odd elements of \mathbb{Z}_2 differ by a square factor if and only if they are congruent mod 8. All lattices considered will be nondegenerate. A lattice is *integral* if all inner products are integers. An integral lattice is called *even* if all its elements have even norm (self-inner-product), and *odd* otherwise. Given some basis for a lattice, one can seek an orthogonal basis by trying to use the Gram-Schmidt diagonalization process. This almost works but not quite. Instead it shows that every lattice is a direct sum of 1-dimensional lattices and copies of the two lattices $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ scaled by powers of 2. (See [3, p. 117] or §4.4 of [4, Ch. 15].) We will write $1_{\mathbb{I}}^{+2}$ and $1_{\mathbb{I}}^{-2}$ for these last two lattices, which are even. We write $1_t^{\pm 1}$ for the lattice $\langle t \rangle$ with $t \in \{\pm 1, \pm 3\}$ and the sign being + if $t = \pm 1$ and – if $t = \pm 3$.

The notation $1_{\mathbb{I}}^{\pm 2}$ and $1_t^{\pm 1}$ is a special case of a more general notation that will be available after theorem 3.1 is proven. It involves the *oddity* $o(L)$ of a lattice L , which means the oddity of $L \otimes \mathbb{Q}_2$ in the sense of [4, p. 371]. This is a $\mathbb{Z}/8$ -valued isometry invariant of quadratic spaces over \mathbb{Q}_2 which may be computed as follows. One diagonalizes the inner product matrix over \mathbb{Q}_2 and adds up the odd parts of the diagonal entries, plus 4 for each diagonal entry which is an *antisquare*, meaning a 2-adic number of the form $2^{\text{odd}}u$ where $u \in \mathbb{Z}_2^\times$ has $\left(\frac{u}{2}\right) = -$. Recall that the Legendre symbol $\left(\frac{u}{2}\right)$ is + or – according to whether $u \equiv \pm 1$ or $u \equiv \pm 3 \pmod{8}$.

Now suppose U is a *unimodular* lattice, meaning that it is integral and the natural map from U to its *dual lattice* $U^* := \text{Hom}(U, \mathbb{Z}_2)$ is an isomorphism. The *sign* of U means the Legendre symbol $(\frac{\det U}{2})$. The symbol for U is $1_{\mathbb{I}}^{\pm n}$ or $1_t^{\pm n}$ where the sign is the sign of U , n is $\dim U$ and the subscript is \mathbb{I} if U is even and the oddity $t \in \mathbb{Z}/8$ if U is odd. Theorem 3.1 shows that two unimodular lattices are isometric if and only if they have the same symbol. Until we have proven this we will only use $1_t^{\pm 1}$ and $1_{\mathbb{I}}^{\pm 2}$, meaning the specific lattices given above.

If q is a power of 2 then we write $q_{\mathbb{I}}^{\pm n}$ or $q_t^{\pm n}$ for the lattice got from $1_{\mathbb{I}}^{\pm n}$ or $1_t^{\pm n}$ by rescaling all inner products by q . For example, $2_{\mathbb{I}}^{-2}$ has inner product matrix $(\begin{smallmatrix} 4 & 2 \\ 2 & 4 \end{smallmatrix})$. The number q is called the *scale* of the symbol (or lattice). We say the scaled lattice has *type* I or II according to whether the unimodular lattice is odd or even. **Caution:** in the type I case, the subscript is the oddity of the unimodular lattice, not the scaled lattice. These may differ by 4 because of the antisquare term in the definition of oddity. For example, the 2-adic lattice 2_3^{-1} has oddity -1 not 3.

Until the more general notation is available we will only use the symbols $q_t^{\pm 1}$ and $q_{\mathbb{I}}^{\pm 2}$. We will usually omit the symbol \oplus from direct sums, writing for example $1_{-1}^{+1} 1_3^{-1} 4_{\mathbb{I}}^{+2}$. To lighten the notation one usually suppresses plus signs in superscripts, for example $1_{-1}^1 1_3^{-1} 4_{\mathbb{I}}^2$, or dimensions when they are 1, for example $1_{-1}^+ 1_3^- 4_{\mathbb{I}}^2$.

2. FINE SYMBOLS

By a *fine decomposition* of a lattice L we mean a direct sum decomposition in which each summand (or *term*) is one of $q_{\pm 1}^1$, $q_{\pm 3}^{-1}$ or $q_{\mathbb{I}}^{\pm 2}$, with the last case only occurring if every term of that scale has type II. This kind of decomposition is finer than the Jordan decompositions considered in the next section. A fine decomposition always exists, by starting with a decomposition as a sum of $q_t^{\pm 1}$'s and $q_{\mathbb{I}}^{\pm 2}$'s and applying the next lemma repeatedly.

Lemma 2.1. *If $\varepsilon, \varepsilon'$ are signs then $1_t^{\varepsilon 1} 1_{\mathbb{I}}^{\varepsilon' 2}$ admits an orthogonal basis.*

Proof. Write M and N for the two summands and consider the three elements of $(M/2M) \oplus (N/2N)$ that lie in neither $M/2M$ nor $N/2N$. Any lifts of them have odd norms and even inner products. Applying row and column operations to their inner product matrix leads to a diagonal matrix with odd diagonal entries. \square

In order to discuss the relation between distinct fine decompositions of a given lattice, we introduce the following special language for 1-dimensional lattices only. We call q_1^{+1} and q_{-3}^{-1} “givers” and q_{-1}^{+1} and

q_3^{-1} “receivers”. (Type II lattices are neither givers nor receivers.) The idea is that a giver can give away two oddity and remain a legal symbol ($q_1^+ \rightarrow q_{-1}^+$ or $q_{-3}^- \rightarrow q_3^-$), while a receiver can accept two oddity. We often use a subscript R or G in place of the oddity, so that 1_G^+ and 1_G^- mean 1_1^+ and 1_{-3}^- , while 1_R^+ and 1_R^- mean 1_{-1}^+ and 1_3^- . Scaling inner products by -3 negates signs and preserves giver/receiver status, while scaling them by -1 preserves signs and reverses giver/receiver status.

A *fine symbol* means a sequence of symbols $q_{\mathbb{II}}^{\pm 2}$ and $q_{R \text{ or } G}^{\pm}$. We pass to numerical subscripts whenever convenient, and regard two symbols as the same if they differ by permuting terms.

Lemma 2.2 (Sign walking). *Consider a fine symbol and two terms of it that satisfy one of the following conditions:*

- (0) *they have the same scale;*
- (1) *they have adjacent scales and different types;*
- (2) *they have adjacent scales and are both givers or both receivers;*
- (3) *their scales differ by a factor of 4 and they have type I.*

Consider also the fine symbol got by negating the signs of these terms and in case (2) also changing both from givers to receivers or vice-versa. Then the lattices represented by the two fine symbols are isometric.

An alternate name for (3) might be sign jumping. Conway and Sloane informally describe it as a composition of two sign walks of type (1). For example,

$$1_1^+ 2_{\mathbb{II}}^{+0} 4_1^1 \rightarrow 1_{-3}^- 2_{\mathbb{II}}^{-0} 4_1^1 \rightarrow 1_{-3}^- 2_{\mathbb{II}}^{+0} 4_{-3}^{-1}.$$

But strictly speaking this doesn't make sense since $2_{\mathbb{II}}^{-0}$ is illegal: a 0-dimensional lattice has determinant 1, hence sign +.

Proof. It suffices to prove the following isometries, where $\varepsilon, \varepsilon'$ are signs, X represents R or G , and X' represents R or G :

- (0) $1_{\mathbb{II}}^{\varepsilon 2} 1_{\mathbb{II}}^{\varepsilon' 2} \cong 1_{\mathbb{II}}^{-\varepsilon 2} 1_{\mathbb{II}}^{-\varepsilon' 2}$ and $1_X^{\varepsilon} 1_{X'}^{\varepsilon'} \cong 1_{X'}^{-\varepsilon} 1_X^{-\varepsilon'}$
- (1) $1_{\mathbb{II}}^{\varepsilon 2} 2_{X'}^{\varepsilon'} \cong 1_{\mathbb{II}}^{-\varepsilon 2} 2_{X'}^{-\varepsilon'}$ and $1_{X'}^{\varepsilon'} 2_{\mathbb{II}}^{\varepsilon 2} \cong 1_{X'}^{-\varepsilon'} 2_{\mathbb{II}}^{-\varepsilon 2}$
- (2) $1_G^{\varepsilon} 2_G^{\varepsilon'} \cong 1_R^{-\varepsilon} 2_R^{-\varepsilon'}$
- (3) $1_X^{\varepsilon} 4_{X'}^{\varepsilon'} \cong 1_X^{-\varepsilon} 4_{X'}^{-\varepsilon'}$

The first part of (0) is trivial except for the assertion $1_{\mathbb{II}}^{+2} 1_{\mathbb{II}}^{+2} \cong 1_{\mathbb{II}}^{-2} 1_{\mathbb{II}}^{-2}$. Choose a norm 4 primitive vector x of the right side. Then choose y to have inner product 1 with x . The span of x and y is even of determinant $\equiv -1 \pmod{8}$, so it is $1_{\mathbb{II}}^{+2}$. Its orthogonal complement must also be even unimodular, hence one of $1_{\mathbb{II}}^{\pm 2}$, hence $1_{\mathbb{II}}^{+2}$ by considering the determinant.

The second part of (0) is best understood using numerical subscripts: $1_t^{\varepsilon} 1_{t'}^{\varepsilon'} \cong 1_{t+4}^{-\varepsilon} 1_{t'+4}^{-\varepsilon'}$, i.e., $\langle t, t' \rangle \cong \langle t+4, t'+4 \rangle$. To see this, note that the

left side represents $t + 4t' \equiv t + 4 \pmod{8}$, that this is odd and therefore corresponds to some direct summand, and the determinants of the two sides are equal. Note that givers and receivers always have oddities congruent to 1 and $-1 \pmod{4}$, so changing a numerical subscript by 4 doesn't alter giver/receiver status. Furthermore, the sign changes since exactly one of $t, t + 4$ lies in $\{\pm 1\}$ and the other in $\{\pm 3\}$. The same argument works for (3), in the form $1_t^\varepsilon 4_{t'}^{\varepsilon'} \cong 1_{t+4}^{-\varepsilon} 4_{t'+4}^{-\varepsilon'}$.

For the first part of (1) we choose a basis for $1_{\mathbb{H}}^{\varepsilon 2}$ with inner product matrix $\begin{pmatrix} 2 & \\ & 1_{\text{or } 2} \end{pmatrix}$ where the lower right corner depends on ε . Replacing the second basis vector by its sum with a generator of $2_{X'}^{\varepsilon'}$, changes the lower right corner by $2 \pmod{4}$. This toggles the 2×2 determinant between -1 and $3 \pmod{8}$. Therefore it gives an even unimodular summand of determinant -3 times that of $1_{\mathbb{H}}^{\varepsilon 2}$, hence of sign $-\varepsilon$. Since the overall determinant is an invariant, the determinant of its complement is therefore -3 times that of $2_{X'}^{\varepsilon' 2}$. So the complement is got from $2_{X'}^{\varepsilon' 2}$ by scaling by -3 . We observed above that scaling by -3 negates the sign and preserves giver/receiver status, so the complement is $2_{X'}^{-\varepsilon' 2}$. The second part of (1) follows from the first by passing to dual lattices and then scaling inner products by 2. (It is easy to see that the dual lattice has the same symbol with each scale replaced by its reciprocal.)

(2) After rescaling by -3 if necessary to take $\varepsilon = +$, it suffices to prove $1_G^+ 2_G^{\varepsilon'} \cong 1_R^- 2_R^{-\varepsilon'}$, i.e., $\langle 1, 2 \rangle \cong \langle 3, 6 \rangle$ and $\langle 1, -6 \rangle \cong \langle 3, -2 \rangle$. In each case one finds a vector on the left side whose norm is odd and appears on the right, and compares determinants. \square

Further equivalences between fine symbols are phrased in terms of ‘‘compartments’’. A *compartment* means a set of type I terms, the set of whose scales forms a sequence of consecutive powers of 2, and which is maximal with these properties. For example in $1_{\mathbb{H}}^2 2_G^- 2_R^- 4_G^+ 16_R^-$ one compartment is $2_G^- 2_R^- 4_G^+$ and the other is 16_R^- .

Lemma 2.3 (Giver permutation and conversion). *Consider a fine symbol and the symbol obtained by one of the following operations. Then the lattices they represent are isometric.*

- (1) *Permute the subscripts G and R within a compartment.*
- (2) *Convert any four G 's in a compartment to R 's, or vice versa.*

Proof. Giver permutation, meaning operation (1), can be achieved by repeated use of the isomorphisms $1_G^\varepsilon 1_R^{\varepsilon'} \cong 1_R^\varepsilon 1_G^{\varepsilon'}$ and $1_G^\varepsilon 2_R^{\varepsilon'} \cong 1_R^\varepsilon 2_G^{\varepsilon'}$ (scaled up or down as necessary). To establish these we first rescale by -3 if necessary, to take $\varepsilon = +$ without loss of generality. This leaves the cases $\langle 1, -1 \rangle \cong \langle -1, 1 \rangle$, $\langle 1, 3 \rangle \cong \langle -1, -3 \rangle$, $\langle 1, -2 \rangle \cong \langle -1, 2 \rangle$ and

$\langle 1, 6 \rangle \cong \langle -1, 10 \rangle$. One proves each by finding a vector on the left whose norm is odd and appears on the right, and comparing determinants.

For giver conversion, meaning operation (2), we assume first that more than one scale is present in the compartment, so we can choose terms of adjacent scales. Assuming four G 's are present in the compartment, we permute a pair of them to our chosen terms, then use sign walking to convert them to receivers. This negates both signs. Then we permute these R 's away, replacing them by the second pair of G 's, and repeat the sign walking. This converts the second pair of G 's to R 's and restores the original signs.

For the case that only a single scale is present we first treat what will be the essential cases, namely $1_G^+ 1_G^+ 1_G^+ 1_G^+ \cong 1_R^+ 1_R^+ 1_R^+ 1_R^+$ and $1_G^- 1_G^+ 1_G^+ 1_G^+ \cong 1_R^- 1_R^+ 1_R^+ 1_R^+$. That is, $\langle 1, 1, 1, 1 \rangle \cong \langle -1, -1, -1, -1 \rangle$ and $\langle -3, 1, 1, 1 \rangle \cong \langle 3, -1, -1, -1 \rangle$. In the first case we exhibit a suitable basis for the left side, namely $(2, 1, 1, 1)$ and the images of $(-1, 2, 1, -1)$ under cyclic permutation of the last 3 coordinates. In the second we note that the left side is the orthogonal sum of the span of $(1, 0, 0, 0)$ and $(0, 1, 1, 1)$, which is a copy of $\langle -3, 3 \rangle$, and the span of $(0, -1, 1, 0)$ and $(0, 0, 1, -1)$, which is a copy of $1_{\mathbb{H}}^{-2}$. Since each of these is isometric to its scaling by -1 , so is their direct sum.

Now we treat the general case when only a single scale is present. Suppose there are at least 4 givers. By scaling by a power of 2 it suffices to treat the unimodular case. By sign walking we may change the signs on any even number of them, so we may suppose at most one $-$ is present. (Recall that sign walking between terms of the same scale doesn't affect subscripts G or R .) By the previous paragraph we may convert four G 's to R 's. Then we reverse the sign walking operations to restore the original signs. \square

The following theorem captures the full classification of 2-adic lattices. But fine symbols package information poorly, and great simplification is possible. We develop this in the next two sections.

Theorem 2.4 (Equivalence of fine symbols). *Two fine symbols represent isometric lattices if and only if they are related by a sequence of sign walking, giver permutation and giver conversion operations.*

Although it is natural to state the theorem here, its proof depends on theorem 3.1. The first place we use it is to prove theorem 4.2, so logically the proof could go anywhere in between. But in fact we have deferred it to section 5 to avoid breaking the flow of ideas.

3. JORDAN SYMBOLS

Theorem 3.1 (Unimodular lattices). *A unimodular lattice is characterized by its dimension, type, sign and oddity.*

Actually, oddity isn't important for even unimodular lattices since it is always 0. One checks this by diagonalizing $1_{\mathbb{II}}^{\pm 2}$ over \mathbb{Q}_2 , obtaining $\langle 1, -1 \rangle$ and $\langle 2, 6 \rangle$, and computing the oddity directly.

Proof. Consider unimodular lattices U, U' with the same dimension, type, sign and oddity, and fine symbols F, F' for them. The product of the signs in F equals the sign of U , and similarly for U' . Since U and U' have the same sign, we may use sign walking to make the signs in F the same as in F' . If U, U' are even then the terms in F are now the same as in F' , so $U \cong U'$. So suppose U, U' are odd.

By giver permutation, and exchanging F and F' if necessary, we may suppose that all non-matching subscripts are R in F and G in F' . And by giver conversion we may suppose that the number of non-matching subscripts is $k \leq 3$. Since changing a receiver to a giver without changing the sign increases the oddity by two, $o(U') = o(U) + 2k$. Since $o(U') \equiv o(U) \pmod{8}$ we have $k = 0$. So the terms in F are the same as in F' , and $U \cong U'$. \square

We now have license to use the notation $q_t^{\pm n}$ and $q_{\mathbb{II}}^{\pm n}$ from section 1. We say that such a symbol is *legal* if it represents a lattice. The legal symbols are

$$\begin{aligned} & q_{\mathbb{II}}^{+0} \\ & q_{\mathbb{II}}^{\pm n} \text{ with } n \text{ positive and even} \\ & q_{\pm 1}^{+1} \text{ and } q_{\pm 3}^{-1} \\ & q_0^{+2}, q_{\pm 2}^{+2}, q_4^{-2} \text{ and } q_{\pm 2}^{-2} \\ & q_t^{\pm n} \text{ with } n > 2 \text{ and } t \equiv n \pmod{2} \end{aligned}$$

A good way to mentally organize these is to regard the conditions for dimension $\neq 1, 2$ as obvious, remember that q_4^2 and q_0^{-2} are illegal, and remember that the subscript of $q_t^{\pm 1}$ determines the sign.

The rules for direct sums of unimodular lattices are easy to remember: signs multiply and dimensions and subscripts add, subject to the special rules $\mathbb{II} + \mathbb{II} = \mathbb{II}$ and $\mathbb{II} + t = t$.

A *Jordan decomposition* of a lattice means a direct sum decomposition whose summands (called *constituents*) are unimodular lattices scaled by different powers of 2. By the *Jordan symbol* for the decomposition we mean the list of the symbols (or *terms*) $q_{\mathbb{II}}^{\pm n}$ and $q_t^{\pm n}$ for the

summands. An example we will use in this section and the next, and mentioned already in the introduction, is

$$1_{\text{II}}^2 2_6^{-2} 4_{-3}^3 16_1^1 32_{\text{II}}^2 64_{\text{II}}^{-2} 128_1^1 256_{-1}^1 512_{\text{II}}^{-4}$$

It is sometimes convenient and sometimes annoying to allow trivial (meaning 0-dimensional) terms in a Jordan decomposition.

The main difficulty of 2-adic lattices is that a given lattice may have several inequivalent Jordan decompositions. The purpose of the Conway-Sloane calculus is to allow one to move easily between all possible isometry classes of Jordan decompositions. Some of the data in the Jordan symbol remains invariant under these moves. First, if one has two Jordan decompositions for the same lattice L , then each term in one has the same dimension as the term of that scale in the other. (Scaling reduces the general case to the integral case, which follows by considering the structure of the abelian group L^*/L .) Second, the type I or II of the term of any given scale is independent of the Jordan decomposition. (One can show this directly, but we won't need it until after theorem 4.2, which implies it.) The signs and oddities of the constituents are not usually invariants of L .

We define a *compartment* of a Jordan decomposition just as we did for fine decompositions: a set of type I constituents, whose scales form a sequence of consecutive powers of 2, which is maximal with these properties. The example above has three compartments: $2_6^{-2} 4_{-3}^3$, 16_1^1 and $128_1^1 256_{-1}^1$. The *oddity* of a compartment means the sum of its subscripts (mod 8 as always). **Caution:** this depends on the Jordan decomposition, and is not an isometry invariant of the underlying lattice. See lemma 4.1(2) for an example of this. Despite this non-invariance, the oddity of a compartment is useful:

Lemma 3.2 (Oddity fusion). *Consider a lattice, a Jordan symbol J for it, and the Jordan symbol J' got by reassigning all the subscripts in a compartment, in such a way that that all resulting terms are legal and the compartment's oddity remains unchanged. Then J, J' represent isometric lattices.*

Proof. By discarding the rest of J we may suppose it is a single compartment. The argument is similar to the odd case of theorem 3.1. We refine J, J' to fine symbols F, F' . By hypothesis, the terms of J' have the same signs as those of J . It follows that for each scale, the product of the signs of F 's terms of that scale is the same as the corresponding product for F' . Therefore sign walking between equal-scale terms lets us suppose that the signs in F are the same as in F' . Recall from the

proof of lemma 2.2(0) that this sort of sign walking amounts to the isomorphisms $1_t^{\varepsilon_1} 1_{t'}^{\varepsilon'_1} \cong 1_{t+4}^{-\varepsilon_1} 1_{t'+4}^{-\varepsilon'_1}$, which don't change the compartment's oddity.

Giver permutation and conversion don't change a compartment's oddity either. This is because changing a giver to a receiver without changing the sign of that term reduces the numerical subscript by 2. So converting one giver to a receiver and one receiver to a giver leaves the compartment's oddity unchanged, as does converting four givers to receivers or vice versa.

By giver permutation and possibly swapping F with F' , we may suppose that the non-matching subscripts are R 's in F and G 's in F' . By giver conversion we may suppose $k \leq 3$ subscripts fail to match, and the assumed equality of oddities shows $k = 0$. So the fine symbols are the same and the lattices are isometric. \square

4. 2-ADIC SYMBOLS

One can translate sign walking between fine symbols to the language of Jordan symbols, but it turns out to be fussier than necessary. Things become simpler once we incorporate oddity fusion into the notation as follows. The *2-adic symbol* of a Jordan decomposition means the Jordan symbol, except that each compartment is enclosed in brackets, the enclosed terms are stripped of their subscripts, and their sum (the compartment's oddity) is attached to the right bracket as a subscript. For our example from section 3 this yields

$$1_{\mathbb{H}}^2 [2^{-2}4^3]_3 [16^1]_1 32_{\mathbb{H}}^2 64_{\mathbb{H}}^{-2} [128^1 256^1]_0 512_{\mathbb{H}}^{-4}$$

If a compartment consists of a single term then one usually omits the brackets: $1_{\mathbb{H}}^2 [2^{-2}4^3]_3 16_1^1 32_{\mathbb{H}}^2 64_{\mathbb{H}}^{-2} [128^1 256^1]_0 512_{\mathbb{H}}^{-4}$. Lemma 3.2 shows that the isometry type of a lattice with given 2-adic symbol is well-defined.

When a compartment has total dimension ≤ 2 then its oddity is constrained by its overall sign in the same way as for an odd unimodular lattice of that dimension. For compartments of dimension 1 this is the same constraint as before. In 2 dimensions, “[1+2-]₀” and “[1-2+]₀” are illegal (cannot come from any fine symbol) because each term 1_{\dots}^{\pm} or 2_{\dots}^{\pm} would have ± 1 as its subscript, while each term 1_{\dots}^- or 2_{\dots}^- would have ± 3 as its subscript. There is no way to choose subscripts summing to 0. The same reasoning shows that “[1+2+]₄” and “[1-2-]₄” are also illegal.

Lemma 4.1 (Sign walking for 2-adic symbols). *Consider the 2-adic symbol of a Jordan decomposition of a lattice and two nontrivial terms of it that satisfy one of the following:*

- (1) *they have adjacent scales and different types;*
- (2) *they have adjacent scales and type I, and their compartment either has dimension > 2 or compartment oddity ± 2 ;*
- (3) *they have type I, their scales differ by a factor of 4, and the term between them is trivial.*

Then the 2-adic symbol got by negating their signs, and changing by 4 the oddity of each compartment involved, represents an isometric lattice.

As remarked after lemma 2.2, one could call (3) sign jumping. One can formulate it even if the intermediate term were nontrivial. But this is not necessary since one could use two sign walks of type (2) resp. (1) if the intermediate term had type I resp. II.

Our example $1_{\mathbb{II}}^2 [2^{-2}4^3]_3 16_1^1 32_{\mathbb{II}}^2 64_{\mathbb{II}}^{-2} [128^1 256^1]_0 512_{\mathbb{II}}^{-4}$ can walk to

$$\begin{aligned} & 1_{\mathbb{II}}^{-2} [2^2 4^3]_{-1} 16_1^1 32_{\mathbb{II}}^2 64_{\mathbb{II}}^{-2} [128^1 256^1]_0 512_{\mathbb{II}}^{-4} && \text{by (1),} \\ \text{or } & 1_{\mathbb{II}}^2 [2^{-2} 4^3]_3 16_1^1 32_{\mathbb{II}}^2 64_{\mathbb{II}}^{-2} [128^1 256^{-1}]_4 512_{\mathbb{II}}^4 && \text{by (1),} \\ \text{or } & 1_{\mathbb{II}}^2 [2^2 4^{-3}]_{-1} 16_1^1 32_{\mathbb{II}}^2 64_{\mathbb{II}}^{-2} [128^1 256^1]_0 512_{\mathbb{II}}^{-4} && \text{by (2),} \\ \text{or } & 1_{\mathbb{II}}^2 [2^{-2} 4^{-3}]_{-1} 16_{-3}^{-1} 32_{\mathbb{II}}^2 64_{\mathbb{II}}^{-2} [128^1 256^1]_0 512_{\mathbb{II}}^{-4} && \text{by (3),} \end{aligned}$$

but no sign walk is possible between the terms of scales 128 and 256.

Proof. Refine the Jordan decomposition to a fine decomposition F , apply the corresponding sign walk operation (1)–(3) from lemma 2.2 to suitable terms of F , and observe the corresponding change in the Jordan symbol. In case (2) care is required because lemma 2.2 requires both terms of F to be givers or both to be receivers. If the compartment has dimension > 2 then we may arrange this by giver permutation (which preserves the compartment oddity and therefore doesn't change the 2-adic symbol). In dimension 2 the (compartment oddity) $\equiv \pm 2$ hypothesis rules out the case that one is a giver and one a receiver, since givers and receivers have subscripts 1 and $-1 \pmod 4$. \square

Theorem 4.2 (Equivalence of 2-adic symbols). *Suppose given two lattices with Jordan decompositions. Then the lattices are isometric if and only if the 2-adic symbols of these decompositions are related by a sequence of the sign walk operations in lemma 4.1.*

Proof. The previous lemma shows that sign walks preserve isometry type. So suppose the lattices are isometric. Refine the Jordan decompositions to fine decompositions, apply theorem 2.4 to obtain a chain

of intermediate fine symbols, and consider the corresponding 2-adic symbols. In the proof of lemma 3.2 we explained why given permutation and conversion don't change the 2-adic symbol, and that sign walking between same-scale terms also has no effect. The effects of the remaining sign walk operations are recorded in lemma 4.1. \square

A lattice may have more than one 2-adic symbol, but the only remaining ambiguity lies in the positions of the signs:

Theorem 4.3. *Suppose two given lattices have 2-adic symbols with the same scales, dimensions, types and signs. Then the lattices are isometric if and only if the symbols are equal (which amounts to having the same compartment oddities).*

Proof. If a 2-adic symbol S of a lattice L admits a sign walk affecting the signs of the terms of scales 2^i , 2^j then we write $\Delta_{i,j}(S)$ for the resulting symbol. No sign walks affect the conditions for $\Delta_{i,j}$ to act on S , since they don't change the type of any term or the oddity mod 4 of any compartment. So we may regard $\Delta_{i,j}$ as acting simultaneously on all 2-adic symbols for L . By its description in terms of negating signs and adjusting compartments' oddities, $\Delta_{i,j}$ may be regarded as an element of order 2 in the group $\{\pm 1\}^T \oplus (\mathbb{Z}/8)^C$ where T is the number of terms present and C is the number of compartments.

We are claiming that if a sequence of sign walks on S restores the original signs, then it also restores the original oddities. We rephrase this in terms of the subgroup A of $\{\pm 1\}^T \oplus (\mathbb{Z}/8)^C$ generated by the $\Delta_{i,j}$. Namely: projecting A to the $\{\pm 1\}^T$ summand has trivial kernel. This is easy to see because the $\Delta_{i,j}$ may be ordered so that they are $\Delta_{i_1,j_1}, \dots, \Delta_{i_n,j_n}$ with $i_1 < j_1 \leq i_2 < j_2 \leq \dots \leq i_n < j_n$. Then the linear independence of their projections to $\{\pm 1\}^T$ is obvious. \square

To get a canonical symbol for a lattice L one starts with any 2-adic symbol S and walks all the minus signs as far left as possible, canceling them whenever possible. To express this formally, we say two scales can interact if their terms are as in lemma 4.1. (We noted in the previous proof that the ability of two scales to interact is independent of the particular 2-adic symbol representing L .) We define a *signway* as an equivalence class of scales, under the equivalence relation generated by interaction. The language suggests a pathway or highway along which signs can move. They can move between two adjacent scales, except when both terms have type II, or both terms have dimension 1 and together form a compartment of oddity 0 or 4. And they can jump across a missing scale, provided both terms have type I. In our example

the signways are the following:

$$\underbrace{1_{\mathbb{I}}^2 [2^{-2}4^3]_3}_{16_1^1} \underbrace{32_{\mathbb{I}}^2}_{64_{\mathbb{I}}^{-2}} \underbrace{[128^1 256^1]_0}_{512_{\mathbb{I}}^{-4}}$$

Note that the absence of a term of scale 8 doesn't break the first signway, while signs cannot propagate between the terms of the "bad" compartment $[128^1 256^1]_0$.

Each signway has a term of smallest scale, and by sign walking we may suppose all terms have sign + except for some of these. In that case we say the symbol is in *canonical form*, which for our example is

$$1_{\mathbb{I}}^{-2} [2^2 4^3]_{-1} 16_1^1 32_{\mathbb{I}}^2 64_{\mathbb{I}}^{-2} [128^1 256^{-1}]_4 512_{\mathbb{I}}^4$$

Theorem 4.3 implies:

Corollary 4.4 (Canonical form). *Given lattices L, L' and 2-adic symbols S, S' for them in canonical form, $L \cong L'$ if and only if $S = S'$. \square*

Conway and Sloane's discussion of the canonical form is in terms of "trains", each of which is a union of one or more of our signways. Our example has two trains, the second consisting of the last two signways. They asserted that signs can walk up and down the length of a train. So, after walking signs leftward, there is at most one sign per train. But this isn't true, as pointed out in [1]. One cannot walk the sign in $[128^1 256^{-1}]_4$ leftward because there is no way to assign subscripts $128_{\pm 3}^- 256_{\pm 1}^+$ so that the compartment has oddity 0.

One can use the ideas of the proof of theorem 4.3 to give numerical invariants for lattices, if one prefers them to a canonical form. For example, one can record the dimensions and types, the *adjusted oddity* of each compartment, and the overall sign of each signway. Here the adjusted oddity of a compartment means its oddity plus 4 for each - sign appearing in its 1st, 3rd, 5th, ... position, with each - sign after the compartment counted as occurring in the "(k+1)st" position, where k is the number of terms in the compartment.

To justify this system of invariants one must check that they are in fact invariant under sign walking, which is easy. Then one shows that there is a unique 2-adic symbol in canonical form having the same invariants as any chosen 2-adic lattice. To do this one first observes that the types of the compartments, together with the adjusted oddities (hence the compartment oddities mod 4), determine the signways. The sign of the first term of each signway is equal to the given overall sign of that signway, and the other signs are +. The signs then allow one to compute the compartment oddities from the adjusted oddities. In fact, these invariants are just a complicated way of recording the canonical

form while pretending not to. They are derived from Theorem 10 of [4, Ch. 15].

5. EQUIVALENCES BETWEEN FINE DECOMPOSITIONS

In this section we give the deferred proof of theorem 2.4: two fine symbols represent isometric lattices if and only if they are related by sign walks and give permutation and conversion. Logically, it belongs anywhere between theorems 3.1 and 4.2. The next two lemmas are standard; our proofs are adapted from Cassels [3, pp. 120–122].

Lemma 5.1. *Suppose L is an integral lattice, that $x, x' \in L$ have the same odd norm, and that their orthogonal complements x^\perp, x'^\perp are either both odd or both even. Then $x^\perp \cong x'^\perp$.*

Proof. First, $(x - x')^2$ is even. If it is twice an odd number then the reflection in it is an isometry of L . This reflection exchanges x and x' , so it gives an isometry between x^\perp and x'^\perp . This argument applies in particular if $x \cdot x'$ is even. So we may restrict to the case that $x \cdot x'$ is odd and $(x - x')^2$ is divisible by 4. Next, note that $(x + x')^2$ differs from $(x - x')^2$ by $4x \cdot x' \equiv 4 \pmod{8}$. So by replacing x' by $-x'$ we may suppose that $(x - x')^2 \equiv 4 \pmod{8}$. This replacement is harmless because $\pm x'$ have the same orthogonal complement.

If it happens that $(x - x') \cdot L \subseteq 2\mathbb{Z}_2$ then the reflection in $x - x'$ preserves L and we may argue as before. So suppose some $y \in L$ has odd inner product with $x - x'$. Then the inner product matrix of $x, x - x', y$ is

$$\begin{pmatrix} 1 & 0 & ? \\ 0 & 0 & 1 \\ ? & 1 & ? \end{pmatrix} \pmod{2},$$

which has odd determinant. Therefore these three vectors span a unimodular summand of L , so L has a Jordan decomposition whose unimodular part L_0 contains both x and x' . Note that x 's orthogonal complement in L_0 is even just if its orthogonal complement in L is, and similarly for x' . So by discarding the rest of the decomposition we may suppose $L = L_0$, without losing our hypothesis that x^\perp, x'^\perp are both odd or both even. Now, x^\perp is unimodular with $\det(x^\perp) = (\det L)/x^2$ and oddity $o(x^\perp) = o(L) - x^2$, and similarly for x' . Since $x^2 = x'^2$, theorem 3.1 implies $x^\perp \cong x'^\perp$. \square

Lemma 5.2. *Suppose L is an integral lattice and $U, U' \subseteq L$ are isometric even unimodular sublattices. Then $U^\perp \cong U'^\perp$.*

Proof. $U \oplus \langle 1 \rangle$ has an orthogonal basis x_1, \dots, x_n by lemma 2.1, and we write x'_1, \dots, x'_n for the basis for $U' \oplus \langle 1 \rangle$ corresponding to it under some

isometry $U \cong U'$. Apply the previous lemma n times, starting with $L \oplus \langle 1 \rangle$. (At the last step we need the observation that the orthogonal complements of U, U' in L are both even or both odd. This holds because these orthogonal complements are even or odd according to whether L is.) \square

Lemma 5.3. *Suppose L is an integral lattice and that 1_G^+ is a term in some fine symbol for L . Then we may apply a sequence of sign walking and giver permutation and conversion operations to transform any other fine symbol F for L into one possessing a term 1_G^+ .*

Proof. We claim first that after some of these operations we may suppose F has a term 1_{\dots}^+ . Because L is odd, F 's terms of scale 1 have the form $1_{R \text{ or } G}^{\pm}$. If F has more than one such term then we can obtain a sign $+$ by sign walking, so suppose it has only one term, of sign $-$. If there are type I terms of scale 4 then again we can use sign walking, so suppose all scale 4 terms have type II. We can do the same thing if there are any terms $2_{\text{II}}^{\pm 2}$. Or terms $2_{R \text{ or } G}^{\pm 1}$, if the compartment consisting of the scale 1 and 2 terms has at least two givers or two receivers. This holds in particular if there is more than one term of scale 2. So

$$F = 1_{R \text{ or } G}^- 4_{\text{II}}^{\dots} 8^{\dots} \dots \quad \text{or} \quad F = 1_{R \text{ or } G}^- 2_{R \text{ or } G}^{\pm} 4_{\text{II}}^{\dots} 8^{\dots} \dots$$

and in the latter case the subscripts cannot be both G 's or both R 's. So there is one of each, and by giver permutation we may suppose

$$F = 1_{R \text{ or } G}^- 4_{\text{II}}^{\dots} 8^{\dots} \dots \quad \text{or} \quad F = 1_G^- 2_R^{\pm} 4_{\text{II}}^{\dots} 8^{\dots} \dots$$

None of these cases occur, because these lattices don't represent 1 mod 8, contrary to the hypothesis that some fine decomposition has a term 1_G^+ . This non-representation is easy to see because L is $\langle \pm 3 \rangle$ or $\langle 5, -2 \rangle$ or $\langle 5, 6 \rangle$, plus a lattice in which all norms are divisible by 8.

So we may suppose F has a term 1_{\dots}^+ . If the compartment C containing it has any givers then we may use giver permutation to complete the proof. So suppose C consists of receivers. If there are 4 receivers then we may convert them to givers, reducing to the previous case. If C has two terms of different scales, neither of which is our 1_{\dots}^+ term, then we may use sign walking to convert them to givers, again reducing to a known case. Only a few cases remain, none of which actually occur, by a similar argument to the previous paragraph.

Namely, after more sign walking we may take F to be

$$(1_R^+ 2_R^{\pm} \text{ or } 1_R^+ 2_R^+ 2_R^{\pm}) 4_{\text{II}}^{\dots} \dots \quad \text{or} \quad (1_R^+ \text{ or } 1_R^+ 1_R^{\pm} \text{ or } 1_R^+ 1_R^+ 1_R^{\pm}) 2_{\text{II}}^{\dots} \dots$$

The first set of possibilities is

$$\left(\langle -1, -2 \rangle \text{ or } \langle -1, 6 \rangle \text{ or } \langle -1, -2, -2 \rangle \text{ or } \langle -1, -2, 6 \rangle \right) \\ \oplus \text{ (a lattice with all norms divisible by 8)}$$

none of which represent 1 mod 8. The second set of possibilities is

$$\left(\langle -1 \rangle \text{ or } \langle -1, -1 \rangle \text{ or } \langle -1, 3 \rangle \text{ or } \langle -1, -1, -1 \rangle \text{ or } \langle -1, -1, 3 \rangle \right) \\ \oplus \text{ (a lattice with all norms divisible by 4)}$$

and only the last two cases represent 1 mod 8. But in these cases every vector x of norm 1 mod 8 projects to $\bar{x} := (1, 1, 1)$ in $U/2U$, where U is the summand $\langle -1, -1, -1 \rangle$ or $\langle -1, -1, 3 \rangle$. There are no odd-norm vectors orthogonal to x since the orthogonal complement of \bar{x} in $U/2U$ consists entirely of self-orthogonal vectors. So while these lattices admit norm 1 summands, they do not admit fine decompositions with 1_G^+ terms. \square

Lemma 5.4. *Suppose $\varepsilon = \pm$. Then lemma 5.3 holds with $1_{\mathbb{H}}^{\varepsilon^2}$ in place of 1_G^+ .*

Proof. If F has two terms of scale 1, or a scale 2 term of type I, then we can use sign walking. The only remaining case is $F = 1_{\mathbb{H}}^{-\varepsilon^2} 2_{\mathbb{H}} 4_{\mathbb{H}} \cdots$. Write U for the $1_{\mathbb{H}}^{-\varepsilon^2}$ summand and note that any two elements of L with the same image in $U/2U$ have the same norm mod 4. Direct calculation shows that the norms of the nonzero elements of $U/2U$ are 0, 0, 2 or 2, 2, 2 mod 4, depending on ε . Now consider the summand $U' \cong 1_{\mathbb{H}}^{\varepsilon^2}$ of L that we assumed to exist. By considering norms mod 4 we see that $U' \rightarrow U/2U$ cannot be injective, which leads to the absurdity that all inner products in U' are even. \square

Proof of theorem 2.4. The “if” part has already been proven in lemmas 2.2 and 2.3, so we prove “only if”. We assume the result for all lattices of lower dimension. By scaling by a power of 2 we may suppose L is integral and some inner product is odd, so each of F and F' has a nontrivial unimodular term.

First suppose L is odd, so the unimodular terms of F and F' have type I. By rescaling L by an odd number we may suppose F has a term 1_G^+ . By lemma 5.3 we may apply our moves to F' so that it also has a term 1_G^+ . The orthogonal complements of the corresponding summands of L are both even (if the unimodular Jordan constituents are 1-dimensional) or both odd (otherwise). By lemma 5.1 these orthogonal complements are isometric. They come with fine decompositions,

given by the remaining terms in F, F' . By induction on dimension these fine decompositions are equivalent by our moves.

If L is even then the same argument applies, using lemmas 5.4 and 5.2 in place of lemmas 5.3 and 5.1. \square

REFERENCES

- [1] Daniel Allcock, *The reflective Lorentzian lattices of rank 3*, in *Memoirs of the A.M.S.* (no. 1033, vol. 220, Nov. 2012).
- [2] Klaus Bartels, *Zur Klassifikation quadratischer Gitter über diskreten Bewertungsringen*, Ph.D. Dissertation Göttingen 1988.
- [3] J.W.S. Cassels, *Rational Quadratic Forms*, Academic Press 1968.
- [4] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, 2nd ed., Springer 1993.
- [5] Burton W. Jones, A canonical quadratic form for the ring of 2-adic integers, *Duke Math. J.* **11** (1944) 715–727.
- [6] Gordon Pall, The arithmetical invariants of quadratic forms, *Bulletin of the A.M.S.* **51** (1945) 185–197.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS AT AUSTIN

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

URL: `http://www.math.utexas.edu/~allcock`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS AT AUSTIN

E-mail address: `igal@math.utexas.edu`

SCHOOL OF MATHEMATICAL AND STATISTICAL SCIENCES, ARIZONA STATE UNIVERSITY

E-mail address: `amark3@asu.edu`